kaspersky

Kaspersky Security Center 15.1 Windows

© 2026 AO Kaspersky Lab

Spis treści

System pomocy Kaspersky Security Center 15.1

Nowości

Informacje o Kaspersky Security Center

- Architektura
- Wymagania sprzętowe i programowe
  - Wymagania Serwera administracyjnego
  - Wymagania Web Console
  - Wymagania dotyczące serwerów mobilnych
  - Wymagania Konsoli administracyjnej
  - Wymagania Agenta sieciowego
- Kompatybilne aplikacje i rozwiązania Kaspersky
- Licencje i funkcje Kaspersky Security Center 15.1
- Informacje o kompatybilności składników Kaspersky Security Center
- Porównanie Kaspersky Security Center: opartego na systemie Windows i opartego na systemie Linux
- Informacje o Kaspersky Next Expert View

Kaspersky Security Center 15.1

- Podstawowe pojęcia
  - Serwer administracyjny
  - Hierarchia Serwerów administracyjnych
  - Wirtualny Serwer administracyjny
  - Serwer urządzeń mobilnych
  - Serwer sieciowy
  - Agent sieciowy
  - Grupy administracyjne
  - Zarządzane urządzenie
  - Urządzenie nieprzypisane
  - Stacja robocza administratora
  - Wtyczka administracyjna
  - Webowa wtyczka administracyjna
  - Zasady
  - Profile zasad
  - Zadania
  - Obszar zadania
  - Jak ustawienia lokalne aplikacji mają się do zasad
  - Punkt dystrybucji
  - Brama połączenia
- Główny scenariusz instalacji
- Porty używane przez Kaspersky Security Center
- Certyfikaty do pracy z Kaspersky Security Center
  - Informacje o certyfikatach Kaspersky Security Center
  - Informacje o certyfikacie Serwera administracyjnego
  - Wymagania dotyczące niestandardowych certyfikatów stosowanych w Kaspersky Security Center
  - Scenariusz: Określanie niestandardowego certyfikatu Serwera administracyjnego

Zastępowanie certyfikatu Serwera administracyjnego za pomocą narzędzia klsetsrvcert
Podłączanie Agentów sieciowych do Serwera administracyjnego przy użyciu narzędzia klmover
Ponowne wystawianie certyfikatu serwera sieciowego
Schematy ruchu sieciowego danych i użycia portów
Serwer administracyjny i zarządzane urządzenia w sieci LAN
Główny Serwer administracyjny w sieci LAN i dwa podrzędne Serwery administracyjne
Serwer administracyjny w sieci LAN, zarządzane urządzenia w Internecie, odwrotny serwer proxy w użyciu
Serwer administracyjny w sieci LAN, zarządzane urządzenia w internecie, brama połączenia w użyciu
Serwer administracyjny w strefie DMZ, zarządzane urządzenia w Internecie
Interakcja komponentów Kaspersky Security Center i aplikacji zabezpieczających: więcej informacji
Konwencje stosowane w schematach interakcji
Serwer administracyjny i DBMS
Serwer administracyjny i Konsola administracyjna
Serwer administracyjny i urządzenie klienckie: zarządzanie aplikacją zabezpieczająca
Aktualizowanie oprogramowania na urządzeniu klienckim poprzez punkt dystrybucji
Hierarchia Serwerów administracyjnych: główny Serwer administracyjny i podrzędny Serwer administracyjny
Hierarchia Serwerów administracyjnych z podrzędnym Serwerem administracyjnym w strefie DMZ
Serwer administracyjny, brama połączenia w segmencie sieci i urządzenie klienckie
Serwer administracyjny i dwa urządzenia w strefie DMZ: brama połączenia i urządzenie klienckie
Serwer administracyjny i Kaspersky Security Center Web Console
Aktywowanie i zarządzanie aplikacją zabezpieczającą na urządzeniu mobilnym
Wdrażanie praktycznego zastosowania aplikacji
Przewodnik po zwiększaniu odporności
Wdrożenie Serwera administracyjnego
Bezpieczeństwo połączenia
Konta i uwierzytelnianie
Zarządzanie ochroną Serwera administracyjnego
Zarządzanie ochroną urządzeń klienckich
Konfigurowanie ochrony dla zarządzanych aplikacji
Konserwacja Serwera administracyjnego
Transfer zdarzeń do systemów innych producentów
Zalecenia dotyczące bezpieczeństwa systemów informatycznych innych firm
Zalecenia dotyczące korzystania z aplikacji zabezpieczających Kaspersky
Przygotowanie do wdrożenia
Planowanie instalacji Kaspersky Security Center
Typowe schematy wdrażania systemu ochrony
Informacje dotyczące planowania instalacji Kaspersky Security Center w sieci organizacji
Wybieranie struktury ochrony firmy
Standardowa konfiguracja Kaspersky Security Center
Standardowa konfiguracja: Jedno biuro
Standardowa konfiguracja: Duże oddziały posiadające swoich administratorów
Standardowa konfiguracja: Małe zdalne biura
Wybieranie systemu zarządzania bazą danych (DBMS) dla Serwera administracyjnego
Stosowanie zbiorczej poprawki CU12 podczas używania SQL Server 2019 jako systemu DBMS
Konfigurowanie serwera MariaDB x64 do pracy z Kaspersky Security Center 15.1
Konfigurowanie serwera MySQL x64 do pracy z Kaspersky Security Center 15.1
Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center 15.1

Zarządzanie urządzeniami mobilnymi z zainstalowanym programem Kaspersky Endpoint Security for Android
Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet
Dostęp do internetu: Serwer administracyjny w sieci lokalnej
Dostęp do internetu: Serwer administracyjny w strefie DMZ
Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej
Informacje o punktach dystrybucji
Zwiększenie limitu deskryptorów plików dla usługi klnagent
Obliczanie liczby i konfigurowanie punktów dystrybucji
Hierarchia Serwerów administracyjnych
Wirtualne Serwery administracyjne
Informacje o ograniczeniach Kaspersky Security Center
Obciążenie sieci
Wstępna zdalna instalacja ochrony antywirusowej
Wstępna aktualizacja baz danych programu antywirusowego
Synchronizowanie klienta z Serwerem administracyjnym
Dodatkowa aktualizacja baz danych programu antywirusowego
Przetwarzanie zdarzeń występujących na klientach przez Serwer administracyjny
Ruch na 24 godziny
Przygotowywanie do zarządzania urządzeniami mobilnymi
Serwer iOS MDM
Standardowa konfiguracja: Kaspersky Device Management for iOS w strefie DMZ
Standardowa konfiguracja: Serwer iOS MDM w sieci lokalnej organizacji
Zarządzanie urządzeniami mobilnymi z zainstalowanym programem Kaspersky Endpoint Security for Android
Informacje o wydajności Serwera administracyjnego
Ograniczenia połączenia z Serwerem administracyjnym
Rezultaty testów wydajnościowych Serwera administracyjnego
Wyniki sprawdzania działania serwera KSN proxy
Ustawienia sieciowe dotyczące interakcji z usługami zewnętrznymi
Instalowanie Agenta sieciowego i aplikacji zabezpieczającej
Wstępne wdrożenie
Konfigurowanie instalatorów
Pakiety instalacyjne
Właściwości MSI i pliki transformacji
Zdalna instalacja przy użyciu narzędzi firm trzecich
Informacje o zadaniach zdalnej instalacji w Kaspersky Security Center
Wdrażanie poprzez przechwycenie i skopiowanie obrazu urządzenia
Niepoprawne kopiowanie obrazu dysku twardego
Zdalna instalacja przy użyciu zasad grupy Microsoft Windows
Wymuszone wdrożenie przy użyciu zadania zdalnej instalacji z Kaspersky Security Center
Uruchamianie pakietów autonomicznych utworzonych przez Kaspersky Security Center
Opcje ręcznej instalacji aplikacji
Tworzenie pliku MST
Zdalna instalacja aplikacji na urządzeniach z zainstalowanym Agentem sieciowym
Zarządzanie ponownym uruchamianiem urządzeń w zadaniu zdalnej instalacji
Aktualizowanie baz danych w pakiecie instalacyjnym aplikacji zabezpieczającej
Korzystanie z narzędzi do zdalnej instalacji aplikacji z Kaspersky Security Center do uruchamiania odpowiednich plików wykonywalnych na zarządzanych urządzeniach

- Monitorowanie wdrożenia
- Konfigurowanie instalatorów
  - Informacje ogólne
  - Instalacja w trybie cichym (z plikiem odpowiedzi)
  - Instalacja Agenta sieciowego w trybie cichym (bez pliku odpowiedzi)
  - Częściowa konfiguracja instalacji poprzez setup.exe
  - Parametry instalacji Serwera administracyjnego
  - Parametry instalacji Agenta sieciowego
- Infrastruktura wirtualna
  - Wskazówki dotyczące zmniejszenia obciążenia na maszynach wirtualnych
  - Obsługa dynamicznych maszyn wirtualnych
  - Obsługa kopiowania maszyn wirtualnych
- Obsługa przywracania systemu plików dla urządzeń z zainstalowanym Agentem sieciowym
- Lokalna instalacja aplikacji
  - Lokalna instalacja Agenta sieciowego
  - Instalowanie Agenta sieciowego w trybie cichym
  - Instalowanie Agenta sieciowego dla systemu Linux w trybie cichym (z plikiem odpowiedzi)
  - Przygotowanie urządzenia z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania do instalacji Agenta sieciowego
  - Instalowanie Agenta sieciowego dla systemu Linux w trybie interaktywnym
  - Lokalna instalacja wtyczki zarządzającej aplikacją
  - Instalowanie aplikacji w trybie cichym
  - Instalowanie aplikacji przy pomocy pakietów autonomicznych
  - Ustawienia pakietu instalacyjnego Agenta sieciowego
  - Przeglądanie Polityki prywatności
- Wdrażanie systemów zarządzania urządzeniami mobilnymi
  - Wdrażanie systemu zarządzania poprzez protokół iOS MDM
    - Instalowanie serwera iOS MDM
    - Instalowanie serwera iOS MDM w trybie cichym
    - Scenariusze instalowania serwera iOS MDM
    - Uproszczony schemat instalacji
    - Schemat zdalnej instalacji z użyciem delegowania protokołu Kerberos (KCD)
    - Pobieranie certyfikatu APNs
    - Odnawianie certyfikatu APNs
    - Konfigurowanie zapasowego certyfikatu serwera iOS MDM
    - Instalowanie certyfikatu APNs na serwerze iOS MDM
    - Konfigurowanie dostępu do usługi Apple Push Notification
    - Publikowanie i instalowanie certyfikatu współdzielonego na urządzeniu mobilnym
  - Dodawanie urządzeń KES do listy zarządzanych urządzeń
  - Połączenie urządzeń KES z Serwerem administracyjnym
    - Bezpośrednie połączenie urządzeń z Serwerem administracyjnym
    - Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD)
    - Korzystanie z Firebase Cloud Messaging
  - Integracja z infrastrukturą kluczy publicznych
  - Kaspersky Security Center Web Server

Instalacja Kaspersky Security Center
- Przygotowanie do instalacji
- Konta do pracy z DBMS
  - Konfigurowanie kont do pracy z SQL Server (uwierzytelnianie Windows)
  - Konfigurowanie kont do pracy z SQL Server (uwierzytelnianie SQL Server)
  - Konfiguracja kont do pracy z MySQL i MariaDB
  - Przenoszenie danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela w systemach DBMS MySQL lub MariaDB
  - Konfiguracja kont do pracy z PostgreSQL i Postgres Pro
- Scenariusz: Autoryzacja Microsoft SQL Server
- Scenariusz: uwierzytelnianie serwera MySQL
- Scenariusz: uwierzytelnianie serwera PostgreSQL
- Zalecenia dotyczące instalacji Serwera administracyjnego
  - Tworzenie kont dla usług Serwera administracyjnego na klastrze typu failover
  - Określanie folderu współdzielonego
  - Zdalna instalacja przy użyciu narzędzi Serwera administracyjnego poprzez zasady grupy Active Directory
  - Zdalna instalacja poprzez dostarczenie ścieżki UNC do pakietu autonomicznego
  - Aktualizowanie z folderu współdzielonego Serwera administracyjnego
  - Instalowanie obrazów systemów operacyjnych
  - Określanie adresu Serwera administracyjnego
- Instalacja standardowa
  - Krok 1. Przeglądanie treści Umowy licencyjnej i Polityki prywatności
  - Krok 2. Wybieranie metody instalacji
  - Krok 3. Instalowanie Kaspersky Security Center Web Console
  - Krok 4. Wybieranie rozmiaru sieci
  - Krok 5. Wybieranie bazy danych
  - Krok 6. Konfigurowanie serwera SQL
  - Krok 7. Wybieranie trybu uwierzytelniania
  - Krok 8. Wypakowywanie i instalowanie plików na dysku twardym
- Instalacja niestandardowa
  - Krok 1. Przeglądanie treści Umowy licencyjnej i Polityki prywatności
  - Krok 2. Wybieranie metody instalacji
  - Krok 3. Wybieranie składników do zainstalowania
  - Krok 4. Instalowanie Kaspersky Security Center Web Console
  - Krok 5. Wybieranie rozmiaru sieci
  - Krok 6. Wybieranie bazy danych
  - Krok 7. Konfigurowanie serwera SQL
  - Krok 8. Wybieranie trybu uwierzytelniania
  - Krok 9. Wybieranie konta do uruchamiania Serwera administracyjnego
  - Krok 10. Wybieranie konta do uruchamiania usług Kaspersky Security Center
  - Krok 11. Wybieranie folderu współdzielonego
  - Krok 12. Konfigurowanie połączenia z Serwerem administracyjnym
  - Krok 13. Określanie adresu Serwera administracyjnego
  - Krok 14. Adres Serwera administracyjnego dla podłączenia urządzeń mobilnych
  - Krok 15. Wybieranie wtyczek do zarządzania aplikacjami
  - Krok 16. Wypakowywanie i instalowanie plików na dysku twardym

Wdrażanie klastra trybu failover Kaspersky Security Center
Scenariusz: Wdrażanie klastra trybu failover Kaspersky Security Center
Informacje o klastrze trybu failover Kaspersky Security Center
Przygotowywanie serwera plików dla klastra trybu failover Kaspersky Security Center
Przygotowywanie węzłów dla klastra trybu failover Kaspersky Security Center
Instalowanie Kaspersky Security Center na węzłach klastra trybu failover Kaspersky Security Center
Ręczne uruchamianie i zatrzymywanie węzłów klastra
Instalowanie Serwera administracyjnego na klastrze trybu failover Windows Server
Krok 1. Przeglądanie treści Umowy licencyjnej i Polityki prywatności
Krok 2. Wybieranie typu instalacji na klastrze
Krok 3. Określanie nazwy wirtualnego Serwera administracyjnego
Krok 4. Określanie szczegółów sieci wirtualnego Serwera administracyjnego
Krok 5. Określanie grupy klastrów
Krok 6. Wybieranie magazynu danych klastra
Krok 7. Określanie konta do zdalnej instalacji
Krok 8. Wybieranie składników do zainstalowania
Krok 9. Wybieranie rozmiaru sieci
Krok 10. Wybieranie bazy danych
Krok 11. Konfigurowanie serwera SQL
Krok 12. Wybieranie trybu uwierzytelniania
Krok 13. Wybieranie konta do uruchamiania Serwera administracyjnego
Krok 14. Wybieranie konta do uruchamiania usług Kaspersky Security Center
Krok 15. Wybieranie folderu współdzielonego
Krok 16. Konfigurowanie połączenia z Serwerem administracyjnym
Krok 17. Określanie adresu Serwera administracyjnego
Krok 18. Adres Serwera administracyjnego dla podłączenia urządzeń mobilnych
Krok 19. Wypakowywanie i instalowanie plików na dysku twardym
Instalowanie Serwera administracyjnego w trybie cichym
Instalowanie Konsoli administracyjnej na stacji roboczej administratora
Zmiany w systemie po instalacji Kaspersky Security Center
Dezinstalowanie aplikacji
Informacje o aktualizacji Kaspersky Security Center
Aktualizowanie Kaspersky Security Center z poprzedniej wersji
Aktualizowanie Kaspersky Security Center na węzłach klastra trybu failover Kaspersky Security Center
Aktualizowanie Kaspersky Security Center na węzłach klastra trybu failover Microsoft
Wstępna konfiguracja Kaspersky Security Center
Przewodnik po zwiększaniu odporności
Kreator wstępnej konfiguracji Serwera administracyjnego
Informacje o kreatorze wstępnej konfiguracji
Uruchamianie kreatora wstępnej konfiguracji Serwera administracyjnego
Krok 1. Konfigurowanie serwera proxy
Krok 2. Wybieranie metody aktywacji aplikacji
Krok 3. Wybór obszarów ochrony i systemów operacyjnych
Krok 4. Wybieranie wtyczek dla zarządzanych aplikacji
Krok 5. Pobieranie pakietów dystrybucyjnych i tworzenie pakietów instalacyjnych
Krok 6. Konfigurowanie użycia Kaspersky Security Network
Krok 7. Konfigurowanie powiadomień e-mail

Krok 8. Konfigurowanie zarządzania aktualizacją
Krok 9. Wstępne konfigurowanie ochrony
Krok 10. Podłączanie urządzeń mobilnych
Krok 11. Pobieranie aktualizacji
Krok 12. Wykrywanie urządzeń
Krok 13. Zamykanie kreatora wstępnej konfiguracji
Konfigurowanie połączenia Konsoli administracyjnej z Serwerem administracyjnym
Konfigurowanie ustawień dostępu do Internetu dla Serwera administracyjnego
Podłączanie urządzeń mobilnych
Scenariusz: Podłączanie urządzeń mobilnych przez bramę połączenia
Scenariusz: Połączanie urządzeń spoza biura poprzez podrzędny Serwer administracyjny w strefie DMZ
Informacje o podłączaniu urządzeń mobilnych
Podłączanie zewnętrznych urządzeń stacjonarnych do Serwera administracyjnego
Informacje o profilach połączenia dla użytkowników mobilnych
Tworzenie profilu połączenia dla użytkowników mobilnych
Informacje o przełączaniu Agenta sieciowego na inne Serwery administracyjne
Tworzenie reguły przełączania Agenta sieciowego według lokalizacji sieciowej
Powiadomienia o zdarzeniach
Konfigurowanie powiadomień o zdarzeniach
Sprawdzanie opcji wysyłania powiadomień
Wyświetlanie powiadomień o zdarzeniach po uruchomieniu pliku wykonywalnego
Szyfrowanie komunikacji z TLS
Konfigurowanie interfejsu
Wykrywanie urządzeń w sieci
Scenariusz: Wykrywanie urządzeń w sieci
Urządzenia nieprzypisane
Wykrywanie urządzeń
Przeszukiwanie sieci Windows
Przeszukiwanie Active Directory
Przeszukiwanie zakresu IP
Przeszukiwanie Zeroconf
Praca z domenami Windows. Przeglądanie i modyfikowanie ustawień domeny
Konfigurowanie reguły zatrzymania dla urządzeń nieprzypisanych
Praca z zakresami IP
Tworzenie zakresu IP
Przeglądanie i modyfikowanie ustawień zakresu IP
Praca z grupami Active Directory. Przeglądanie i modyfikowanie ustawień grupy
Tworzenie reguł automatycznego przenoszenia urządzeń do grup administracyjnych
Używanie dynamicznego trybu VDI na urządzeniach klienckich
Włączanie dynamicznego trybu VDI we właściwościach pakietu instalacyjnego Agenta sieciowego
Wyszukiwanie urządzeń będących częścią VDI
Przenoszenie urządzeń z VDI do grupy administracyjnej
Inwentaryzacja sprzętu
Dodawanie informacji o nowych urządzeniach
Konfigurowanie kryteriów wykorzystywanych do określania urządzeń firmowych
Konfiguracja pól niestandardowych

Licencjonowanie
Zdarzenia przekroczenia limitu licencji
Informacje o licencjonowaniu
Informacje o licencji
Informacje o Umowie licencyjnej użytkownika końcowego
Informacje o certyfikacie licencji
Informacje o kluczu licencyjnym
Informacje o pliku klucza
Informacje o subskrypcji
Informacje o kodzie aktywacyjnym
Wycofanie zgody z Umową Licencyjną Użytkownika Końcowego
Informacje o przekazywaniu danych
Opcje licencjonowania Kaspersky Security Center
Funkcje licencjonowania Kaspersky Security Center i zarządzanych aplikacji
Aplikacje Kaspersky. Scentralizowane wdrażanie
Zastępowanie aplikacji zabezpieczających firm trzecich
Instalowanie aplikacji przy pomocy zadania zdalnej instalacji
Instalowanie aplikacji na wybranych urządzeniach
Instalowanie aplikacji na urządzeniach klienckich z grupy administracyjnej
Instalowanie aplikacji przy użyciu zasad grupy Active Directory
Instalacja zdalna aplikacji na urządzeniach z systemem macOS
Instalowanie aplikacji na podrzędnych Serwerach administracyjnych
Instalowanie aplikacji przy pomocy kreatora zdalnej instalacji
Praca z wtyczkami zarządzającymi
Wyświetlanie raportu wdrażania ochrony
Zdalne usuwanie aplikacji
Zdalne usuwanie aplikacji z urządzeń klienckich w grupie administracyjnej
Zdalne usuwanie aplikacji z wybranych urządzeń
Praca z pakietami instalacyjnymi
Tworzenie pakietu instalacyjnego
Tworzenie autonomicznych pakietów instalacyjnych
Tworzenie niestandardowego pakietu instalacyjnego
Przeglądanie i edytowanie właściwości niestandardowych pakietów instalacyjnych
Uzyskiwanie pakietu instalacyjnego Agenta sieciowego z pakietu dystrybucyjnego Kaspersky Security Center
Rozsyłanie pakietów instalacyjnych na podrzędne Serwery administracyjne
Rozsyłanie pakietów instalacyjnych poprzez punkty dystrybucji
Przesyłanie rezultatów instalacji aplikacji do Kaspersky Security Center
Definiowanie adresu serwera proxy KSN pod kątem pakietów instalacyjnych
Pobieranie aktualnych wersji aplikacji
Przygotowanie urządzenia z systemem Windows do zdalnej instalacji
Przygotowanie urządzenia z systemem Linux i zdalna instalacja Agenta sieciowego na urządzeniu z systemem Linux
Przygotowanie urządzenia z systemem SUSE Linux Enterprise Server 15 do instalacji Agenta sieciowego
Przygotowanie urządzenia macOS do zdalnej instalacji Agenta sieciowego
Aplikacje Kaspersky: licencjonowanie i aktywacja
Licencjonowanie zarządzanych aplikacji
Wyświetlanie informacji o używanych kluczach licencyjnych
Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego

- Usuwanie klucza licencyjnego Serwera administracyjnego
- Rozsyłanie klucza licencyjnego na urządzenia klienckie
- Automatyczne rozsyłanie kluczy licencyjnych
- Tworzenie i przeglądanie raportu użycia klucza licencyjnego
- Przeglądanie informacji o kluczach licencyjnych aplikacji
- Eksportowanie pliku klucza licencyjnego

Konfigurowanie ochrony sieci

- Scenariusz: Konfigurowanie ochrony sieci
- Konfiguracja i przydzielanie zasad: Metoda skoncentrowana na urządzeniu
- Informacje o metodach zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku
- Ręczna konfiguracja zasady Kaspersky Endpoint Security
  - Konfigurowanie zasady w sekcji Zaawansowana ochrona przed zagrożeniami
  - Konfigurowanie zasady w sekcji Podstawowa ochrona przed zagrożeniami
  - Konfigurowanie zasady w sekcji Ustawienia ogólne
  - Konfigurowanie zasad w sekcji Konfiguracja zdarzenia
- Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security
- Ręczna konfiguracja grupowego zadania skanowania urządzeń z zainstalowanym programem Kaspersky Endpoint Security
- Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
- Ręczna konfiguracja grupowego zadania instalacji uaktualnień i naprawy luk
- Określanie maksymalnej liczby zdarzeń w repozytorium zdarzeń
- Określenie maksymalnego okresu przechowywania informacji o wyeliminowanych lukach
- Zarządzanie zadaniami
  - Tworzenie zadania
  - Tworzenie zadania Serwera administracyjnego
  - Tworzenie zadania dla określonych urządzeń
  - Tworzenie zadania lokalnego
  - Wyświetlanie dziedziczonego zadania grupowego w obszarze roboczym grupy zagnieżdżonej
  - Automatyczne włączanie urządzeń przed uruchomieniem zadania
  - Automatyczne wyłączanie urządzenia po zakończeniu zadania
  - Ograniczanie czasu uruchamiania zadania
  - Eksportowanie zadania
  - Importowanie zadania
  - Konwertowanie zadań
  - Ręczne uruchamianie i zatrzymywanie zadania
  - Ręczne wstrzymywanie i wznawianie zadania
  - Monitorowanie wykonywania zadania
  - Przeglądanie wyników wykonywania zadań przechowywanych na Serwerze administracyjnym
  - Konfigurowanie filtrowania informacji o wynikach wykonywania zadań
  - Modyfikowanie zadania. Wycofywanie zmian
  - Porównywanie zadań
  - Konta do uruchamiania zadań
  - Eksportowanie historii wykonania zadania
  - Kreator zmiany haseł w zadaniach
    - Krok 1. Określanie danych uwierzytelniających
    - Krok 2. Wybieranie działania, jakie ma zostać podjęte
    - Krok 3. Sprawdzanie wyników
- Tworzenie hierarchii grup administracyjnych podległych wirtualnemu Serwerowi administracyjnemu

Zasady i profile zasad
Hierarchia zasad i korzystanie z zasad
Hierarchia zasad
Profile zasad
Dziedziczenie ustawień zasady
Zarządzanie zasadami
Tworzenie zasady
Wyświetlanie zasady dziedziczonej w podgrupie
Aktywowanie zasady
Aktywowanie zasady automatycznie po wystąpieniu zdarzenia Ataku wirusa
Stosowanie zasady użytkownika mobilnego
Modyfikowanie zasady. Wycofywanie zmian
Porównywanie zasad
Przeglądanie wykresu stanu dystrybucji zasad
Usuwanie zasady
Kopiowanie zasady
Eksportowanie zasady
Importowanie zasady
Konwertowanie zasad
Zarządzanie profilami zasad
Tworzenie profilu zasad
Modyfikowanie profilu zasad
Usuwanie profilu zasad
Tworzenie reguły aktywacji profilu zasad
Reguły przenoszenia urządzeń
Klonowanie reguł przenoszenia urządzeń
Kategoryzacja oprogramowania
Wymagania wstępne do zainstalowania aplikacji na urządzeniach w organizacji klienta
Przeglądanie i modyfikowanie lokalnych ustawień aplikacji
Aktualizowanie Kaspersky Security Center i zarządzanych aplikacji
Scenariusz: Regularne aktualizowanie baz danych i aplikacji Kaspersky
Informacje o aktualizowaniu baz danych, modułów i aplikacji Kaspersky
Informacje o używaniu plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky
Włączanie funkcji Pobierz pliki diff
Tworzenie zadania pobierania aktualizacji do repozytorium Serwera administracyjnego
Tworzenie zadania Pobierz uaktualnienia do repozytoriów punktów dystrybucji
Konfigurowanie zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego
Sprawdzanie pobranych uaktualnień
Konfigurowanie zasad testowych i zadań pomocniczych
Wyświetlanie pobranych uaktualnień
Automatyczna instalacja uaktualnień dla Kaspersky Endpoint Security na urządzeniach
Tryb offline pobierania aktualizacji
Włączanie i wyłączanie trybu offline pobierania uaktualnień
Automatyczne aktualizowanie i instalowanie poprawek dla komponentów Kaspersky Security Center
Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center

Automatyczne rozsyłanie uaktualnień
Automatyczne rozsyłanie uaktualnień do urządzeń klienckich
Automatyczne rozsyłanie uaktualnień do podrzędnych Serwerów administracyjnych
Automatyczne przypisywanie punktów dystrybucji
Ręczne wskazywanie urządzenia jako punktu dystrybucji
Usuwanie urządzenia z listy punktów dystrybucji
Pobieranie uaktualnień przez punkty dystrybucji
Usuwanie aktualizacji oprogramowania z repozytorium
Instalacja poprawki dla aplikacji Kaspersky w trybie klastra
Zarządzanie aplikacjami firm trzecich na urządzeniach klienckich
Informacje o aplikacjach innych firm
Instalowanie aktualizacji oprogramowania firm trzecich
Scenariusz: Aktualizowanie oprogramowania innej firmy
Przeglądanie informacji o dostępnych aktualizacjach aplikacji innych firm
Zatwierdzanie i odrzucanie aktualizacji oprogramowania
Synchronizacja aktualizacji z Windows Update z Serwerem administracyjnym
Krok 1. Określanie, czy zmniejszyć ruch sieciowy
Krok 2. Aplikacje
Krok 3. Kategorie uaktualnień
Krok 4. Języki aktualizacji
Krok 5. Wybieranie konta do uruchamiania zadania
Krok 6. Konfigurowanie terminarza uruchamiania zadania
Krok 7. Definiowanie nazwy zadania
Krok 8. Kończenie tworzenia zadania
Ręczne instalowanie uaktualnień na urządzeniach
Konfigurowanie aktualizacji systemu Windows w zasadzie Agenta sieciowego
Eliminowanie luk w oprogramowaniu innych firm
Scenariusz: Wyszukiwanie i usuwanie luk w oprogramowaniu firm trzecich
Informacje o wyszukiwaniu i eliminowaniu luk w oprogramowaniu
Przeglądanie informacji o lukach w oprogramowaniu
Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach
Skanowanie aplikacji w poszukiwaniu luk
Naprawianie luk w aplikacjach
Naprawianie luk w odizolowanej sieci
Scenariusz: Eliminowanie luk w oprogramowaniu innych firm w odizolowanej sieci
Eliminowanie luk w oprogramowaniu innych firm w odizolowanej sieci
Konfigurowanie serwera administracyjnego z dostępem do internetu w celu usunięcia luk w odizolowanej sieci
Konfigurowanie izolowanych Serwerów administracyjnych w celu usunięcia luk w odizolowanej sieci
Przesyłanie poprawek i instalowanie aktualizacji w odizolowanej sieci
Wyłączanie możliwości przesyłania poprawek i instalowania aktualizacji w odizolowanej sieci
Ignorowanie luk w oprogramowaniu
Wybieranie poprawek użytkownika dla luk w programach innych firm
Reguły instalacji aktualizacji
Grupy aplikacji
Korzystanie z Kontroli aplikacji do zarządzania plikami wykonywalnymi
Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich
Tworzenie kategorii aplikacji dla zasad Kaspersky Endpoint Security for Windows

Tworzenie kategorii aplikacji z zawartością dodaną ręcznie
Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń
Tworzenie kategorii aplikacji zawierającej pliki wykonywalne z określonego folderu
Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji
Konfigurowanie zarządzania uruchamianiem aplikacji na urządzeniach klienckich
Wyświetlanie wyników analizy statycznej reguł uruchamiania zastosowanych na plikach wykonywalnych
Przeglądanie rejestru aplikacji
Zmienianie czasu uruchomienia inwentaryzacji oprogramowania
Informacje o zarządzaniu kluczem licencyjnym dla aplikacji innych firm
Tworzenie grup licencjonowanych aplikacji
Zarządzanie kluczami licencyjnymi dla grup licencjonowanych aplikacji
Inwentaryzacja plików wykonywalnych
Przeglądanie informacji o plikach wykonywalnych
Monitorowanie i raportowanie
Scenariusz: Monitorowanie i raportowanie
Monitorowanie koloru wskaźnika i rejestrowanych zdarzeń w Konsoli administracyjnej
Praca z raportami, statystykami i powiadomieniami
Praca z raportami
Tworzenie szablonu raportu
Przeglądanie i edytowanie właściwości szablonu raportu
Rozszerzony format filtra w szablonach raportu
Konwertowanie filtra do rozszerzonego formatu
Konfigurowanie rozszerzonego filtra
Tworzenie i przeglądanie raportu
Zapisywanie raportu
Tworzenie zadania dostarczania raportu
Krok 1. Wybieranie typu zadania
Krok 2. Wybieranie typu raportu
Krok 3. Działania podejmowane na raporcie
Krok 4. Wybieranie konta do uruchamiania zadania
Krok 5. Konfigurowanie terminarza zadania
Krok 6. Definiowanie nazwy zadania
Krok 7. Kończenie tworzenia zadania
Zarządzanie statystykami
Konfigurowanie powiadomień o zdarzeniach
Tworzenie certyfikatu dla serwera SMTP
Wybory zdarzeń
Przeglądanie wyboru zdarzeń
Dostosowywanie wyboru zdarzeń
Tworzenie kryterium wyboru zdarzenia
Eksportowanie wyboru zdarzeń do pliku tekstowego
Usuwanie zdarzeń z wyboru
Dodawanie aplikacji do wykluczeń na żądanie użytkownika
Wybory urządzeń
Wyświetlanie wyboru urządzeń
Konfigurowanie kryteriów wyboru urządzeń
Eksportowanie ustawień wyboru urządzeń do pliku

Tworzenie kryteriów wyboru urządzeń
Tworzenie wyboru urządzeń zgodnie z zaimportowanymi ustawieniami
Usuwanie urządzeń z grup administracyjnych w wyborze
Monitorowanie instalacji i dezinstalacji aplikacji
Zdarzenia składników Kaspersky Security Center
Struktura danych opisu typu zdarzeń
Zdarzenia Serwera administracyjnego
Zdarzenia krytyczne Serwera administracyjnego
Zdarzenia błędu funkcjonalnego Serwera administracyjnego
Zdarzenia ostrzegające Serwera administracyjnego
Zdarzenia informacyjne Serwera administracyjnego
Zdarzenia Agenta sieciowego
Zdarzenia błędu funkcjonalnego Agenta sieciowego
Zdarzenia ostrzegające Agenta sieciowego
Zdarzenia informacyjne Agenta sieciowego
Zdarzenia serwera iOS MDM
Zdarzenia błędu funkcjonalnego serwera iOS MDM
Zdarzenia ostrzegające serwera iOS MDM
Zdarzenia informacyjne serwera iOS MDM
Blokowanie często występujących zdarzeń
Informacje o blokowaniu często występujących zdarzeń
Zarządzanie blokowaniem często występujących zdarzeń
Usuwanie blokowania często występujących zdarzeń
Eksportowanie listy często występujących zdarzeń do pliku
Kontrolowanie zmian w stanie maszyn wirtualnych
Monitorowanie stanu ochrony antywirusowej przy użyciu informacji z rejestru systemu
Przeglądanie i konfigurowanie działań, gdy urządzenia wykazują brak aktywności
Wyłączanie ogłoszeń Kaspersky
Dostosowanie punktów dystrybucji i bram połączenia
Standardowa konfiguracja punktów dystrybucji: Jedno biuro
Standardowa konfiguracja punktów dystrybucji: Małe zdalne biura
Wskazywanie zarządzanego urządzenia jako punktu dystrybucji
Podłączanie urządzenia Linux jako bramy połączenia w strefie zdemilitaryzowanej
Podłączanie urządzenia Linux do Serwera administracyjnego za pośrednictwem bramy połączenia
Dodawanie bramy połączenia w strefie DMZ jako punktu dystrybucji
Automatyczne przypisywanie punktów dystrybucji
Informacje o lokalnej instalacji Agenta sieciowego na urządzeniu określonym jako punkt dystrybucji
Informacje o używaniu punktu dystrybucji jako bramy połączenia
Dodawanie zakresów adresów IP do listy zakresów przeszukiwanych przez punkt dystrybucji
Używanie punktu dystrybucji jako serwera push
Inne podstawowe prace
Zarządzanie Serwerami administracyjnymi
Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego Serwera administracyjnego
Nawiązywanie połączenia z Serwerem administracyjnym i przełączanie pomiędzy Serwerami administracyjnymi
Uprawnienia dostępu do Serwera administracyjnego i jego obiektów
Warunki połączenia z Serwerem administracyjnym przez internet

Nawiązywanie szyfrowanego połączenia z Serwerem administracyjnym
Autoryzacja Serwera administracyjnego po podłączeniu urządzenia
Autoryzacja Serwera administracyjnego podczas podłączania Konsoli administracyjnej
Konfigurowanie listy dozwolonych adresów IP do łączenia się z Serwerem administracyjnym
Użycie narzędzia klscflag do zamknięcia portu 13291
Odłączanie od Serwera administracyjnego
Dodawanie Serwera administracyjnego do drzewa konsoli
Usuwanie Serwera administracyjnego z drzewa konsoli
Dodawanie wirtualnego Serwera administracyjnego do drzewa konsoli
Zmienianie konta usługi Serwera administracyjnego. Narzędzie klsrvswch
Zmiana poświadczeń DBMS
Zmiana folderu współdzielonego Serwera administracyjnego
Rozwiązywanie problemów z węzłami Serwera administracyjnego
Przeglądanie i modyfikowanie ustawień Serwera administracyjnego
Dostosowywanie ogólnych ustawień Serwera administracyjnego
Ustawienia interfejsu Konsoli administracyjnej
Przetwarzanie i przechowywanie zdarzeń na Serwerze administracyjnym
Przeglądanie raportów połączeń z Serwerem administracyjnym
Kontrola epidemii wirusów
Ograniczanie ruchu sieciowego
Konfigurowanie serwera sieciowego
Praca z użytkownikami wewnętrznymi
Tworzenie kopii zapasowej i przywracanie ustawień Serwera administracyjnego
Używanie migawek systemu plików do skrócenia czasu tworzenia kopii zapasowej
Urządzenie z zainstalowanym Serwerem administracyjnym nie działa
Ustawienia Serwera administracyjnego lub bazy danych są uszkodzone
Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego
Zadanie Utwórz kopię zapasową danych Serwera administracyjnego
Narzędzie do tworzenia kopii zapasowej i odzyskiwania danych (klbackup)
Tworzenie kopii zapasowej i przywracanie danych w trybie interaktywnym
Tworzenie kopii zapasowej i przywracanie danych w trybie cichym
Korzystanie z narzędzia klbackup w celu przełączania zarządzanych urządzeń pod zarządzanie innego Serwera administracyjnego
Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego podczas korzystania z MySQL lub MariaDB
Optymalizacja tworzenia kopii zapasowej i przywracanie danych Serwera administracyjnego
Przenoszenie Serwera administracyjnego na inne urządzenie
Unikanie konfliktów między kilkoma Serwerami administracyjnymi
Zarządzanie grupami administracyjnymi
Tworzenie grup administracyjnych
Przenoszenie grup administracyjnych
Usuwanie grup administracyjnych
Automatyczne tworzenie struktury grup administracyjnych
Automatyczna instalacja aplikacji na urządzeniach w grupie administracyjnej
Zarządzanie urządzeniami klienckimi
Łączenie urządzenia klienckiego z Serwerem administracyjnym
Ręczne łączenie urządzenia klienckiego z Serwerem administracyjnym. Narzędzie klmover

Tunelowanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym
Zdalne połączenie z pulpitem urządzenia klienckiego
Łączenie z urządzeniami klienckimi Windows
Łączenie z urządzeniami klienckimi macOS
Nawiązywanie połączenia z urządzeniami poprzez udostępnianie pulpitu Windows
Konfigurowanie ponownego uruchamiania urządzenia klienckiego
Audyt działań na zdalnym urządzeniu klienckim
Sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym
Automatyczne sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym
Ręczne sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym. Narzędzie klnagchk
Informacje o sprawdzaniu czasu połączenia pomiędzy urządzeniem a Serwerem administracyjnym
Identyfikowanie urządzeń klienckich na Serwerze administracyjnym
Przenoszenie urządzeń do grupy administracyjnej
Zmienianie Serwera administracyjnego dla urządzeń klienckich
Przenoszenie urządzeń podłączonych do Serwera administracyjnego przez bramy połączeń na inny Serwer administracyjny
Klastry i grupy serwerów
Zdalne włączanie, wyłączanie i ponowne uruchamianie urządzeń klienckich
Informacje o korzystaniu z ciągłego połączenia pomiędzy zarządzanym urządzeniem a Serwerem administracyjnym
Informacje o wymuszonej synchronizacji
Informacje o terminarzu połączenia
Wysyłanie wiadomości na urządzenia użytkowników
Zarządzanie Kaspersky Security for Virtualization
Konfigurowanie przełączania stanów urządzeń
Znakowanie urządzeń i przeglądanie przydzielonych znaczników
Automatyczne znakowanie urządzeń
Przeglądanie i konfigurowanie znaczników przydzielonych do urządzenia
Zdalna diagnostyka urządzeń klienckich. Narzędzie do zdalnej diagnostyki Kaspersky Security Center
Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim
Generowania pliku zrzutu dla aplikacji
Włączanie i wyłączanie śledzenia, pobieranie pliku śledzenia
Pobierania ustawień aplikacji
Pobierania dzienników zdarzeń
Pobieranie kilku elementów informacji diagnostycznych
Uruchamianie diagnostyki i pobieranie wyników
Uruchamianie, zatrzymywanie i ponowne uruchamianie aplikacji
Urządzenia chronione UEFI
Ustawienia zarządzanego urządzenia
Ogólne ustawienia zasady
Ustawienia zasady Agenta sieciowego
Zarządzanie kontami użytkowników
Praca z kontami użytkowników
Dodawanie konta użytkownika wewnętrznego
Edytowanie konta użytkownika wewnętrznego
Zmienianie liczby dozwolonych prób wprowadzenia hasła
Konfigurowanie sprawdzania unikatowości nazwy użytkownika wewnętrznego
Dodawanie grupy bezpieczeństwa

- Dodawanie użytkownika do grupy
- Konfigurowanie praw dostępu do funkcji aplikacji. Kontrola dostępu oparta o rolę
  - Prawa dostępu do funkcji aplikacji
  - Informacje o rolach użytkowników
  - Dodawanie roli użytkownika
  - Przypisywanie roli do użytkownika lub grupy bezpieczeństwa
  - Przydzielanie uprawnień użytkownikom i grupom
  - Przydzielanie ról użytkownika do podrzędnych Serwerów administracyjnych
- Wskazywanie użytkownika jako właściciela urządzenia
- Dostarczanie wiadomości użytkownikom
- Przeglądanie listy urządzeń mobilnych użytkownika
- Instalowanie certyfikatu dla użytkownika
- Wyświetlanie listy certyfikatów wydanych dla użytkownika
- Informacje o administratorze wirtualnego Serwera administracyjnego

Zdalna instalacja systemów operacyjnych i aplikacji
- Tworzenie obrazów systemów operacyjnych
- Instalowanie obrazów systemów operacyjnych
- Konfigurowanie adresu serwera proxy KSN
- Dodawanie sterowników dla Windows Preinstallation Environment (WinPE)
- Dodawanie sterowników do pakietu instalacyjnego z obrazem systemu operacyjnego
- Konfigurowanie narzędzia sysprep.exe
- Instalowanie systemów operacyjnych na urządzeniach w sieci
- Instalowanie systemów operacyjnych na urządzeniach klienckich
- Tworzenie pakietów instalacyjnych aplikacji
- Tworzenie certyfikatu dla pakietów instalacyjnych aplikacji
- Instalowanie aplikacji na urządzeniach klienckich

Zarządzanie rewizjami obiektów
- Informacje o rewizjach obiektów
- Przeglądanie sekcji Historia rewizji
- Porównywanie rewizji obiektu
- Określanie czasu przechowywania rewizji obiektu oraz informacji o usuniętym obiekcie
- Przeglądanie rewizji obiektu
- Zapisywanie rewizji obiektu do pliku
- Wycofywanie zmian
- Dodawanie opisu rewizji

Usuwanie obiektów
- Usuwanie obiektu
- Przeglądanie informacji o usuniętych obiektach
- Trwałe usuwanie obiektów z listy usuniętych obiektów

Zarządzanie urządzeniami mobilnymi
- Scenariusz: Wdrażanie Zarządzania urządzeniami mobilnymi
- Informacje o zasadzie grupy do zarządzania urządzeniami iOS MDM
- Włączanie Zarządzania urządzeniami mobilnymi
- Modyfikowanie ustawień Zarządzania urządzeniami mobilnymi
- Wyłączanie Zarządzania urządzeniami mobilnymi

Praca z poleceniami dla urządzeń mobilnych
Polecenia zarządzania urządzeniem mobilnym
Korzystanie z Firebase Cloud Messaging
Wysyłanie poleceń
Przeglądanie stanów poleceń w raporcie poleceń
Praca z certyfikatami urządzeń mobilnych
Uruchamianie kreatora instalacji certyfikatu
Krok 1. Wybieranie typu certyfikatu
Krok 2. Wybieranie typu urządzenia
Krok 3. Wybieranie użytkownika
Krok 4. Wybieranie źródła certyfikatu
Krok 5. Przypisywanie znacznika do certyfikatu
Krok 6. Określanie ustawień publikowania certyfikatu
Krok 7. Wybieranie metody powiadamiania użytkownika
Krok 8. Generowanie certyfikatu
Konfigurowanie reguł wydawania certyfikatów
Integracja z infrastrukturą kluczy publicznych
Włączanie obsługi Kerberos Constrained Delegation
Dodawanie urządzeń mobilnych iOS do listy zarządzanych urządzeń
Dodawanie urządzeń mobilnych Android do listy zarządzanych urządzeń
Zarządzanie urządzeniami iOS MDM
Podpisywanie profilu iOS MDM za pomocą certyfikatu
Dodawanie profilu konfiguracyjnego
Instalowanie profilu konfiguracyjnego na urządzeniu
Usuwanie profilu konfiguracyjnego z urządzenia
Dodanie nowego urządzenia poprzez opublikowanie odnośnika do profilu
Dodanie nowego urządzenia mobilnego poprzez zainstalowanie profilu przez administratora
Dodawanie profilu informacyjnego
Instalowanie profilu informacyjnego na urządzeniu
Usuwanie profilu informacyjnego z urządzenia
Dodawanie zarządzanej aplikacji
Instalowanie aplikacji na urządzeniu mobilnym
Usuwanie aplikacji z urządzenia
Konfigurowanie roamingu na urządzeniu mobilnym iOS MDM
Przeglądanie informacji o urządzeniu iOS MDM
Odłączanie urządzenia iOS MDM od funkcji zarządzania
Wysyłanie poleceń na urządzenie
Sprawdzanie stanu wykonania wysłanych poleceń
Zarządzanie urządzeniami KES
Tworzenie pakietów aplikacji mobilnych dla urządzeń KES
Włączanie uwierzytelniania opartego na certyfikatach urządzeń KES
Przeglądanie informacji o urządzeniu KES
Odłączanie urządzenia KES od funkcji zarządzania
Szyfrowanie i ochrona danych
Przeglądanie listy zaszyfrowanych urządzeń
Wyświetlanie listy zdarzeń szyfrowania
Eksportowanie listy zdarzeń szyfrowania do pliku tekstowego

Tworzenie i przeglądanie raportów z szyfrowania
Przesyłanie kluczy szyfrowania między Serwerami administracyjnymi
Repozytoria danych
Eksportowanie listy obiektów w repozytorium do pliku tekstowego
Pakiety instalacyjne
Główne stany plików w repozytorium
Wywoływanie reguł w trybie Inteligentne uczenie
Przeglądanie listy obiektów wykrytych przy użyciu reguł Adaptacyjnej kontroli anomalii
Dodawanie wykluczeń z reguł Adaptacyjnej kontroli anomalii
Krok 1. Wybieranie aplikacji
Krok 2. Wybieranie zasady (zasad)
Krok 3. Przetwarzanie zasady (zasad)
Kwarantanna i Kopia zapasowa
Włączanie zdalnego zarządzania dla plików w repozytoriach
Przeglądanie właściwości pliku umieszczonego w repozytorium
Usuwanie plików z repozytoriów
Przywracanie plików z repozytoriów
Zapisywanie plików z repozytoriów na dysku
Skanowanie plików w Kwarantannie
Aktywne zagrożenia
Leczenie nieprzetworzonego pliku
Zapisywanie nieprzetworzonego pliku na dysku
Usuwanie plików z folderu „Aktywne zagrożenia”
Kaspersky Security Network (KSN)
Informacje o KSN
Konfigurowanie dostępu do Kaspersky Security Network
Włączanie i wyłączanie KSN
Przeglądanie zaakceptowanego Oświadczenia KSN
Przeglądanie statystyk serwera proxy KSN
Akceptowanie zaktualizowanego Oświadczenia KSN
Udoskonalona ochrona przy pomocy Kaspersky Security Network
Sprawdzanie, czy punkt dystrybucji działa jako serwer proxy KSN
Przełączanie między pomocą online i pomocą offline
Eksportowanie zdarzeń do systemów SIEM
Konfigurowanie eksportowania zdarzeń do systemów SIEM
Czynności niezbędne do wykonania przed rozpoczęciem pracy
Informacje o zdarzeniach w Kaspersky Security Center
Informacje o eksportowaniu zdarzeń
Informacje o konfigurowaniu eksportowania zdarzeń w systemie SIEM
Oznaczenie zdarzeń do wyeksportowania do systemów SIEM w formacie Syslog
Oznaczanie zdarzeń aplikacji Kaspersky do eksportu w formacie Syslog
Oznaczanie ogólnych zdarzeń do eksportu w formacie Syslog
Informacje dotyczące eksportowania zdarzeń przy użyciu formatu Syslog
Informacje dotyczące eksportowania zdarzeń przy użyciu formatów CEF i LEEF
Konfigurowanie Kaspersky Security Center do wyeksportowania zdarzeń do systemu SIEM

- Eksportowanie zdarzeń bezpośrednio z bazy danych
  - Tworzenie zapytania SQL przy użyciu narzędzia klsql2
  - Przykład zapytania SQL w narzędziu klsql2
  - Sprawdzanie nazwy bazy danych Kaspersky Security Center
- Przeglądanie wyników eksportowania

Używanie protokołu SNMP do wysyłania statystyk do aplikacji firm trzecich

- Konfigurowanie usługi SNMP do użytku z Kaspersky Security Center
- Agent SNMP i identyfikatory obiektów
- Uzyskiwanie nazwy licznika ciągu znaków z identyfikatora obiektu
- Wartości identyfikatorów obiektów dla SNMP
- Rozwiązywanie problemów

Praca w środowisku chmury

- Informacje o pracy w środowisku chmury
- Scenariusz: Wdrażanie ochrony dla środowiska chmury
- Wymagania wstępne wdrożenia Kaspersky Security Center w środowisku chmury
- Wymagania sprzętowe dla Serwera administracyjnego w środowisku chmury
- Opcje licencjonowania w środowisku chmury
- Opcje bazy danych do pracy w środowisku chmury
- Praca w środowisku chmury Amazon Web Services
  - Informacje o pracy w środowisku chmury Amazon Web Services
  - Tworzenie roli IAM i kont użytkowników IAM dla instancji Amazon EC2
    - Zapewnianie, że Serwer administracyjny Kaspersky Security Center posiada uprawnienia do pracy z AWS
    - Tworzenie roli IAM dla Serwera administracyjnego
    - Tworzenie konta użytkownika IAM do pracy z Kaspersky Security Center
    - Tworzenie roli IAM dla instalacji aplikacji na instancjach Amazon EC2
  - Praca z Amazon RDS
    - Tworzenie instancji Amazon RDS
    - Tworzenie grupy opcji dla instancji Amazon RDS
    - Modyfikowanie grupy opcji
    - Modyfikowanie uprawnień dla roli IAM dla instancji bazy danych Amazon RDS
    - Przygotowanie komory Amazon S3 dla bazy danych
    - Przenoszenie bazy danych do Amazon RDS
- Praca w środowisku chmury Microsoft Azure
  - Informacje o pracy w Microsoft Azure
  - Tworzenie subskrypcji, identyfikatora aplikacji i hasła
  - Przypisywanie roli do ID aplikacji w Azure
  - Instalowanie Serwera administracyjnego w Microsoft Azure i wybieranie bazy danych
  - Praca z Azure SQL
    - Tworzenie konta magazynu Azure
    - Tworzenie bazy danych Azure SQL i serwera SQL
    - Przenoszenie bazy danych do Azure SQL
- Praca w Google Cloud
  - Tworzenie adresu e-mail klienta, identyfikatora projektu i klucza prywatnego
  - Praca z Google Cloud SQL dla instancji MySQL
- Wymagania wstępne urządzeń klienckich w środowisku chmury niezbędnych do pracy z Kaspersky Security Center
- Tworzenie pakietów instalacyjnych wymaganych do konfiguracji środowiska chmury

Konfigurowanie środowiska chmury
Informacje o Kreatorze konfiguracji środowiska chmury
Krok 1. Wybieranie metody aktywacji aplikacji
Krok 2. Wybieranie środowiska chmury
Krok 3. Autoryzacja w środowisku chmury
Krok 4. Konfigurowanie synchronizacji z chmurą i wybieranie dalszych działań
Krok 5. Konfigurowanie Kaspersky Security Network w środowisku chmury
Krok 6. Konfigurowanie powiadomień e-mail w środowisku chmury
Krok 7. Tworzenie wstępnej konfiguracji ochrony środowiska chmury
Krok 8. Wybieranie działania, jeśli system operacyjny musi być uruchomiony ponownie podczas instalacji (dla środowiska chmury)
Krok 9. Pobieranie uaktualnień przez Serwer administracyjny
Sprawdzanie konfiguracji
Grupa urządzeń w chmurze
Przeszukiwanie segmentu sieci
Dodawanie połączeń dla przeszukiwania segmentu chmury
Usuwanie połączeń dla przeszukiwania segmentu chmury
Konfigurowanie terminarza przeszukiwania
Instalowanie aplikacji na urządzeniach w środowisku chmury
Przeglądanie właściwości urządzeń w chmurze
Synchronizacja z chmurą
Wdrożenie Kaspersky Security Center w Yandex.Cloud
Dodatki
Zaawansowane funkcje
Automatyzacja działania Kaspersky Security Center. Narzędzie klakaut
Narzędzia niestandardowe
Tryb klonowania dysku Agenta sieciowego
Przygotowywanie urządzenia referencyjnego z zainstalowanym Agentem sieciowym do utworzenia obrazu systemu operacyjnego
Konfigurowanie odbierania wiadomości od komponentu Monitor integralności pliku
Konserwacja Serwera administracyjnego
Dostęp do publicznych serwerów DNS
Okno Metoda powiadamiania użytkownika
Okno Wybór urządzeń
Okno Określ nazwę nowego obiektu
Funkcje korzystania z interfejsu do zarządzania
Drzewo konsoli
Jak zaktualizować dane w obszarze roboczym
Jak poruszać się po drzewie konsoli
Jak w obszarze roboczym otworzyć okno właściwości obiektu
Jak w obszarze roboczym wybrać grupę obiektów
Jak zmienić zestaw kolumn w obszarze roboczym
Informacje dodatkowe
Polecenia menu kontekstowego
Lista zarządzanych urządzeń. Opis kolumn
Stany przypisane do urządzeń, zadań i zasad
Ikony stanów plików w Konsoli administracyjnej

- Wyszukiwanie i eksportowanie danych
  - Wyszukiwanie urządzeń
  - Ustawienia wyszukiwania urządzeń
  - Używanie masek w zmiennych typu string
  - Używanie wyrażeń regularnych w polu wyszukiwania
  - Eksportowanie list z okien dialogowych
- Ustawienia zadań
  - Ogólne ustawienia zadania
  - Ustawienia zadania pobierania aktualizacji do repozytorium serwera administracyjnego
  - Ustawienia zadania Pobierz uaktualnienia do repozytoriów punktów dystrybucji
  - Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji
  - Ustawienia zadania Zainstaluj wymagane aktualizacje i napraw luki
- Globalna lista podsieci
  - Dodawanie podsieci do globalnej listy podsieci
  - Przeglądanie i modyfikowanie właściwości podsieci z globalnej listy podsieci
- Korzystanie z Agenta sieciowego dla systemu Windows, Linux i macOS: Porównanie

Kaspersky Security Center Web Console

- Diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center i konsoli Kaspersky Security Center Web Console
- Porty używane przez Kaspersky Security Center Web Console
- Interfejs Kaspersky Security Center Web Console
- Przypinanie i odpinanie sekcji menu głównego
- Scenariusz: Instalacja i wstępna konfiguracja Kaspersky Security Center Web Console
- Instalacja
  - Instalowanie Kaspersky Security Center (Instalacja standardowa)
  - Instalowanie Kaspersky Security Center Web Console
  - Instalowanie Kaspersky Security Center Web Console połączonej z Serwerem administracyjnym zainstalowanym na węzłach klastra przełączania awaryjnego
  - Aktualizowanie Kaspersky Security Center Web Console
  - Certyfikaty do pracy z Kaspersky Security Center Web Console
    - Ponowne wystawianie certyfikatu dla Kaspersky Security Center Web Console
    - Zastępowanie certyfikatu dla Kaspersky Security Center Web Console
    - Określanie certyfikatów zaufanych Serwerów administracyjnych w Kaspersky Security Center Web Console
    - Konwersja certyfikatu PFX do formatu PEM
- Migracja z Kaspersky Security Center Windows
  - Migracja do Kaspersky Next Expert View
  - Migracja do Kaspersky Next XDR Expert
  - Migracja do Kaspersky Security Center Linux
    - Migracja do Kaspersky Security Center Linux przy użyciu kopii zapasowej danych Serwera administracyjnego
    - Migracji do Kaspersky Security Center Linux za pomocą Kreatora migracji
      - Eksportowanie obiektów grupowych z Kaspersky Security Center Windows
      - Importowanie pliku eksportowania do Kaspersky Security Center Linux
      - Przełączanie zarządzanych urządzeń na zarządzane przez Kaspersky Security Center Linux
- Logowanie do Kaspersky Security Center Web Console i wylogowywanie
- Identity and Access Manager w Kaspersky Security Center Web Console
  - Informacje o Identity and Access Manager
  - Włączanie Identity and Access Manager: scenariusz

- Konfigurowanie Identity and Access Manager w Kaspersky Security Center Web Console
- Rejestrowanie interfejsu aplikacji Kaspersky Industrial CyberSecurity for Networks w Kaspersky Security Center Web Console
- Czas życia tokenów i limit czasu autoryzacji dla Identity and Access Manager
- Pobieranie i dystrybucja certyfikatów IAM
- Wyłączanie Identity and Access Manager

Konfigurowanie uwierzytelniania domeny przy użyciu protokołów NTLM i Kerberos

Konfigurowanie Serwera administracyjnego

- Konfigurowanie połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym
- Konfigurowanie rejestrowania zdarzeń połączenia serwera administracyjnego
- Konfigurowanie ustawień dostępu do Internetu dla Serwera administracyjnego
- Określanie maksymalnej liczby zdarzeń w repozytorium zdarzeń
- Ustawienia połączenia urządzeń chronionych UEFI
- Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego Serwera administracyjnego
- Przeglądanie listy podrzędnych Serwerów administracyjnych
- Usuwanie hierarchii Serwerów administracyjnych
- Konserwacja Serwera administracyjnego
- Konfigurowanie interfejsu
- Zarządzanie wirtualnymi Serwerami administracyjnymi
  - Tworzenie wirtualnego Serwera administracyjnego
  - Włączanie i wyłączanie wirtualnego Serwera administracyjnego
  - Przypisywanie administratora do wirtualnego Serwera administracyjnego
  - Zmienianie Serwera administracyjnego dla urządzeń klienckich
  - Usuwanie wirtualnego Serwera administracyjnego
- Włączanie ochrony konta przed nieautoryzowaną modyfikacją
- Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego
  - Tworzenie zadania wykonywania kopii zapasowej
- Przenoszenie Serwera administracyjnego na inne urządzenie
- Sprawdzanie integralności modułów za pomocą narzędzi klscmodchk i integrity_checker

Początkowa konfiguracja Kaspersky Security Center Web Console

- Kreator wstępnej konfiguracji (Kaspersky Security Center Web Console)
  - Krok 1. Określenie ustawień połączenia internetowego
  - Krok 2. Pobieranie żądanych uaktualnień
  - Krok 3. Wybór elementów do zabezpieczenia
  - Krok 4. Wybieranie szyfrowania w rozwiązaniach
  - Krok 5. Konfigurowanie instalacji wtyczek dla zarządzanych aplikacji
  - Krok 6. Instalowanie wybranych wtyczek
  - Krok 7. Pobieranie pakietów dystrybucyjnych i tworzenie pakietów instalacyjnych
  - Krok 8. Konfigurowanie Kaspersky Security Network
  - Krok 9. Wybieranie metody aktywacji aplikacji
  - Krok 10. Określanie ustawień zarządzania aktualizacjami firm trzecich
  - Krok 11. Tworzenie podstawowej konfiguracji ochrony sieci
  - Krok 12. Konfigurowanie powiadomień e-mail
  - Krok 13. Przeprowadzanie przeszukiwania sieci
  - Krok 14. Zamykanie kreatora wstępnej konfiguracji

- Podłączanie urządzeń mobilnych
  - Scenariusz: Podłączanie urządzeń mobilnych przez bramę połączenia
  - Scenariusz: Połączanie urządzeń spoza biura poprzez podrzędny Serwer administracyjny w strefie DMZ
  - Informacje o podłączaniu urządzeń mobilnych
  - Podłączanie zewnętrznych urządzeń stacjonarnych do Serwera administracyjnego
  - Informacje o profilach połączenia dla użytkowników mobilnych
  - Tworzenie profilu połączenia dla użytkowników mobilnych
  - Informacje o przełączaniu Agenta sieciowego na inne Serwery administracyjne
  - Tworzenie reguły przełączania Agenta sieciowego według lokalizacji sieciowej
- Kreator wdrażania ochrony
  - Krok 1. Uruchamianie kreatora wdrażania ochrony
  - Krok 2. Wybieranie pakietu instalacyjnego
  - Krok 3. Wybieranie metody rozsyłania pliku klucza lub kodu aktywacyjnego
  - Krok 4. Wybieranie wersji Agenta sieciowego
  - Krok 5. Wybór urządzeń
  - Krok 6. Określanie ustawień zadania zdalnej instalacji
  - Krok 7. Zarządzanie ponownym uruchomieniem
  - Krok 8. Usuwanie niekompatybilnych aplikacji przed instalacją
  - Krok 9. Przenoszenie urządzeń do grupy Zarządzane urządzenia
  - Krok 10. Wybieranie kont w celu uzyskania dostępu do urządzeń
  - Krok 11. Uruchamianie instalacji
- Wdrażanie aplikacji Kaspersky poprzez Kaspersky Security Center Web Console
  - Scenariusz: Wdrażanie aplikacji Kaspersky poprzez Kaspersky Security Center Web Console
  - Uzyskiwanie wtyczek dla aplikacji firmy Kaspersky
  - Pobieranie i tworzenie pakietów instalacyjnych dla aplikacji Kaspersky
  - Zmienianie ograniczenia rozmiaru danych niestandardowego pakietu instalacyjnego
  - Pobieranie pakietów dystrybucyjnych dla aplikacji Kaspersky
  - Sprawdzanie, czy pomyślnie wdrożono Kaspersky Endpoint Security
  - Tworzenie autonomicznych pakietów instalacyjnych
  - Przeglądanie listy autonomicznych pakietów instalacyjnych
  - Tworzenie niestandardowego pakietu instalacyjnego
  - Rozsyłanie pakietów instalacyjnych na podrzędne Serwery administracyjne
  - Instalowanie aplikacji przy pomocy zadania zdalnej instalacji
    - Zdalna instalacja aplikacji
    - Instalowanie aplikacji przy użyciu zasad grupy Active Directory
    - Instalowanie aplikacji na podrzędnych Serwerach administracyjnych
  - Określanie ustawień zdalnej instalacji na urządzeniach z systemem Unix
  - Uruchamianie i zatrzymywania działania aplikacji Kaspersky
  - Zarządzanie urządzeniami mobilnymi
  - Zastępowanie aplikacji zabezpieczających firm trzecich
- Wykrywanie urządzeń w sieci
  - Scenariusz: Wykrywanie urządzeń w sieci
  - Wykrywanie urządzeń
    - Przeszukiwanie sieci Windows
    - Przeszukiwanie zakresu IP
    - Dodawanie i modyfikowanie zakresu IP
    - Przeszukiwanie Zeroconf

Przeszukiwanie kontrolera domeny
Uwierzytelnianie i połączenie z kontrolerem domeny
Konfigurowanie kontrolera domeny Samba
Konfigurowanie reguły zatrzymania dla urządzeń nieprzypisanych
Inwentaryzacja sprzętu
Dodawanie informacji o nowych urządzeniach
Konfigurowanie kryteriów wykorzystywanych do określania urządzeń firmowych
Aplikacje Kaspersky: licencjonowanie i aktywacja
Licencjonowanie zarządzanych aplikacji
Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
Dodawanie klucza licencyjnego z Serwera administracyjnego
Rozsyłanie klucza licencyjnego na urządzenia klienckie
Automatyczne rozsyłanie kluczy licencyjnych
Wyświetlanie informacji o używanych kluczach licencyjnych
Usuwanie klucza licencyjnego z repozytorium
Wycofanie zgody z Umową Licencyjną Użytkownika Końcowego
Odnawianie licencji dla aplikacji Kaspersky
Korzystanie z Kaspersky Marketplace do wyboru rozwiązań biznesowych firmy Kaspersky
Konfigurowanie ochrony sieci
Scenariusz: Konfigurowanie ochrony sieci
Informacje o metodach zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku
Konfiguracja i przydzielanie zasad: Metoda skoncentrowana na urządzeniu
Konfiguracja i przydzielanie zasad: Metoda skoncentrowana na użytkowniku
Ustawienia zasady Agenta sieciowego
Porównanie ustawień zasady Agenta sieciowego według systemów operacyjnych
Włączanie i wyłączanie trybu niskiego zużycia zasobów dla Agenta sieciowego
Konfigurowanie ustawień ochrony aplikacji zarządzanych
Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security
Zdalne usuwanie aplikacji lub aktualizacji oprogramowania
Zadania
Informacje o zadaniach
Informacje o obszarze zadania
Tworzenie zadania
Ręczne uruchamianie zadania
Przeglądanie listy zadań
Ogólne ustawienia zadania
Eksportowanie zadania
Importowanie zadania
Uruchamianie kreatora zmiany haseł w zadaniach
Krok 1. Określanie danych uwierzytelniających
Krok 2. Wybieranie działania, jakie ma zostać podjęte
Krok 3. Sprawdzanie wyników
Tworzenie zadania zdalnego wykonywania skryptów
Zdalne instalowanie aplikacji na urządzeniach za pomocą zadania Zdalne wykonywanie skryptów
Konfigurowanie powiadomień i monitorowania dla zadania Zdalne wykonywanie skryptów
Przygotowanie archiwum dla zadania Zdalne wykonywanie skryptów
Tworzenie pakietu instalacyjnego na podstawie pliku manifestu

Zarządzanie urządzeniami klienckimi
Ustawienia zarządzanego urządzenia
Tworzenie grup administracyjnych
Ręczne dodawanie urządzeń do grupy administracyjnej
Ręczne przenoszenie urządzeń lub klastrów do grupy administracyjnej
Tworzenie reguł przenoszenia urządzeń
Kopiowanie reguł przenoszenia urządzeń
Warunki dla reguły przenoszenia urządzenia
Informacje o klastrach i macierzach serwerowych
Właściwości klastra lub macierzy serwerowej
Przeglądanie i konfigurowanie działań, gdy urządzenia wykazują brak aktywności
Informacje o stanach urządzeń
Konfigurowanie przełączania stanów urządzeń
Zdalne połączenie z pulpitem urządzenia klienckiego
Nawiązywanie połączenia z urządzeniami poprzez udostępnianie pulpitu Windows
Wybory urządzeń
Przeglądanie listy urządzeń z wyboru urządzeń
Tworzenie kryteriów wyboru urządzeń
Konfigurowanie kryteriów wyboru urządzeń
Eksportowanie listy urządzeń z wyboru urządzeń
Usuwanie urządzeń z grup administracyjnych w wyborze
Znaczniki urządzeń
Tworzenie znacznika urządzenia
Zmienianie nazwy znacznika urządzenia
Usuwanie znacznika urządzenia
Przeglądanie urządzeń, do których przypisano znacznik
Przeglądanie znaczników przydzielonych do urządzenia
Ręczne oznaczanie urządzenia
Usuwanie przydzielonego znacznika z urządzenia
Wyświetlanie reguł automatycznego oznaczania urządzeń
Edytowanie reguły automatycznego znakowania urządzeń
Tworzenie reguły automatycznego znakowania urządzeń
Uruchamianie reguł automatycznego znakowania urządzeń
Usuwanie reguły automatycznego oznaczania urządzeń
Zarządzanie znacznikami urządzeń za pomocą narzędzia klscflag
Zasady i profile zasad
Informacje o zasadach i profilach zasad
Informacje o blokadzie i zablokowanych ustawieniach
Dziedziczenie zasad i profili zasad
Hierarchia zasad
Profile zasad w hierarchii zasad
Implementacja ustawień na zarządzanym urządzeniu
Zarządzanie zasadami
Przeglądanie listy zasad
Tworzenie zasady
Modyfikowanie zasady
Ogólne ustawienia zasady

Włączanie i wyłączanie opcji dziedziczenia zasady
Kopiowanie zasady
Przenoszenie zasady
Eksportowanie zasady
Importowanie zasady
Przeglądanie wykresu stanu dystrybucji zasad
Usuwanie zasady
Zarządzanie profilami zasad
Przeglądanie profili zasad
Zmiana priorytetu profilu zasad
Tworzenie profilu zasad
Modyfikowanie profilu zasad
Kopiowanie profilu zasad
Tworzenie reguły aktywacji profilu zasad
Usuwanie profilu zasad
Szyfrowanie i ochrona danych
Przeglądanie listy zaszyfrowanych dysków
Wyświetlanie listy zdarzeń szyfrowania
Tworzenie i przeglądanie raportów z szyfrowania
Udzielanie dostępu do zaszyfrowanego dysku w trybie offline
Użytkownicy i role użytkownika
Informacje o rolach użytkowników
Przeglądanie kont użytkowników i sesji
Konfigurowanie praw dostępu do funkcji aplikacji. Kontrola dostępu oparta o rolę
Prawa dostępu do funkcji aplikacji
Informacje o rolach użytkowników
Nadawanie praw dostępu do określonych obiektów
Przydzielanie praw dostępu użytkownikom i grupom bezpieczeństwa
Dodawanie konta użytkownika wewnętrznego
Tworzenie grupy bezpieczeństwa
Edytowanie konta użytkownika wewnętrznego
Edytowanie grupy bezpieczeństwa
Przypisywanie roli do użytkownika lub grupy bezpieczeństwa
Dodawanie kont użytkowników do wewnętrznej grupy bezpieczeństwa
Wskazywanie użytkownika jako właściciela urządzenia
Konfigurowanie weryfikacji dwuetapowej dla wszystkich użytkowników
Informacje o weryfikacji dwuetapowej
Włączanie weryfikacji dwuetapowej dla własnego konta (Web Console)
Włączanie weryfikacji dwuetapowej dla własnego konta (opartej na MMC)
Włączanie wymaganej weryfikacji dwuetapowej dla wszystkich użytkowników (Web Console)
Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników (opartej na MMC)
Wyłączanie weryfikacji dwuetapowej dla konta użytkownika (Web Console)
Wyłączanie weryfikacji dwuetapowej dla konta użytkownika (opartej na MMC)
Wyłączanie wymaganej weryfikacji dwuetapowej dla wszystkich użytkowników (Web Console)
Wyłączanie wymaganej weryfikacji dwuetapowej dla wszystkich użytkowników (opartej na MMC)
Wykluczanie kont z weryfikacji dwuetapowej (Web Console)
Wykluczanie kont z weryfikacji dwuetapowej (opartej na MMC)

Edytowanie nazwy wystawcy kodu zabezpieczającego (Web Console)
Edytowanie nazwy wystawcy kodu zabezpieczającego (opartej na MMC)
Konfigurowanie weryfikacji dwuetapowej dla własnego konta (Web Console)
Konfigurowanie weryfikacji dwuetapowej dla własnego konta (opartej na MMC)
Generowanie nowego tajnego klucza
Uniemożliwienie nowym użytkownikom konfigurowania dla siebie weryfikacji dwuetapowej
Przypisywanie użytkownika jako właściciela urządzenia z systemem Linux po instalacji Agenta sieciowego
Usuwanie użytkownika lub grupy bezpieczeństwa
Zmiana hasła do konta użytkownika
Tworzenie roli użytkownika
Edytowanie roli użytkownika
Edytowanie obszaru roli użytkownika
Usuwanie roli użytkownika
Kojarzenie profili zasad z rolami
Przydzielanie ról użytkownika do podrzędnych Serwerów administracyjnych
Zmiana hasła do konta
Wycofanie uprawnień lokalnego administratora
Zarządzanie rewizjami obiektów
Przywracanie poprzedniej wersji obiektu
Dodawanie opisu rewizji
Wyświetlanie i zapisywanie rewizji zasady
Usuwanie obiektów
Kaspersky Security Network (KSN)
Informacje o KSN
Konfigurowanie dostępu do KSN
Włączanie i wyłączanie korzystania z KSN
Przeglądanie zaakceptowanego Oświadczenia KSN
Akceptowanie zaktualizowanego Oświadczenia KSN
Sprawdzanie, czy punkt dystrybucji działa jako serwer proxy KSN
Scenariusz: Aktualizowanie Kaspersky Security Center i zarządzanych aplikacji zabezpieczających
Aktualizowanie baz danych i aplikacji Kaspersky
Scenariusz: Regularne aktualizowanie baz danych i aplikacji Kaspersky
Informacje o aktualizowaniu baz danych, modułów i aplikacji Kaspersky
Tworzenie zadania Pobierz aktualizacje do repozytorium serwera administracyjnego
Sprawdzanie pobranych uaktualnień
Tworzenie zadania Pobierz uaktualnienia do repozytoriów punktów dystrybucji
Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center
Pobieranie pakietu instalacyjnego dla Kaspersky Endpoint Security for Windows
Zatwierdzanie i odrzucanie aktualizacji oprogramowania
Aktualizowanie Serwera administracyjnego
Włączanie i wyłączanie trybu offline pobierania uaktualnień
Aktualizowanie baz danych i modułów Kaspersky na urządzeniach offline
Tworzenie kopii zapasowych i przywracanie wtyczek webowych
Dostosowanie punktów dystrybucji i bram połączenia
Standardowa konfiguracja punktów dystrybucji: Jedno biuro
Standardowa konfiguracja punktów dystrybucji: Małe zdalne biura

Informacje o przypisywaniu punktów dystrybucji
Automatyczne przypisywanie punktów dystrybucji
Ręczne przypisywanie punktów dystrybucji
Modyfikowanie listy punktów dystrybucji dla grupy administracyjnej
Wymuszona synchronizacja
Włączanie serwera push
Zarządzanie aplikacjami firm trzecich na urządzeniach klienckich
Instalowanie aktualizacji oprogramowania firm trzecich
Scenariusz: Aktualizowanie oprogramowania innej firmy
Instalowanie aktualizacji oprogramowania firm trzecich
Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji
Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji
Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki
Dodawanie reguł dla instalacji aktualizacji
Tworzenie zadania Zainstaluj aktualizacje Windows Update
Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich
Eksportowanie listy dostępnych aktualizacji oprogramowania do pliku
Zatwierdzanie oraz odrzucanie aktualizacji oprogramowania firm trzecich
Tworzenie zadania Wykonaj synchronizację Windows Update
Automatyczne aktualizowanie aplikacji innych firm
Eliminowanie luk w oprogramowaniu innych firm
Scenariusz: Wyszukiwanie i usuwanie luk w oprogramowaniu firm trzecich
Informacje o wyszukiwaniu i eliminowaniu luk w oprogramowaniu
Eliminowanie luk w oprogramowaniu innych firm
Tworzenie zadania Napraw luki
Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki
Dodawanie reguł dla instalacji aktualizacji
Wybieranie poprawek użytkownika dla luk w programach innych firm
Przeglądanie informacji o lukach w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach
Przeglądanie informacji o lukach w oprogramowaniu wykrytych na wybranym zarządzanym urządzeniu
Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach
Eksportowanie listy luk w oprogramowaniu do pliku
Ignorowanie luk w oprogramowaniu
Zarządzanie aplikacjami uruchomionymi na urządzeniach klienckich
Korzystanie z Kontroli aplikacji do zarządzania plikami wykonywalnymi
Tryby i kategorie Kontroli aplikacji
Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich
Tworzenie kategorii aplikacji z zawartością dodaną ręcznie
Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń
Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranego folderu
Przeglądanie listy kategorii aplikacji
Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji
Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows
Uzyskiwanie i przeglądanie listy aplikacji zainstalowanych na urządzeniach klienckich
Tworzenie pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky
Przeglądanie i modyfikowanie ustawienia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky
Ustawienia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky

Znaczniki aplikacji
Tworzenie znacznika aplikacji
Zmienianie nazwy znacznika aplikacji
Przydzielanie znaczników do aplikacji
Usuwanie przydzielonych znaczników z aplikacji
Usuwanie znacznika aplikacji
Monitorowanie i raportowanie
Scenariusz: Monitorowanie i raportowanie
Informacje o typach monitorowania i raportowania
Pulpit nawigacyjny i widżety
Korzystanie z pulpitu nawigacyjnego
Dodawanie widżetów do pulpitu nawigacyjnego
Ukrywanie widżetu na pulpicie nawigacyjnym
Przenoszenie widżetu na pulpicie nawigacyjnym
Zmiana wyglądu i rozmiaru widżetu
Zmiana ustawień widżetu
Informacje o trybie korzystania tylko z pulpitu
Konfigurowanie trybu korzystania tylko z pulpitu
Raporty administracyjne i ochrony
Korzystanie z raportów
Tworzenie szablonu raportu
Przeglądanie i edytowanie właściwości szablonu raportu
Eksportowanie raportu do pliku
Generowanie i przeglądanie raportu
Tworzenie zadania dostarczania raportu
Usuwanie szablonów raportu
Zdarzenia i wybory zdarzeń
Informacje o zdarzeniach Kaspersky Security Center
Używanie wyborów zdarzeń
Tworzenie kryterium wyboru zdarzenia
Edytowanie kryterium wyboru zdarzenia
Przeglądanie listy wyboru zdarzeń
Eksportowanie wyboru zdarzeń
Importowanie wyboru zdarzeń
Przeglądanie szczegółów zdarzenia
Eksportowanie zdarzeń do pliku
Przeglądanie historii obiektu ze zdarzenia
Usuwanie zdarzeń
Usuwanie wyborów zdarzeń
Ustawianie czasu przechowywania dla zdarzenia
Zdarzenia składników Kaspersky Security Center
Struktura danych opisu typu zdarzeń
Zdarzenia Serwera administracyjnego
Zdarzenia krytyczne Serwera administracyjnego
Zdarzenia błędu funkcjonalnego Serwera administracyjnego
Zdarzenia ostrzegające Serwera administracyjnego
Zdarzenia informacyjne Serwera administracyjnego

Zdarzenia Agenta sieciowego
Zdarzenia błędu funkcjonalnego Agenta sieciowego
Zdarzenia ostrzegające Agenta sieciowego
Zdarzenia informacyjne Agenta sieciowego
Zdarzenia serwera iOS MDM
Zdarzenia błędu funkcjonalnego serwera iOS MDM
Zdarzenia ostrzegające serwera iOS MDM
Zdarzenia informacyjne serwera iOS MDM
Blokowanie często występujących zdarzeń
Informacje o blokowaniu często występujących zdarzeń
Zarządzanie blokowaniem często występujących zdarzeń
Usuwanie blokowania często występujących zdarzeń
Powiadomienia i stany urządzeń
Korzystanie z powiadomień
Przeglądanie powiadomień na ekranie
Informacje o stanach urządzeń
Konfigurowanie przełączania stanów urządzeń
Konfigurowanie dostarczania powiadomień
Wyświetlanie powiadomień o zdarzeniach po uruchomieniu pliku wykonywalnego
Ogłoszenia firmy Kaspersky
Informacje o ogłoszeniach firmy Kaspersky
Określanie ustawień ogłoszeń Kaspersky
Wyłączanie ogłoszeń Kaspersky
Przeglądanie informacji dotyczących wykrycia zagrożeń
Cloud Discovery
Włączanie funkcji Cloud Discovery za pomocą widżetu
Dodanie widżetu Cloud Discovery do pulpitu nawigacyjnego
Przeglądanie informacji o korzystaniu z usług w chmurze
Poziom ryzyka usługi w chmurze
Blokowanie dostępu do niechcianych usług w chmurze
Rejestrowanie aktywności Kaspersky Security Center Web Console
Integracja Kaspersky Security Center z innymi rozwiązaniami
Nawiązywanie połączenia w tle
Eksportowanie zdarzeń do systemów SIEM
Konfigurowanie eksportowania zdarzeń do systemów SIEM
Czynności niezbędne do wykonania przed rozpoczęciem pracy
Informacje o zdarzeniach w Kaspersky Security Center
Informacje o eksportowaniu zdarzeń
Informacje o konfigurowaniu eksportowania zdarzeń w systemie SIEM
Oznaczenie zdarzeń do wyeksportowania do systemów SIEM w formacie Syslog
Informacje dotyczące oznaczania zdarzeń do wyeksportowania do systemu SIEM w formacie Syslog
Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog
Oznaczanie ogólnych zdarzeń do eksportu w formacie Syslog
Informacje dotyczące eksportowania zdarzeń przy użyciu formatów CEF i LEEF
Konwersja zdarzeń do formatu CEF lub LEEF
Informacje dotyczące eksportowania zdarzeń przy użyciu formatu Syslog
Konfigurowanie Kaspersky Security Center do wyeksportowania zdarzeń do systemu SIEM

Eksportowanie zdarzeń bezpośrednio z bazy danych
Tworzenie zapytania SQL przy użyciu narzędzia klsql2
Przykład zapytania SQL w narzędziu klsql2
Sprawdzanie nazwy bazy danych Kaspersky Security Center
Przeglądanie wyników eksportowania
Praca z Kaspersky Security Center Web Console i środowiskiem w chmurze
Konfiguracja środowiska chmury w Kaspersky Security Center Web Console
Krok 1. Sprawdzanie wymaganych wtyczek i pakietów instalacyjnych
Krok 2. Licencjonowanie aplikacji
Krok 3. Wybieranie środowiska chmury i autoryzacji
Krok 4. Przeszukiwanie segmentu, konfigurowanie synchronizacji z chmurą i wybieranie dalszych działań
Krok 5. Wybieranie aplikacji, w odniesieniu do której mają zostać utworzone zasada i zadania
Krok 6. Konfigurowanie Kaspersky Security Network dla Kaspersky Security Center
Krok 7. Tworzenie wstępnej konfiguracji ochrony
Przeszukiwanie segmentu sieci za pośrednictwem Kaspersky Security Center Web Console
Dodawanie połączeń dla przeszukiwania segmentu chmury
Usuwanie połączenia dla przeszukiwania segmentu chmury
Konfigurowanie terminarza przeszukiwania za pośrednictwem Kaspersky Security Center Web Console
Przeglądanie wyników przeszukiwania segmentu chmury za pośrednictwem Kaspersky Security Center Web Console
Przeglądanie właściwości urządzeń w chmurze za pośrednictwem Kaspersky Security Center Web Console
Synchronizacja z chmurą: konfigurowanie reguły przenoszenia
Zdalna instalacja aplikacji na maszynach wirtualnych Azure
Tworzenie zadania Utwórz kopię zapasową danych Serwera administracyjnego przy użyciu systemu DBMS w chmurze
Zdalna diagnostyka urządzeń klienckich
Otwieranie okna zdalnej diagnostyki
Włączanie i wyłączanie śledzenia dla aplikacji
Pobieranie plików śledzenia aplikacji
Usuwanie plików śledzenia
Pobierania ustawień aplikacji
Pobierania dzienników zdarzeń
Uruchamianie, zatrzymywanie, ponowne uruchamianie aplikacji
Uruchamianie zdalnej diagnostyki Agenta sieciowego Kaspersky Security Center i pobieranie wyników
Uruchamianie aplikacji na urządzeniu klienckim
Generowania pliku zrzutu dla aplikacji
Uruchamianie zdalnej diagnostyki na urządzeniu klienckim z systemem Linux
Pobieranie i usuwanie plików z Kwarantanny i Kopia zapasowa
Pobieranie plików z Kwarantanny i Kopii zapasowej
Zmiana języka interfejsu oprogramowania Kaspersky Security Center Web Console
Dokumentacja API
Praktyczne zastosowanie aplikacji dla dostawców usługi
Planowanie instalacji Kaspersky Security Center
Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet
Standardowa konfiguracja Kaspersky Security Center
Informacje o punktach dystrybucji
Hierarchia Serwerów administracyjnych
Wirtualne Serwery administracyjne
Zarządzanie urządzeniami mobilnymi z zainstalowanym programem Kaspersky Endpoint Security for Android

Instalacja i wstępna konfiguracja
Zalecenia dotyczące instalacji Serwera administracyjnego
Tworzenie kont dla usług Serwera administracyjnego na klastrze typu failover
Wybieranie systemu zarządzania bazą danych
Określanie adresu Serwera administracyjnego
Konfigurowanie ochrony w sieci organizacji klienta
Ręczna konfiguracja zasady Kaspersky Endpoint Security
Konfigurowanie zasady w sekcji Zaawansowana ochrona przed zagrożeniami
Konfigurowanie zasady w sekcji Podstawowa ochrona przed zagrożeniami
Konfigurowanie zasady w sekcji Ustawienia ogólne
Konfigurowanie zasad w sekcji Konfiguracja zdarzenia
Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security
Ręczna konfiguracja grupowego zadania skanowania urządzeń z zainstalowanym programem Kaspersky Endpoint Security
Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
Ręczna konfiguracja grupowego zadania instalacji uaktualnień i naprawy luk
Tworzenie struktury grup administracyjnych i przydzielanie punktów dystrybucji
Standardowa konfiguracja klienta MSP: Jedno biuro
Standardowa konfiguracja klienta MSP: Wiele małych, zdalnych biur
Hierarchia zasad i korzystanie z zasad
Hierarchia zasad
Profile zasad
Zadania
Reguły przenoszenia urządzeń
Kategoryzacja oprogramowania
Informacje o aplikacjach wielodostępowych
Tworzenie kopii zapasowej i przywracanie ustawień Serwera administracyjnego
Urządzenie z zainstalowanym Serwerem administracyjnym nie działa
Ustawienia Serwera administracyjnego lub bazy danych są uszkodzone
Instalowanie Agenta sieciowego i aplikacji zabezpieczającej
Wstępne wdrożenie
Konfigurowanie instalatorów
Pakiety instalacyjne
Właściwości MSI i pliki transformacji
Zdalna instalacja przy użyciu narzędzi firm trzecich
Informacje ogólne o zadaniach zdalnej instalacji w Kaspersky Security Center
Zdalna instalacja przy użyciu zasad grupy Microsoft Windows
Wymuszone wdrożenie przy użyciu zadania zdalnej instalacji z Kaspersky Security Center
Uruchamianie pakietów autonomicznych utworzonych przez Kaspersky Security Center
Opcje ręcznej instalacji aplikacji
Zdalna instalacja aplikacji na urządzeniach z zainstalowanym Agentem sieciowym
Zarządzanie ponownym uruchamianiem urządzeń w zadaniu zdalnej instalacji
Aktualizowanie baz danych w pakiecie instalacyjnym aplikacji antywirusowej
Usuwanie niekompatybilnych aplikacji zabezpieczających firm trzecich
Usuwanie Agenta sieciowego chronionego hasłem za pomocą wiersza poleceń
Korzystanie z narzędzi do zdalnej instalacji aplikacji z Kaspersky Security Center do uruchamiania odpowiednich plików wykonywalnych na zarządzanych urządzeniach

Monitorowanie wdrożenia
Konfigurowanie instalatorów
Informacje ogólne
Instalacja w trybie cichym (z plikiem odpowiedzi)
Instalacja Agenta sieciowego w trybie cichym (bez pliku odpowiedzi)
Częściowa konfiguracja instalacji poprzez setup.exe
Parametry instalacji Serwera administracyjnego
Ustawienia pakietu instalacyjnego Agenta sieciowego
Infrastruktura wirtualna
Wskazówki dotyczące zmniejszenia obciążenia na maszynach wirtualnych
Obsługa dynamicznych maszyn wirtualnych
Obsługa kopiowania maszyn wirtualnych
Obsługa przywracania systemu plików dla urządzeń z zainstalowanym Agentem sieciowym
Informacje o profilach połączenia dla użytkowników mobilnych
Wdrażanie funkcji Zarządzanie urządzeniami mobilnymi
Połączenie urządzeń KES z Serwerem administracyjnym
Bezpośrednie połączenie urządzeń z Serwerem administracyjnym
Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD)
Korzystanie z Firebase Cloud Messaging
Integracja z infrastrukturą kluczy publicznych
Kaspersky Security Center Web Server
Inne podstawowe prace
Monitorowanie koloru wskaźnika i rejestrowanych zdarzeń w Konsoli administracyjnej
Zdalny dostęp do zarządzanych urządzeń
Korzystanie z opcji „Nie odłączaj od Serwera administracyjnego" w celu zapewnienia ciągłej łączności między zarządzanym urządzeniem a Serwerem administracyjnym
Informacje o sprawdzaniu czasu połączenia pomiędzy urządzeniem a Serwerem administracyjnym
Informacje o wymuszonej synchronizacji
Informacje o tunelowaniu
Poradnik dotyczący rozmiarów
Informacje o podręczniku
Informacje o ograniczeniach Kaspersky Security Center
Wyliczenia dla Serwerów administracyjnych
Obliczanie zasobów sprzętowych dla Serwera administracyjnego
Wymagania sprzętowe dla systemu zarządzania bazą danych i Serwera administracyjnego
Obliczanie pojemności bazy danych
Obliczanie przestrzeni dyskowej (z użyciem oraz bez użycia funkcji Zarządzanie lukami i poprawkami)
Obliczanie liczby i konfigurowanie Serwerów administracyjnych
Zalecenia dotyczące łączenia dynamicznych maszyn wirtualnych z Kaspersky Security Center
Wyliczenia dla punktów dystrybucji i bram połączenia
Wymagania wobec punktu dystrybucji
Obliczanie liczby i konfigurowanie punktów dystrybucji
Obliczanie liczby bram połączenia
Zapisywanie informacji o zdarzeniach dla zadań i zasad
Szczególne względy i optymalne ustawienia określonych zadań
Częstotliwość wykrywania urządzeń
Zadanie tworzenia kopii zapasowej danych Serwera administracyjnego i zadanie konserwacji Serwera administracyjnego

Grupowe zadania aktualizacji Kaspersky Endpoint Security
Zadanie inwentaryzacji
Szczegóły dotyczące obciążenia sieci pomiędzy Serwerem administracyjnym a chronionymi urządzeniami
Zużycie ruchu sieciowego w różnych scenariuszach
Przeciętne zużycie ruchu sieciowego w ciągu 24 godzin
Kontakt z działem pomocy technicznej
Jak uzyskać pomoc techniczną
Pomoc techniczna poprzez Kaspersky CompanyAccount
Uzyskiwanie plików zrzutu Serwera administracyjnego
Źródła informacji o aplikacji
Słownik
Administrator dostawcy usługi
Administrator Kaspersky Security Center
Administrator klienta
Agent autoryzacji
Agent sieciowy
Aktualizacja
Aktualizacja Kaspersky Security Center
Aktywny klucz
Amazon Machine Image (AMI)
Antywirusowe bazy danych
Atak MITM
Atak wirusa
AWS API (Application Program Interface)
Bezpośrednie zarządzanie aplikacjami
Brama połączenia
Certyfikat współdzielony
Certyfikatu Serwera administracyjnego
Cloud Discovery
Dodatkowy (lub rezerwowy) klucz licencyjny
Domena rozgłoszeniowa
Dostawca usługi ochrony antywirusowej
Dostępne aktualizacje
FileTransferBridge
Folder Kopia zapasowa
Funkcja rozpoznawania lokalizacji w sieci (NLA)
Grupa administracyjna
Grupa licencjonowanych aplikacji
HTTPS
Identity and Access Management (IAM)
Instalacja lokalna
Instalacja ręczna
Instalacja wymuszona
Instalacja zdalna
Instancja Amazon EC2
Istotność poprawki
JavaScript

Kaspersky Private Security Network (KPSN)
Kaspersky Security Center System Health Validator (SHV)
Kaspersky Security Center Web Server
Kaspersky Security Network (KSN)
Klient Serwera administracyjnego (urządzenie klienckie)
Klucz dostępu AWS IAM
Konsola administracyjna
Konsola zarządzania AWS
Kopia zapasowa danych Serwera administracyjnego
Lightweight Nagent (LWNGT)
Luka
Macierzysty Serwer administracyjny
Niekompatybilna aplikacja
Ochrona antywirusowa sieci
Okres licencji
Operator Kaspersky Security Center
Pakiet instalacyjny
Plik klucza
Priorytet zdarzenia
Profil informacyjny
Profil iOS MDM
Profil konfiguracyjny
Próg aktywności wirusa
Przewodnik po zwiększaniu odporności
Przywracanie
Przywrócenie danych Serwera administracyjnego
Punkt dystrybucji
Repozytorium zdarzeń
Rola IAM
Scentralizowane zarządzanie aplikacjami
Serwer administracyjny
Serwer iOS MDM
Serwer urządzeń mobilnych
Serwery aktualizacji Kaspersky
Sklep aplikacji
Środowisko chmury
SSL
Stacja robocza administratora
Stan ochrony
Stan ochrony sieci
Strefa zdemilitaryzowana (DMZ)
Uprawnienia administracyjne
Urządzenie chronione UEFI
Urządzenie iOS MDM
Urządzenie KES
Ustawienia programu
Ustawienia zadania

Użytkownicy wewnętrzni
Użytkownik IAM
Windows Server Update Services (WSUS)
Wirtualny Serwer administracyjny
Właściciel urządzenia
Wtyczka administracyjna
Zadanie
Zadanie dla określonych urządzeń
Zadanie grupowe
Zadanie lokalne
Zarządzane urządzenia
Zasada
Informacje o kodzie firm trzecich
Informacje o znakach towarowych
Znane problemy

System pomocy Kaspersky Security Center 15.1

	**Nowości** Zapoznaj się z nowościami w najnowszym wydaniu produktu.		**Konfigurowanie ochrony sieci** Zarządzaj bezpieczeństwem organizacji.
	**Wymagania sprzętowe i programowe** Sprawdź, które systemy operacyjne i wersje aplikacji są obsługiwane.		**Aplikacje Kaspersky. Aktualizowanie baz danych i modułów aplikacji** Zachowaj niezawodność systemu ochrony.
	**Instalacja i wstępna konfiguracja** Rozplanuj korzystanie z zasobów, instalację Serwera administracyjnego, instalację Agenta sieciowego i aplikacji zabezpieczających na urządzeniach klienckich, a także przyłączenie urządzeń do grup administracyjnych.		**Monitorowanie i raportowanie** Sprawdź swoją infrastrukturę, stany ochrony i statystyki. Zarządzaj dostępem do usług w chmurze za pomocą Cloud Discovery.
	**Wykrywanie urządzeń w sieci** Wyszukuj istniejące i nowe urządzenia w sieci organizacji.		**Zastępowanie aplikacji zabezpieczających firm trzecich** Poznaj metody odinstalowywania niekompatybilnych aplikacji.
	**Aplikacje Kaspersky. Scentralizowane wdrażanie** Zdalnie instaluj aplikacje Kaspersky.		**Dostosowanie punktów dystrybucji i bram połączenia** Konfiguruj punkty dystrybucji.
	**Aktualizowanie Kaspersky Security Center z poprzedniej wersji** Aktualizuj Kaspersky Security Center 15.1 z poprzedniej wersji.		**Praktyczne zastosowanie aplikacji dla dostawców usługi (tylko pomoc online)** Zapoznaj się z zaleceniami dotyczącymi instalacji, konfiguracji i korzystania z aplikacji, a także sposobami rozwiązywania typowych problemów występujących podczas działania aplikacji.
	**Aplikacje Kaspersky. Licencjonowanie i aktywacja** Aktywuj aplikacje Kaspersky w kilku krokach.		**Podręcznik dotyczący rozmiarów (tylko pomoc online)** Aby zapewnić optymalną wydajność w różnych warunkach pracy, należy wziąć pod uwagę liczbę urządzeń w sieci, topologię sieci oraz zestaw funkcji Kaspersky Security Center, jakich potrzebujesz.
	**Eksportowanie zdarzeń do systemów SIEM** Skonfiguruj eksportowanie zdarzeń do systemów SIEM w celu przeprowadzenia analizy.		**Zarządzanie lukami i poprawkami** Wyszukaj i wyeliminuj luki w oprogramowaniu firm trzecich.
	**Praca w środowisku chmury** Zainstaluj Kaspersky Security Center w środowiskach chmury: Amazon Web Services™, Microsoft Azure™, Google™ Cloud Platform.		**Często Zadawane Pytania (Tylko język angielski)** Znajdź instrukcje rozwiązywania typowych problemów.
	**Przewodnik szybkiego uruchomienia Kaspersky Endpoint Security for Business** Zacznij korzystać z Kaspersky Endpoint Security for Business: zainstaluj i skonfiguruj to rozwiązanie. Możesz również sprawdzić porównanie funkcji Kaspersky Security Center, aby wybrać najbardziej odpowiedni sposób zarządzania bezpieczeństwem sieci.		

Nowości

Kaspersky Security Center 15.1 Aktualizacja 2

Kaspersky Security Center 15.1 Aktualizacja 2 koncentruje się na naprawianiu problemów zgłaszanych przez użytkowników i zespół testujący:

- Zadania są teraz wykonywane poprawnie w zakresie zarządzanych urządzeń opartych na systemie Linux, określonych przez zaimportowanie pliku TXT.
- Teraz, gdy aplikacja Kaspersky jest instalowana za pomocą zadania instalacji zdalnej utworzonego na wirtualnym Serwerze administracyjnym, pakiety instalacyjne są przesyłane do zarządzanych urządzeń za pośrednictwem narzędzi systemu operacyjnego wyłącznie za pośrednictwem punktu dystrybucji zarządzanego przez ten wirtualny Serwer administracyjny.
- Rozwiązano problem, w wyniku którego podrzędny Serwer administracyjny nie mógł nawiązać ponownego połączenia z głównym Serwerem administracyjnym po rotacji certyfikatu podrzędnego Serwera.
- Rozwiązano problemy związane z połączeniami TLS.
- Rozwiązano problem powodujący występowanie wielu błędów „Nieprawidłowy typ rzutowania" podczas logowania użytkownika.
- Kaspersky Security Center teraz poprawnie wysyła powiadomienia o zdarzeniach pocztą e-mail.
- Naprawiono problem z dodawaniem folderu *Aktualizacje* do kopii zapasowej podczas uaktualniania Kaspersky Security Center z wersji 14.2 do wersji 15.1.
- Data wygaśnięcia licencji aplikacji Kaspersky jest teraz poprawnie wyświetlana w Kaspersky Security Center Web Console.
- Polecenia **Zlokalizuj urządzenie mobilne** i **Pobierz historię lokalizacji urządzenia** działają teraz poprawnie.
- Naprawiono problem, w wyniku którego pakiety instalacyjne z certyfikatami mobilnymi nie były automatycznie usuwane po 1 godzinie od pobrania lub po 24 godzinach od momentu ich nieużywania.
- Profil zasady aktywowany przez konkretny znacznik jest teraz prawidłowo stosowany do urządzeń, których opisy zawierają ten znacznik.
- Naprawiono problem powodujący wyświetlanie komunikatów o błędach bazy danych PostgreSQL w dzienniku zdarzeń.
- Wykluczanie konta z dwuetapowej weryfikacji działa teraz prawidłowo.
- Naprawiono problem, w wyniku którego wylogowywanie się z Kaspersky Security Center Web Console nie działało poprawnie w przypadku korzystania z uwierzytelniania domeny z włączonym Menedżerem tożsamości i dostępu.
- Teraz podczas aktualizacji zarządzającej wtyczki internetowej kliknięcie łącza z wymaganą wersją wtyczki spowoduje rozpoczęcie pobierania.

- Naprawiono problemy w raportach:
  - Po utworzeniu zadania dostarczania raportów o zagrożeniach i aktualizacjach oraz ustawieniu harmonogramu zadań na **Co miesiąc** raporty będą poprawnie wypełniane danymi.
  - W szablonie *Raport o stanie składników aplikacji* filtry według nazwy komponentu są prawidłowo stosowane.
  - *Raport wdrażania ochrony* można teraz filtrować, aby wyświetlić tylko te urządzenia, na których nie zainstalowano aplikacji Kaspersky. Pomaga to zwizualizować liczbę urządzeń, na których aplikacje mają zostać zainstalowane przez instalatora.
- Widżet **Cloud Discovery** jest prawidłowo wyświetlany niezależnie od tego, czy masz uprawnienie **Wykonaj** w obszarze **Funkcje ogólne: Podstawowa funkcjonalność**.
- Poprawiona wydajność procedur składowanych i operacji na bazach danych.
- Naprawiono problem, w wyniku którego wygasłe certyfikaty powiązane z nieistniejącymi użytkownikami powodowały zatrzymanie procesu odnawiania dla wszystkich użytkowników.
- Rozwiązano problemy wpływające na prawidłowe przetwarzanie certyfikatów.
- Po uaktualnieniu Kaspersky Security Center z wersji 14.2 do 15.1 pobieranie autonomicznego pakietu instalacyjnego z pomocniczego wirtualnego Serwera administracyjnego w Konsoli administracyjnej działa teraz poprawnie.
- Naprawiono błąd w Kaspersky Security Center Web Console gdzie, po włączeniu korzystania z Kaspersky Security Network (KSN) w zasadach aplikacji Kaspersky zaakceptowanie Oświadczenia KSN nie było dostępne dla następujących aplikacji: Kaspersky Endpoint Security for Linux w wersji 12.2 lub starszej, Kaspersky Industrial CyberSecurity for Linux Nodes w wersji 1.5 lub starszej, Kaspersky Security for Virtualization Light Agent w wersji 6.0 i 6.1, Kaspersky Embedded Systems Security for Linux w wersji 3.3 oraz Kaspersky Security for Windows Server w wersji 11.0.1.897.
- Naprawiono problem, w wyniku którego profil zasad nie był stosowany do urządzeń opartych na systemie Linux, które znajdowały się w grupie domen Active Directory.
- Naprawiono problem, który występował podczas prób nawiązania połączenia z kilku podrzędnych Serwerów administracyjnych drugiego poziomu do głównego Serwera administracyjnego.

Kaspersky Security Center 15.1

Kaspersky Security Center 15.1 posiada kilka nowych funkcji i ulepszeń:

- Cloud Discovery. To jest nowa funkcja, która umożliwia monitorowanie korzystania z usług w chmurze na zarządzanych urządzeniach z systemem Windows i blokowanie dostępu do usług w chmurze, które użytkownik uważa za niepożądane. Ta funkcja jest dostępna tylko w Kaspersky Security Center Web Console.
- Funkcja przeszukiwania kontrolera domeny umożliwia teraz przeszukiwanie kontrolera domeny Samba za pośrednictwem punktu dystrybucji opartego na systemie Linux. Wprowadzono dodatkowe udoskonalenia mające na celu obsługę przeszukiwania dużych domen.
- Ulepszona zdalna diagnostyka zarządzanych urządzeń z systemem Linux.

- Rozszerzona inwentaryzacja sprzętu urządzeń macOS. Agent sieciowy na urządzeniu z systemem macOS wysyła adres MAC i numer seryjny urządzenia do Serwera administracyjnego.
- Teraz możesz sprawdzić połączenie z systemem SIEM.
- Maksymalna długość hasła dla użytkownika wewnętrznego została zwiększona do 256 znaków.
- Podczas migracji z Kaspersky Security Center Windows do Kaspersky Security Center Linux możesz przełączyć zarządzane urządzenia tak, aby były zarządzane przez Kaspersky Security Center Linux, przywracając certyfikat i klucz prywatny Serwera administracyjnego z kopii zapasowej.
- Po uruchomieniu narzędzia Cleaner lub klmover w celu usunięcia Agenta sieciowego chronionego hasłem zostaniesz poproszony o podanie hasła dezinstalacyjnego.
- Aktualizacja z Kaspersky Endpoint Security for Windows do Kaspersky Security for Windows Server nie wymaga już ponownego uruchomienia urządzenia docelowego.
- Użytkownik może zostać przypisany jako właściciel urządzenia podczas lub po instalacji Agenta sieciowego na urządzeniu klienckim w systemie Linux.
- W przypadku instalacji oprogramowania na zarządzanych urządzeniach za pomocą niestandardowych skryptów możesz teraz otrzymać raport dotyczący instalacji zdalnej.
- Jeśli wykonujesz kilka niestandardowych skryptów na zarządzanym urządzeniu, możesz ustawić priorytet dla każdego skryptu, aby określić kolejność wykonywania. Skrypty będą wykonywane od tego o najwyższym priorytecie do tego o najniższym priorytecie.
- Rozszerzony audyt zasad. Możesz teraz wyświetlić treść rewizji zasad i zapisać ją w pliku. Obecnie te funkcje są dostępne tylko dla zasady Serwera administracyjnego i zasady Agenta sieciowego.
- Rozwiązania podwyższająca poziom komfortu użytkownika, w tym:
  - Personalizacja menu głównego poprzez przypinanie sekcji konsoli Kaspersky Security Center Web Console w celu szybkiego dostępu z sekcji **Przypięte**.
  - Zoptymalizowana praca z tabelami. Domyślny widok każdej tabeli zawiera teraz najczęściej używane kolumny. Obecnie możesz zaznaczyć wszystkie elementy na bieżącej stronie lub w całej tabeli, a także posortować elementy w całej tabeli.
  - Lepsza konfiguracja funkcja dostarczania raportów. Możesz teraz określić maksymalnie 20 adresów e-mail, na które chcesz wysłać raport, oraz harmonogram dostarczania raportu.
- Możesz cofnąć uprawnienia administratora lokalnego dla kont na zarządzanych urządzeniach z systemem Linux. Zapewnia to dodatkową warstwę kontroli nad kontami użytkowników. Można na przykład wycofać uprawnienia administratora lokalnego po zakończeniu jednorazowego przypisania.
- Możesz zmienić hasło do konta lokalnego, na zarządzanych urządzeniach z systemem Linux, na przykład gdy użytkownik zapomni hasła do tego konta lub w celu wykonania zaplanowanej zmiany hasła.
- W podsekcji **Zarządzanie certyfikatami użytkownika** możesz określić, które certyfikaty główne mają zostać zainstalowane. Certyfikaty te mogą służyć np. do weryfikacji autentyczności stron internetowych czy serwerów internetowych.
- Raport o atakach sieciowych zawiera teraz adres MAC i port atakującego urządzenia.

- Nowa opcja wymuszająca na użytkowniku wewnętrznym zmianę hasła przy następnej próbie zalogowania się do Kaspersky Security Center Web Console.
- Licencja komercyjna nie jest już sprawdzana podczas eksportowania zdarzeń do systemu SIEM w formatach CEF lub LEEF.
- Jeśli migrujesz z jednej aplikacji Kaspersky do innej, a Twoja bieżąca aplikacja jest chroniona hasłem, możesz teraz określić hasło dezinstalacyjne w zadaniu instalacji zdalnej.
- Protokół Exchange ActiveSync nie jest już obsługiwany.

Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 posiada kilka nowych funkcji i ulepszeń:

- Wydano nowy przewodnik zwiększania bezpieczeństwa. Zdecydowanie zalecamy uważne przeczytanie przewodnika i postępowanie zgodnie z zaleceniami dotyczącymi bezpieczeństwa w celu skonfigurowania Kaspersky Security Center i infrastruktury sieciowej.

  Zainstaluj również najnowszą aktualizację Kaspersky Security Center. Ta aktualizacja zawiera funkcje ochrony infrastruktury, takie jak dwuetapowa weryfikacja kont użytkowników i inne ulepszenia.
- Dostęp do serwerów Kaspersky jest teraz weryfikowany automatycznie. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznego DNS.
- Uprawnienia użytkownika na wirtualnym Serwerze administracyjnym są dostępne do konfiguracji w dowolnym momencie niezależnie od podstawowego Serwera administracyjnego. Użytkownikom Serwera podstawowego można również przypisać prawa do zarządzania Serwerem wirtualnym.
- Kaspersky Security Center obsługuje teraz pracę z następującymi systemami DBMS:
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (wszystkie wersje)
  - Postgres Pro 14.x (wszystkie wersje)
  - MariaDB 10.1, 10.4, 10.5
- Możesz użyć Kaspersky Security Center Web Console do wyeksportowania zasad i zadań do pliku, a następnie zaimportowania zasad i zadań do Kaspersky Security Center Windows lub Kaspersky Security Center Linux.
- Opcja **Nie używaj serwera proxy** została usunięta z następujących zadań:
  - *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
  - *Pobierz aktualizacje do repozytoriów punktów dystrybucji*

- Aby chronić urządzenia klienckie w środowisku chmury, możesz wdrożyć Kaspersky Endpoint Security for Windows zamiast Kaspersky Security for Windows Server. Ta funkcja jest teraz dostępna po udostępnieniu wersji Kaspersky Endpoint Security 12.0 for Windows.

- Praca z kluczami szyfrowania jest teraz ograniczona prawami dostępu do obszaru funkcyjnego **Funkcje ogólne**: **Zarządzanie kluczem szyfrowania**. Użytkownicy Kaspersky Security Center mogą teraz eksportować klucze szyfrowania, jeśli mają uprawnienia do **Odczytu**, oraz importować klucze szyfrowania, jeśli mają uprawnienia do **Zapisu**.

Kaspersky Security Center 14

Kaspersky Security Center 14 posiada kilka nowych funkcji i ulepszeń:

- Możesz instalować aktualizacje i eliminować luki w zabezpieczeniach oprogramowania innych firm (z wyjątkiem oprogramowania firmy Microsoft) w odizolowanej sieci. Takie sieci obejmują Serwery administracyjne i zarządzane urządzenia, które nie mają dostępu do Internetu. Aby naprawić luki w tego rodzaju sieci, musisz pobrać wymagane aktualizacje za pomocą Serwera administracyjnego z dostępem do Internetu, a następnie przesłać poprawki do odizolowanych Serwerów administracyjnych.

- Do urządzeń z systemem macOS dodano profile połączeń dla użytkowników mobilnych. Korzystając z profili połączeń, możesz skonfigurować reguły dla Agentów sieciowych na urządzeniach macOS, aby łączyły się z tym samym lub różnymi Serwerami administracyjnymi, w zależności od lokalizacji urządzenia.

- Agenta sieciowego można teraz zainstalować na urządzeniach z systemem Microsoft Windows 10 IoT Enterprise.

- W ustawieniu **Raport o zagrożeniach** możesz teraz filtrować listę zagrożeń, aby wyświetlić tylko te zagrożenia, które zostały wykryte przez Cloud Sandbox.

- Kaspersky Security Center obsługuje teraz Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 jako aplikację zarządzaną.

Kaspersky Security Center Web Console posiada kilka nowych funkcji i ulepszeń:

- Możesz skonfigurować tryb samego pulpitu dla pracowników, którzy nie zarządzają siecią, ale chcą przeglądać statystyki ochrony sieci w Kaspersky Security Center (na przykład dla menedżera najwyższego poziomu). Gdy użytkownik ma włączony ten tryb, wyświetlany jest tylko pulpit nawigacyjny z predefiniowanym zestawem widżetów. Dzięki temu może monitorować statystyki określone w widżetach, na przykład stan ochrony wszystkich zarządzanych urządzeń, liczbę ostatnio wykrytych zagrożeń lub listę najczęstszych zagrożeń w sieci.

- Kaspersky Security Center Web Console obsługuje teraz Kaspersky Security for iOS jako aplikację zabezpieczającą.

- We właściwościach zadania możesz określić, czy chcesz zastosować zadanie do podgrup i podrzędnych Serwerów administracyjnych (w tym wirtualnych).

- Kaspersky Security Center obsługuje teraz Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 jako aplikację zarządzaną.

Kaspersky Security Center 13.2

Kaspersky Security Center 13.2 posiada kilka nowych funkcji i ulepszeń:

- Możesz teraz zainstalować Serwer administracyjny, Konsolę administracyjną, konsolę Kaspersky Security Center 13.2 Web Console i Agenta sieciowego na następujących nowych systemach operacyjnych (szczegóły w wymaganiach oprogramowania):
  - Microsoft Windows 11
  - Microsoft Windows 10 21H2 (October 2021 Update)
  - Windows Server 2022
- Możesz użyć MySQL 8.0 jako bazy danych.
- Możesz zainstalować Kaspersky Security Center na klastrze typu failover Kaspersky Security Center, aby zapewnić wysoką dostępność Kaspersky Security Center.
- Kaspersky Security Center pracuje teraz z adresami IPv6 oraz z adresami IPv4. Serwer administracyjny może przeszukiwać sieci posiadające urządzenia z adresami IPv6.

Kaspersky Security Center 13.2 Web Console posiada kilka nowych funkcji i ulepszeń:

- Możesz teraz zarządzać urządzeniami mobilnymi działającymi pod kontrolą systemu Android poprzez konsolę Kaspersky Security Center 13.2 Web Console.
- Platforma handlowa Kaspersky jest dostępna jako nowa sekcja menu: możesz wyszukać aplikację Kaspersky poprzez Kaspersky Security Center 13.2 Web Console.
- Kaspersky Security Center obsługuje teraz następujące aplikacje Kaspersky:
  - Kaspersky Endpoint Detection and Response Optimum 2.0
  - Kaspersky Sandbox 2.0
  - Kaspersky Industrial CyberSecurity for Networks 3.1

Kaspersky Security Center 13.1

Kaspersky Security Center 13.1 posiada kilka nowych funkcji i ulepszeń:

- Udoskonalono integrację z systemami SIEM. Teraz można wyeksportować zdarzenia do systemów SIEM za pośrednictwem zaszyfrowanego kanału (TLS). Funkcja jest dostępna dla Kaspersky Security Center Web Console i Konsoli administracyjnej opartej na MMC.
- Teraz możesz pobierać poprawki dla Serwera administracyjnego jako pakiet dystrybucyjny, którego możesz używać do przyszłych aktualizacji do nowszych wersji.

- Do Kaspersky Security Center 13.1 Web Console, dla Kaspersky Endpoint Detection and Response Optimum dodano nową sekcję **Powiadomienia**. Do pracy z zagrożeniami wykrytymi przez Kaspersky Endpoint Detection and Response Optimum dodano kilka nowych widżetów.

- W Kaspersky Security Center 13.1 Web Console możesz teraz otrzymywać powiadomienia na temat wygasłych licencji dla aplikacji firmy Kaspersky.

- Czas odpowiedzi dla Kaspersky Security Center 13.1 Web Console został wydłużony.

Kaspersky Security Center 13

Do konsoli Kaspersky Security Center 13 Web Console dodano następujące funkcje:

- Zaimplementowano weryfikację dwuetapową. Możesz włączyć weryfikację dwuetapową, aby zmniejszyć ryzyko nieautoryzowanego dostępu do konsoli Kaspersky Security Center 13 Web Console.

- Zaimplementowano uwierzytelnianie domeny przy użyciu protokołów NTLM i Kerberos (technologia pojedynczego logowania). Funkcja pojedynczego logowania umożliwia użytkownikowi systemu Windows włączenie bezpiecznego uwierzytelniania w konsoli Kaspersky Security Center 13 Web Console bez konieczności ponownego wprowadzania hasła w sieci firmowej.

- Teraz możesz skonfigurować wtyczkę do pracy z Kaspersky Managed Detection and Response. Możesz użyć tej integracji do przeglądania incydentów i zarządzania stacjami roboczymi.

- Możesz teraz określić ustawienia dla Kaspersky Security Center 13 Web Console w kreatorze instalacji Serwera administracyjnego.

- Wyświetlane są powiadomienia o nowych wydaniach aktualizacji i poprawek. Możesz zainstalować aktualizację natychmiast lub później w dowolnym momencie. Możesz teraz zainstalować łaty dla Serwera administracyjnego poprzez konsolę Kaspersky Security Center 13 Web Console.

- Podczas pracy z tabelami można teraz określić kolejność i szerokość kolumn, sortować dane i określać rozmiar strony.

- Możesz teraz otworzyć dowolny raport, klikając jego nazwę.

- Konsola Kaspersky Security Center 13 Web Console jest teraz dostępna w języku koreańskim.

- W menu **Monitorowanie i raportowanie** dostępna jest nowa sekcja, Zapowiedzi firmy Kaspersky. Ta sekcja zawiera informacje dotyczące Twojej wersji Kaspersky Security Center i zarządzanych aplikacji, zainstalowanych na zarządzanych urządzeniach. Kaspersky Security Center okresowo aktualizuje informacje w tej sekcji, usuwając nieaktualne ogłoszenia i dodając nowe informacje. Jednakże możesz wyłączyć ogłoszenia Kaspersky, jeśli chcesz.

- Zaimplementowano dodatkowe uwierzytelnianie po zmianie ustawień konta użytkownika. Możesz włączyć ochronę konta użytkownika przed nieautoryzowaną modyfikacją. Jeżeli opcja jest włączona, modyfikowanie ustawień konta użytkownika wymaga autoryzacji przez użytkownika z uprawnieniami do modyfikacji.

Do Kaspersky Security Center 13 dodano następujące funkcje:

- Zaimplementowano weryfikację dwuetapową. Możesz włączyć weryfikację dwuetapową, aby zmniejszyć ryzyko nieautoryzowanego dostępu do Konsoli administracyjnej. Jeżeli opcja jest włączona, modyfikowanie ustawień konta użytkownika wymaga autoryzacji przez użytkownika z uprawnieniami do modyfikacji. Możesz teraz włączyć lub wyłączyć weryfikację dwuetapową dla urządzeń KES.

- Możesz wysyłać wiadomości do Serwera administracyjnego przez HTTP. Dostępna jest Dokumentacja i biblioteka Pythona do pracy z OpenAPI Serwera administracyjnego.

- Możesz wystawić zapasowy certyfikat do użycia w profilach iOS MDM, aby zapewnić bezproblemowe przełączanie zarządzanych urządzeń iOS po wygaśnięciu certyfikatu iOS MDM Server.

- Folder aplikacji dla wielu dzierżawców nie jest już wyświetlany w Konsoli administracyjnej.

Informacje o Kaspersky Security Center

Sekcja zawiera informacje o przeznaczeniu Kaspersky Security Center, jego głównych funkcjach i komponentach oraz sposobach zakupu Kaspersky Security Center.

Informacje dostępne w pomocy online mogą różnić się od informacji w dokumentacji dołączonej do aplikacji. W tym przypadku, system pomocy online jest uznawany za aktualny. Internetowy system pomocy można otworzyć, klikając odnośniki w interfejsie aplikacji lub klikając odpowiedni odnośnik w dokumentacji. Internetowy system pomocy może być aktualizowany bez wcześniejszego powiadamiania o tym fakcie. W razie potrzeby możesz przełączać się między pomocą online i pomocą offline.

Kaspersky Security Center służy do scentralizowanego wykonywania podstawowych zadań dotyczących administracji i zarządzania w sieci firmy. Aplikacja zapewnia administratorowi dostęp do szczegółowych informacji dotyczących poziomu ochrony sieci firmy; pozwala na skonfigurowanie wszystkich składników ochrony opartych o aplikacje Kaspersky.

Kaspersky Security Center jest aplikacją przeznaczoną dla administratorów sieci firmowych oraz dla pracowników odpowiedzialnych za ochronę urządzeń w różnych organizacjach.

Korzystając z Kaspersky Security Center, możesz:

- Utworzyć hierarchię Serwerów administracyjnych, aby zarządzać siecią firmy oraz sieciami odległych biur lub organizacji klienta.

  Organizacja klienta to organizacja, której ochrona antywirusowa jest zapewniana przez dostawcę usługi.

- Utworzyć hierarchię grup administracyjnych, aby zarządzać wyborem urządzeń klienckich jako całością.
- Zarządzać systemem ochrony antywirusowej zbudowanym w oparciu o aplikacje Kaspersky.
- Utworzyć obrazy systemów operacyjnych i instalować je na urządzeniach klienckich w sieci oraz wykonywać zdalną instalację aplikacji firmy Kaspersky i innych dostawców oprogramowania.
- Zdalnie zarządzać aplikacjami firmy Kaspersky i innych producentów, które są zainstalowane na urządzeniach klienckich. Instalować aktualizacje, wyszukiwać i eliminować luki.
- Wykonywać scentralizowane wdrażanie kluczy licencyjnych dla aplikacji Kaspersky na urządzenia klienckie, monitorowanie ich wykorzystania i odnawianie licencji.
- Otrzymywać statystyki i raporty dotyczące pracy aplikacji i urządzeń.
- Otrzymywać powiadomienia na temat zdarzeń krytycznych występujących podczas działania aplikacji Kaspersky.
- Zarządzać urządzeniami mobilnymi.
- Zarządzać szyfrowaniem informacji przechowywanych na dyskach twardych urządzeń i nośników wymiennych oraz dostępem użytkowników do zaszyfrowanych danych.
- Wykonywać inwentaryzację sprzętu podłączonego do sieci firmy.
- Centralnie zarządzać plikami umieszczonymi w Kwarantannie lub Kopii zapasowej przez aplikacje zabezpieczające, a także zarządzać plikami, których przetwarzanie zostało odroczone.

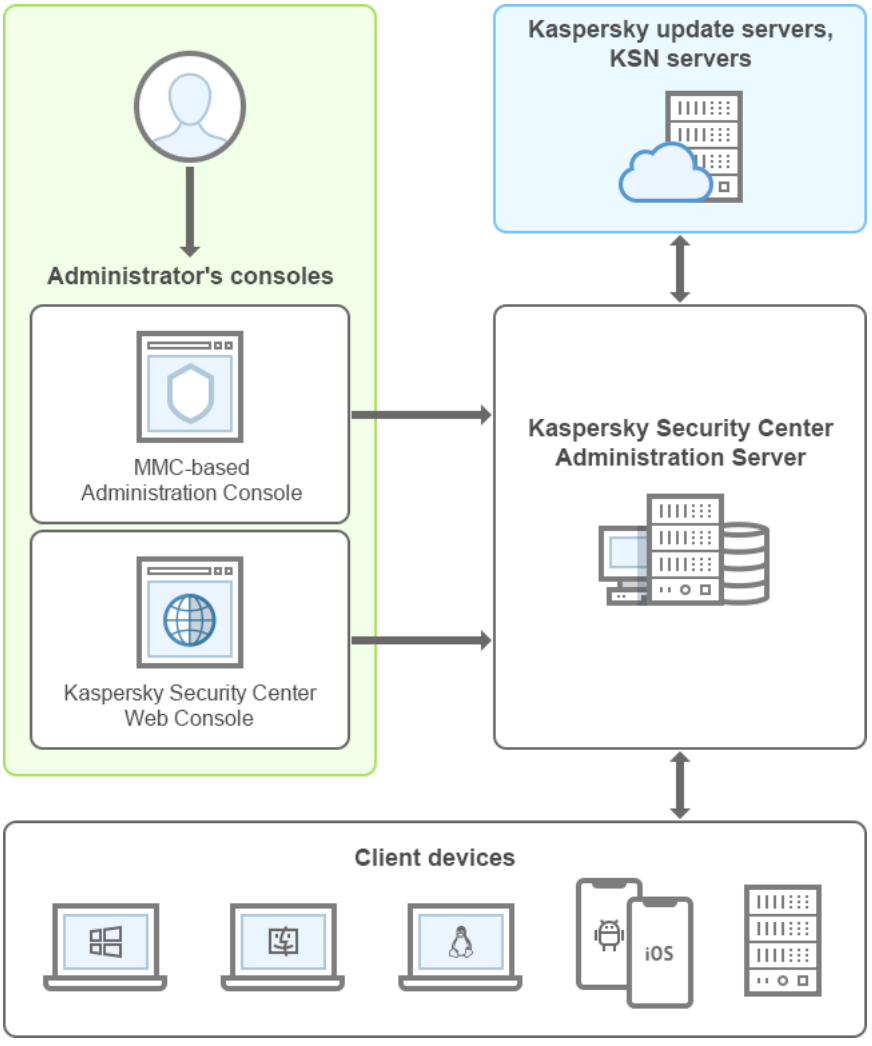
Możesz kupić Kaspersky Security Center za pośrednictwem Kaspersky (na przykład na stronie https://www.kaspersky.com) lub za pośrednictwem firm partnerskich.

Jeśli Kaspersky Security Center zakupiono za pośrednictwem Kaspersky, możesz skopiować aplikację z naszej strony internetowej. Informacje wymagane do aktywacji aplikacji są wysyłane do Ciebie e-mailem po przetworzeniu płatności.

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), przy czym funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Architektura

Ta sekcja zawiera opis komponentów Kaspersky Security Center i ich interakcji.



Architektura Kaspersky Security Center

Kaspersky Security Center zawiera następujące główne moduły:

- *Konsola administracyjna* (zwana dalej również *Konsolą*). Jest interfejsem użytkownika umożliwiającym zarządzanie usługami Serwera administracyjnego i Agenta sieciowego. Konsola administracyjna jest zaimplementowana jako rozszerzenie konsoli Microsoft Management Console (MMC). Konsola administracyjna pozwala na zdalne połączenie z Serwerem administracyjnym przez Internet.

- *Kaspersky Security Center Web Console*. Oferuje interfejs webowy do tworzenia i utrzymania systemu ochrony sieci organizacji klienta zarządzanej przez Kaspersky Security Center.

- *Serwer administracyjny Kaspersky Security Center* (zwany również *Serwer*). Scentralizowane repozytorium informacji dotyczących aplikacji zainstalowanych w sieci firmowej oraz informacji dotyczących sposobu zarządzania tymi aplikacjami.

- *Serwery aktualizacji Kaspersky*. Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji.

- *Serwery KSN*. Serwery, które zawierają bazę danych firmy Kaspersky, zawierającej ciągle aktualizowane informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji Kaspersky po wykryciu zagrożenia, ulepszenie działania niektórych składników ochrony oraz zmniejszenie ryzyka wystąpienia fałszywych alarmów.

- *Urządzenia klienckie*. Urządzenia klienckie firmy chronione przez Kaspersky Security Center. Każde urządzenie, które musi być chronione, musi posiadać zainstalowaną jedną z aplikacji zabezpieczających Kaspersky.

Wymagania sprzętowe i programowe

- Wymagania Serwera administracyjnego
- Wymagania Web Console
- Wymagania dotyczące serwerów mobilnych
- Wymagania Konsoli administracyjnej
- Wymagania Agenta sieciowego

Wymagania dotyczące wersji systemu Android i iOS w zakresie wdrażania ochrony i zarządzania urządzeniami mobilnymi można znaleźć w Pomocy dla Kaspersky Security for Mobile i Pomocy dla Kaspersky Secure Mobility Management.

Wymagania Serwera administracyjnego

Minimalne wymagania sprzętowe:

- Procesor o częstotliwości taktowania 1 GHz lub wyższej. W przypadku 64-bitowych systemów operacyjnych minimalna częstotliwość taktowania procesora to 1.4 GHz.
- Pamięć RAM: 4 GB.
- Dostępne miejsce na dysku: 10 GB. Jeśli korzystasz z funkcji Zarządzanie lukami i poprawkami, na dysku powinno znajdować się przynajmniej 100 GB wolnego miejsca.

W celu przeprowadzenia zdalnej instalacji w środowiskach chmury, wymagania Serwera administracyjnego i serwera bazy danych tak samo jak wymagania dla fizycznego Serwera administracyjnego (w zależności od ilości urządzeń, którymi chcesz zarządzać).

Wymagania programowe:

- Microsoft® Data Access Components (MDAC) 2.8
- Microsoft Windows® DAC 6.0
- Microsoft Windows Installer 4.5

Obsługiwane są następujące systemy operacyjne:

Do komunikacji międzyprocesowej w systemie operacyjnym musi być dostępny interfejs pętli zwrotnej.

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-bitowy
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (Opcja instalacji) (LTSB) 64-bitowy
- Windows Server 2019 Standard/Datacenter/Core 64-bitowy
- Windows Server 2022 Standard/Datacenter/Core 64-bitowy
- Windows Server 2025 Standard/Datacenter/Core 64-bitowy
- Windows Storage Server 2019 64-bitowy

Obsługiwane są następujące platformy wirtualizacji:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Microsoft Hyper-V Server 2019 64-bitowy
- Microsoft Hyper-V Server 2022 64-bitowy

- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

Obsługiwane są następujące serwery baz danych (można zainstalować na innym urządzeniu):

- Microsoft SQL Server 2016 (wszystkie wersje) 64-bitowy
- Microsoft SQL Server 2017 (wszystkie wersje) na 64-bitowy system Windows/Linux
- Microsoft SQL Server 2019 (wszystkie wersje) na 64-bitowy system Windows/Linux (wymaga dodatkowych działań)
- Microsoft SQL Server 2022 (wszystkie wersje) na 64-bitowy system Windows/Linux
- MySQL 5.7 Community 32-bitowy/64-bitowy
- MySQL Standard Edition 8.0 (wersja 8.0.20 i nowsze) 32-bitowy/64-bitowy
- MySQL Enterprise Edition 8.0 (wersja 8.0.20 i nowsze) 32-bitowy/64-bitowy
- MariaDB 10.5 (kompilacja 10.5.27 i nowsze) 32-bitowe/64-bitowe
- MariaDB Galera Cluster 10.3 32-bitowy/64-bitowy z silnikiem magazynowania InnoDB
- PostgreSQL 13.x 64-bitowy
- PostgreSQL 14.x 64-bitowy
- PostgreSQL 15.x 64-bitowy
- Postgres Pro 13.x Windows/Linux 64-bitowy
- Postgres Pro 14.x Windows/Linux 64-bitowy

Szczegóły i ograniczenia można znaleźć w następującym temacie: Wybieranie DBMS.

SIEM i inne systemy zarządzania informacjami:

- HP (Micro Focus) ArcSight ESM 7.0
- IBM QRadar 7.3
- Splunk 7.1

Wymagania Web Console

Kaspersky Security Center Web Console Server

Minimalne wymagania sprzętowe:

- CPU: 4 rdzenie, częstotliwość taktowania wynosząca 2.5 GHz
- Pamięć RAM: 8 GB
- Dostępne miejsce na dysku: 40 GB

Minimalne wymagania dotyczące certyfikatów Serwera administracyjnego:

- Algorytm podpisu certyfikatu SHA-2
- Minimalna długość klucza 2048

Jeśli musisz ponownie wystawić certyfikat, zapoznaj się z bazą wiedzy Kaspersky Security Center.

Systemy operacyjne obsługiwane przez serwer Kaspersky Security Center Web Console Server

Systemy operacyjne. Microsoft Windows (tylko 64-bitowe wersje) Do komunikacji międzyprocesowej w systemie operacyjnym musi być dostępny interfejs pętli zwrotnej.	Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials/Server Core Windows Server 2016 Standard/Datacenter/Essentials/Server Core (Opcja instalacyjna) (LTSB) Windows Server 2019 Standard/Datacenter/Core Windows Server 2022 Standard/Datacenter/Core Windows Server 2025 Standard/Datacenter/Core Windows Storage Server 2019
Platformy wirtualizacji	VMware vSphere 6.7 VMware vSphere 7.0 VMware vSphere 8.0 Citrix XenServer 7.1 LTSR Citrix XenServer 8.x Parallels Desktop 18 Oracle VM VirtualBox 7.x

Urządzenia klienckie

W przypadku urządzenia klienckiego do korzystania z Kaspersky Security Center Web Console wymagana jest tylko przeglądarka internetowa.

Minimalna rozdzielczość ekranu wynosi 1366x768 pikseli.

Wymagania sprzętowe i programowe urządzenia są takie same, jak wymagania dotyczące przeglądarki używanej do pracy z Kaspersky Security Center Web Console.

Przeglądarki:

- Google Chrome 128.0.6613.120 lub nowsza
- Microsoft Edge w wersji 128.0.2739.67 lub nowszej
- Safari 17.6 dla systemu macOS
- Przeglądarka „Yandex" 24.7.3.1081 lub nowsza
- Wydłużone wsparcie techniczne Mozilla Firefox w wersji 115.14.0 lub nowszej

Wymagania dotyczące serwerów mobilnych

Serwer zarządzania urządzeniami mobilnymi iOS (iOS MDM)

Wymagania sprzętowe:

- Procesor o częstotliwości taktowania 1 GHz lub wyższej. W przypadku 64-bitowych systemów operacyjnych minimalna częstotliwość taktowania procesora to 1.4 GHz.
- Pamięć RAM: 2 GB.
- Dostępne miejsce na dysku: 2 GB.

Wymagania programowe: Microsoft Windows (wersja obsługiwanego systemu operacyjnego jest definiowana przez wymagania Serwera administracyjnego).

Wymagania Konsoli administracyjnej

Wymagania sprzętowe:

- Procesor o częstotliwości taktowania 1 GHz lub wyższej. W przypadku 64-bitowych systemów operacyjnych minimalna częstotliwość taktowania procesora to 1.4 GHz.
- Pamięć RAM: 512 MB.
- Dostępne miejsce na dysku: 1 GB.

Wymagania programowe:

- System operacyjny Microsoft Windows (obsługiwana wersja systemu operacyjnego jest określana przez wymagania Serwera administracyjnego):
  - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials 64-bitowy
  - Windows Server 2016 Standard/Datacenter/Essentials (LTSB) 64-bitowy
  - Windows Server 2019 Standard/Datacenter 64-bitowy

    - Windows Server 2022 Standard/Datacenter 64-bitowy
    - Windows Server 2025 Standard/Datacenter/Core 64-bitowy
    - Windows Storage Server 2019 64-bitowy
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 11.0 działająca na systemach:
    - Microsoft Windows Server 2012 R2
    - Microsoft Windows Server 2016
    - Microsoft Windows Server 2019
    - Microsoft Windows Storage Server 2019
- Microsoft Edge działający na Microsoft Windows Server 2022 Standard

Wymagania Agenta sieciowego

Minimalne wymagania sprzętowe:

- Procesor o częstotliwości taktowania 1 GHz lub wyższej. W przypadku 64-bitowych systemów operacyjnych minimalna częstotliwość taktowania procesora to 1.4 GHz.
- Pamięć RAM: 512 MB.
- Dostępne miejsce na dysku: 1 GB.

Wymagania dotyczące oprogramowania dla urządzeń opartych na systemie Linux: musi być zainstalowany interpreter języka Perl w wersji 5.10 lub nowszej.

Systemy operacyjne. Microsoft Windows	Windows Embedded POSReady 2009 z najnowszym pakietem Service Pack 32-bitowy Windows Embedded Standard 7 z dodatkiem Service Pack 1 32-bitowy/64-bitowy Windows Embedded 8.1 Industry Pro 32-bitowy/64-bitowy Windows 10 Enterprise 2015 LTSB 32-bitowy/64-bitowy Windows 10 Enterprise 2016 LTSB 32-bitowy/64-bitowy Windows 10 IoT Enterprise 2015 LTSB 32-bitowy/64-bitowy Windows 10 IoT Enterprise 2016 LTSB 32-bitowy/64-bitowy Windows 10 Enterprise 2019 LTSC 32-bitowy/64-bitowy Windows 10 IoT Enterprise version 1703 32-bitowy/64-bitowy Windows 10 IoT Enterprise version 1709 32-bitowy/64-bitowy Windows 10 IoT Enterprise version 1803 32-bitowy/64-bitowy Windows 10 IoT Enterprise version 1809 32-bitowy/64-bitowy Windows 10 20H2 IoT Enterprise 32-bitowy/64-bitowy Windows 10 21H2 IoT Enterprise 32-bitowy/64-bitowy Windows 10 IoT Enterprise 32-bitowy/64-bitowy Windows 10 IoT Enterprise version 1909 32-bitowy/64-bitowy Windows 10 IoT Enterprise LTSC 2021 32-bitowy/64-bitowy Windows 10 IoT Enterprise version 1607 32-bitowy/64-bitowy Windows 10 TH1 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 TH2 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 RS1 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 RS2 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 RS3 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 RS4 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 RS5 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 RS6 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 19H1 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 10 20H1 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 20H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 21H1 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 21H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Windows 10 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-bitowy/64-bitowy Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM 64-bitowy Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64-bitowy Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bitowy Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bitowy Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bitowy Windows 8 Pro/Enterprise 32-bitowy/64-bitowy Windows 8.1 Pro/Enterprise 32-bitowy/64-bitowy Windows 7 Home/Pro/Enterprise/Ultimate z dodatkiem Service Pack 1 32-bitowy/64-bitowy Microsoft Windows XP Professional z Service Pack 2 32-bitowy/64-bitowy (obsługiwany tylko przez Agenta sieciowego w wersji 10.5.1781, o który można poprosić za pośrednictwem pomocy technicznej) Windows XP Professional z dodatkiem Service Pack 3 i nowszym 32-bitowym (obsługiwany przez Agenta sieciowego w wersji 14.0.0.20023) Windows XP Professional dla systemów wbudowanych z dodatkiem Service Pack 3 32-bitowy (obsługiwany przez Agenta sieciowego w wersji 14.0.0.20023) Windows MultiPoint Server 2011 Standard/Premium 64-bitowy Windows Server 2003 SP1 32-bitowy/64-bitowy (obsługiwany tylko przez Agenta sieciowego w wersji 10.5.1781) Windows Server 2003 SP2 Standard/Enterprise 32-bitowy/64-bitowy (obsługiwany tylko przez Agenta sieciowego w wersji 10.5.1781) Windows Server 2003 R2 Standard/Enterprise z dodatkiem SP2 32-bitowy/64-bitowy (obsługiwany tylko przez Agenta sieciowego w wersji 10.5.1781) Windows Server 2008 Standard/Enterprise/Datacenter z dodatkiem Service Pack 2 32-bitowy/64-bitowy Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation/ z dodatkiem Service Pack 1 i nowszy 64-bitowy

	Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core 64-bitowy Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-bitowy Windows Server 2016 Standard/Datacenter/Essentials/Server Core (Opcja instalacji) (LTSB) 64-bitowy Windows Server 2019 Standard/Datacenter/Core 64-bitowy Windows Server 2019 RS5 Standard/Essentials 64-bitowy Windows Server 2022 Standard/Datacenter/Core 64-bitowy Windows Server 2022 21H2 Standard/Datacenter 64-bitowy Windows Server 2025 Standard/Datacenter/Core 64-bitowy Windows Storage Server 2019 64-bitowy

Systemy operacyjne. Linux	Debian GNU/Linux 10.x (Buster) 32-bitowy/64-bitowy Debian GNU/Linux 11.x (Bullseye) 32-bitowy/64-bitowy Debian GNU/Linux 12 (Bookworm) 32-bitowy/64-bitowy Ubuntu Server 18.04 LTS (Bionic Beaver) 64-bitowy Ubuntu Server 20.04 LTS (Focal Fossa) 64-bitowy Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-bitowy Ubuntu Server 22.04 LTS ARM 64-bitowy Ubuntu Server 24.04 LTS (Noble Numbat) 64-bitowy CentOS 6.7 i nowsze wersje 32-bitowe CentOS 6.x (do 6.6) 32-bitowy/64-bitowy CentOS 7.x 64-bitowy CentOS Stream 8 64-bitowy CentOS Stream 9 64-bitowy CentOS Stream 9 ARM 64-bitowy Red Hat Enterprise Linux Server 6.x 32-bitowy/64-bitowy Red Hat Enterprise Linux Server 7.x 64-bitowy Red Hat Enterprise Linux Server 8.x 64-bitowy Red Hat Enterprise Linux Server 9.x 64-bitowy SUSE Linux Enterprise Server 12 (wszystkie pakiety Service Pack) 64-bitowy SUSE Linux Enterprise Server 15 (wszystkie pakiety Service Pack) 64-bitowy SUSE Linux Enterprise Server 15 (wszystkie pakiety Service Pack) ARM 64-bitowy openSUSE 15 64-bitowy EulerOS 2.0 SP10 64-bitowy EulerOS 2.0 SP10 ARM 64-bitowy Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.5), 64-bit Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.6) 64-bitowy Astra Linux Special Edition RUSB.10015-16 (wydanie 1) (aktualizacja operacyjna 1.6) 64-bitowy Astra Linux Special Edition RUSB.10015-17 (aktualizacja operacyjna 1.7.3) 64-bitowy Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.7) 64-bitowy Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.8) 64-bitowy Astra Linux Special Edition RUSB.10015-37 (aktualizacja operacyjna 7.7) 64-bitowy Astra Linux Special Edition RUSB.10152-02 (aktualizacja operacyjna 4.7) ARM 64-bitowy Astra Linux Common Edition (aktualizacja operacyjna 2.12) 64-bitowy ALT Workstation 10.1 64-bitowy ALT Server 10.1 64-bitowy ALT Education 10.1 64-bitowy ALT SP Server 10 32-bit/64-bitowy ALT SP Server 10 ARM 64-bitowy ALT SP Workstation 10 32-bit/64-bitowy ALT SP Workstation 10 ARM 64-bitowy ALT Server 10 64-bitowy ALT Server 10 ARM 64-bitowy ALT Workstation 10 32-bitowy/64-bitowy ALT 8 SP Workstation (8.4) ARM 64-bitowy ALT 8 SP Server (8.4) ARM 64-bitowy ALT 8 SP Server (LKNV.11100-01) 32-bitowy/64-bitowy ALT 8 SP Server (LKNV.11100-02) 32-bitowy/64-bitowy ALT 8 SP Server (LKNV.11100-03) 32-bitowy/64-bitowy ALT 8 SP Workstation (LKNV.11100-01) 32-bitowy/64-bitowy ALT 8 SP Workstation (LKNV.11100-02) 32-bitowy/64-bitowy ALT 8 SP Workstation (LKNV.11100-03) 32-bitowy/64-bitowy Mageia 4 32-bitowy Oracle Linux 7 64-bitowy Oracle Linux 8 64-bitowy Oracle Linux 9 64-bitowy Linux Mint 20.x 64-bitowy

	Linux Mint 21.1 i nowsze wersje 64-bitowe AlterOS 7.5 i nowszy 64-bitowy GosLinux IC6/7.17 64-bitowy GosLinux IC6/7.2 64-bitowy SberOS 3.3.1 64-bitowy Platform V SberLinux OS Server (SLO) 8.8 64-bitowy Platform V SberLinux OS Server (SLO) 8.9.2 64-bitowy RED OS 7.3 ARM 64-bitowy RED OS 7.3 Server 64-bitowy RED OS 7.3 Certified Edition 64-bitowy RED OS 8 Certified Edition 64-bitowy ROSA Enterprise Linux Server 7.9 64-bitowy ROSA Enterprise Linux Desktop 7.9 64-bitowy ROSA COBALT 7.9 64-bitowy ROSA CHROME 12 64-bitowy AlmaLinux 8 i nowszy 64-bitowy AlmaLinux 9 i nowszy 64-bitowy Rocky Linux 8 i nowszy 64-bitowy Rocky Linux 9 i nowszy 64-bitowy Atlant, kompilacja Alcyone, wersja 2022.02 64-bitowy MSVSPHERE 9.2 SERVER 64-bitowy MSVSPHERE 9.2 ARM 64-bitowy SynthesisM Server 8.6 64-bitowy SynthesisM Client 8.6 64-bitowy OSnova 2.10 64-bitowy Kylin 10 64-bitowy EMIAS 1.0 64-bitowy Amazon Linux 2 64-bitowy MosOS 15.4 Arbat 64-bitowy OS MES (Moscow Electronic School) 64-bitowy
Systemy operacyjne. macOS	Listę obsługiwanych systemów operacyjnych znajdziesz w Pomocy Kaspersky Endpoint Security for Mac.

Dla Agenta sieciowego architektura Apple Silicon (M1) jest także obsługiwana (tak jak Intel).

Obsługiwane są następujące platformy wirtualizacji:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- KVM (maszyna wirtualna oparta na jądrze)

W wersjach systemu Windows starszych niż Microsoft Windows Server 2008 R2 (wersje serwerowe) i Microsoft Windows 7 (wersje na komputery stacjonarne) Agent sieciowy nie obsługuje następujących funkcji:

- Ponowna translacja aktualizacji (używana przez punkty dystrybucji)
- Serwer proxy KSN (używany przez punkty dystrybucji)
- Zadanie wykrywania luk w zabezpieczeniach

Na urządzeniach działających pod kontrolą systemu Microsoft Windows 10 w wersji RS4 lub RS5, Kaspersky Security Center może nie wykrywać niektórych luk w folderach, w których włączono uwzględnianie wielkości liter.

Przed zainstalowaniem Agenta sieciowego na urządzeniach z systemem Windows 7, Windows Server 2008, Windows Server 2008 R2 upewnij się, że została zainstalowana aktualizacja zabezpieczeń KB3063858 dla systemu operacyjnego Windows (Aktualizacja zabezpieczeń dla systemu Windows 7 (KB3063858), Aktualizacja zabezpieczeń dla systemu Windows 7 dla komputerów z procesorem x64 (KB3063858), Aktualizacja zabezpieczeń dla systemu Windows Server 2008 (KB3063858), Aktualizacja zabezpieczeń dla systemu Windows Server 2008 x64 Edition (KB3063858), Aktualizacja zabezpieczeń dla systemu Windows Server 2008 R2 x64 Edition (KB3063858).

W Microsoft Windows XP Agent sieciowy może nie wykonać niektórych działań poprawnie.

Możesz zainstalować lub zaktualizować Agenta sieciowego dla Windows XP tylko w systemie Microsoft Windows XP. Obsługiwane edycje systemu Microsoft Windows XP i odpowiadające im wersje Agenta sieciowego są wymienione na liście obsługiwanych systemów operacyjnych. Z tej strony możesz pobrać wymaganą wersję Agenta sieciowego dla systemu Microsoft Windows XP.

Zalecamy zainstalowanie tej samej wersji Agenta sieciowego co Kaspersky Security Center.

Kaspersky Security Center w pełni obsługuje Agenta sieciowego w tej samej lub nowszej wersji.

Agent sieciowy dla systemu macOS jest dostarczany wraz z aplikacją zabezpieczającą Kaspersky dla tego systemu operacyjnego.

Kompatybilne aplikacje i rozwiązania Kaspersky

Kaspersky Security Center obsługuje scentralizowane wdrażanie i zarządzanie wszystkimi aplikacjami i rozwiązaniami firmy Kaspersky, które są obecnie obsługiwane. Poniższa tabela pokazuje, jakie aplikacje i rozwiązania firmy Kaspersky są obsługiwane przez Konsolę administracyjną opartą na MMC i Kaspersky Security Center Web Console. Aby poznać wersje aplikacji i rozwiązań, odwiedź stronę internetową Product Support Lifecycle.

Nazwa aplikacji lub rozwiązania firmy Kaspersky	Obsługiwane przez Konsolę administracyjną opartą na konsoli MMC	Porty obsługiwane przez Kaspersky Security Center Web Console
Dla stacji roboczych		
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Kaspersky Endpoint Security for Linux Elbrus Edition	✓	✓
Kaspersky Endpoint Security for Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security for Windows	✓	✓
Kaspersky Embedded Systems Security for Linux	–	✓
Do rozwiązań przemysłowych		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks (scentralizowana zdalna instalacja nie jest obsługiwana)	✓	✓
Dla urządzeń mobilnych		
Kaspersky Endpoint Security for Android	✓	✓
Kaspersky Security for iOS	–	✓
Dla serwerów plików		
Kaspersky Security for Windows Server	✓	✓
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Dla środowisk wirtualnych		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	–
Do wykrywania ataków ukierunkowanych		
Kaspersky Sandbox Server	–	✓
Kaspersky Endpoint Detection and Response Optimum	–	✓
Kaspersky Managed Detection and Response	–	✓
Dla urządzeń KasperskyOS		
Kaspersky IoT Secure Gateway	–	✓
Kaspersky Thin Client	–	✓
Bazy danych reputacji		
Kaspersky Private Security Network	–	✓

Licencje i funkcje Kaspersky Security Center 15.1

Kaspersky Security Center wymaga licencji dla niektórych swoich funkcji.

Poniższa tabela wyświetla, które licencje obejmują które funkcje Kaspersky Security Center.

Aby włączyć funkcje Kaspersky Security Center, konieczne jest włączenie Serwera administracyjnego, dodając klucz licencyjny Serwera administracyjnego.

Konieczne jest ręczne dodanie klucza licencyjnego dla każdego Serwera administracyjnego.

Licencje i funkcje Kaspersky Security Center

Funkcje Kaspersky Security Center	Zarządzanie lukami i poprawkami Kaspersky	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise	Kaspersky EDR Optimum
Ocena luk	✓	✓	✓	✓	✓	✓	✓
Zarządzanie poprawkami	✓	–	✓	✓	–	✓	✓
Kontrola dostępu oparta o rolę	✓	✓	✓	✓	✓	✓	✓
Instalacja systemów operacyjnych i aplikacji	✓	–	✓	✓	–	✓	✓
Zarządzanie urządzeniami mobilnymi (czyli zarządzanie urządzeniami iOS i Android użytkowników)	✓	✓	✓	✓	–	–	✓
Configure cloud environment do pracy w środowiskach chmury, takich jak AWS, Microsoft Azure lub Google Cloud	–	–	–	–	✓	✓	–
Eksportowanie zdarzeń do systemów SIEM: Syslog	✓	✓	✓	✓	✓	✓	✓
Eksportowanie zdarzeń do systemów SIEM: QRadar firmy IBM i Micro Focus firmy ArcSight	✓	✓	✓	✓	✓	✓	✓

Informacje o kompatybilności składników Kaspersky Security Center

W poniższej tabeli znajdziesz informacje dotyczące kompatybilności komponentów Kaspersky Security Center.

Kompatybilność składników Kaspersky Security Center

Moduł	Kompatybilny z
Serwer administracyjny Kaspersky Security Center 15.1	• Konsola administracyjna Kaspersky Security Center 15.1. • Kaspersky Security Center 15.1 Web Console. • Agent sieciowy Kaspersky Security Center w następujących wersjach: 16.3, 16.2, 16.1, 16, 15.4, 15.1, 15, 14.2, 14.

Moduł	Kompatybilny z
Kaspersky Security Center 15.1 Web Console	Serwer administracyjny Kaspersky Security Center w następujących wersjach: 15.1 i 14.2.
Główny Serwer administracyjny Kaspersky Security Center 15.1	Podrzędne Serwery administracyjne: • Kaspersky Security Center Windows w następujących wersjach: 14, 14.2, 15.1 • Kaspersky Security Center Linux w następujących wersjach: 14.2, 15, 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2, 16.3
Podrzędny Serwer administracyjny Kaspersky Security Center 15.1	Główny Serwery administracyjny: • Kaspersky Security Center Windows w następujących wersjach: 14, 14.2, 15.1 • Kaspersky Security Center Linux w następujących wersjach: 14.2, 15, 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2, 16.3

Zalecamy korzystanie z najnowszej wersji Serwera administracyjnego Kaspersky Security Center i Kaspersky Security Center Web Console. W przeciwnym razie funkcjonalność Kaspersky Security Center może być ograniczona. Możesz niezależnie zainstalować i uaktualnić Serwer administracyjny Kaspersky Security Center i Kaspersky Security Center Web Console. W takim przypadku, musisz upewnić się, że wersja zainstalowanej konsoli Kaspersky Security Center Web Console jest zgodna z wersją Serwera administracyjnego, z którym się łączysz.

Jeśli posiadasz najnowszą wersję Kaspersky Security Center Web Console i poprzednią wersję Kaspersky Security Center i podczas uwierzytelniania domeny wystąpi błąd, tekst błędu będzie zawierał domyślny komunikat.

Porównanie Kaspersky Security Center: opartego na systemie Windows i opartego na systemie Linux

Kaspersky dostarcza Kaspersky Security Center jako rozwiązanie lokalne dla dwóch platform — Windows i Linux. W rozwiązaniu opartym na systemie Windows Serwer administracyjny jest instalowany na urządzeniu z systemem Windows, a rozwiązanie oparte na systemie Linux ma wersję Serwera administracyjnego zaprojektowaną do zainstalowania na urządzeniu z systemem Linux. Ta pomoc online zawiera informacje o Kaspersky Security Center Windows. Szczegółowe informacje na temat rozwiązania opartego na systemie Linux można znaleźć w Pomocy online Kaspersky Security Center Linux.

Poniższa tabela umożliwia porównanie głównych funkcji Kaspersky Security Center jako rozwiązania opartego na systemie Windows i jako rozwiązania opartego na systemie Linux.

Porównanie funkcji Kaspersky Security Center działającego jako rozwiązanie oparte na systemie Windows i rozwiązanie oparte na systemie Linux

Funkcja lub właściwość	Kaspersky Security Center	
	Rozwiązanie oparte na systemie Windows	Rozwiązanie oparte na systemie Linux
Serwer administracyjny		
Lokalizacja systemu zarządzania bazą danych (DBMS)	Lokalnie	Lokalnie (Microsoft SQL nie jest obsługiwany)
System operacyjny do zainstalowania Serwera administracyjnego	Windows	Linux
Hierarchia Serwerów administracyjnych	✓	✓
Obsługa wirtualnych Serwerów administracyjnych	✓	✓

Funkcja lub właściwość	Kaspersky Security Center	
	Rozwiązanie oparte na systemie Windows	Rozwiązanie oparte na systemie Linux
Używanie SNMP do wysyłania statystyk Serwera administracyjnego do aplikacji innych firm	✓	Do wdrożenia w 2026 roku
Serwer sieciowy do publikowania pakietów instalacyjnych i innych plików	✓	✓
Instalowanie Serwera administracyjnego na jednolokalizacyjnym klastrze trybu failover Windows Server	✓	—
Wdrażanie klastra trybu failover Kaspersky Security Center	✓ Dotyczy to tylko klastra jednolokalizacyjnego	✓ Począwszy od wersji 16.2 Kaspersky Security Center Linux, geograficznie rozproszony klaster trybu failover jest obsługiwany
Konsola administracyjna		
Typ Konsoli administracyjnej	Oparte na MMC i oparte na sieci Web	Internetowe
System operacyjny do zainstalowania konsoli administracyjnej opartej na sieci Web	Windows lub Linux	Linux
Zaloguj się do konsoli, korzystając z uwierzytelniania domeny	✓	✓ Pojedyncze logowanie nie jest obsługiwane w wersjach 15.1–15.4 (włącznie)
Zarządzanie urządzeniami klienckimi i grupami administracyjnymi		
Maksymalna liczba zarządzanych urządzeń (na jeden Serwer administracyjny)	100 000	50 000 (z PostgreSQL i Postgres Pro)
Przeszukiwanie sieci	✓	✓ Od wersji 16 obsługiwane są kontrolery domeny FreeIPA i ALD Pro
Ochrona urządzeń zarządzanych przez systemy Windows, macOS i Linux	✓	✓
Ochrona urządzeń mobilnych	✓ Podstawowe zarządzanie urządzeniami mobilnymi	✓ MDM i korzystanie z funkcjonalności Kaspersky Secure Mobility Management (w ramach licencji)
Zarządzenie ochroną maszyn wirtualnych	✓	✓
Ochrona infrastruktury chmury publicznej	✓	—
Zdalne połączenie z pulpitem urządzenia klienckiego	✓	✓ Od wersji 15.3
Szyfrowanie i ochrona danych	✓	✓ (Na zarządzanych urządzeniach z systemem Windows, na których zainstalowano Kaspersky Endpoint Security for Windows lub Kaspersky Endpoint Security for Mac)
Wsparcie klastrów i macierzy serwerów w grupach administracyjnych	✓	✓
Hierarchia Grupy administracyjnej	✓	✓
Dodawanie bramy połączenia w strefie DMZ jako punktu dystrybucji	✓ (Konsola administracyjna opartą na MMC)	Do wdrożenia w 2026 roku
Praca z użytkownikami		
Tworzenie i zarządzanie kontami użytkowników	✓	✓
Zarządzanie aplikacjami Kaspersky		
Zasady aplikacji	✓	✓
Zadania dla aplikacji Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
KSN Proxy	✓	✓

Funkcja lub właściwość	Kaspersky Security Center	
	Rozwiązanie oparte na systemie Windows	Rozwiązanie oparte na systemie Linux
Kaspersky Private Security Network	✓	✓
Centralne wdrażanie kluczy licencyjnych dla aplikacji Kaspersky	✓	✓
Zdalna diagnostyka urządzeń klienckich	✓	✓
Automatyczna aktualizacja aplikacji Kaspersky	✓	✓
Obsługa adaptacyjnej kontroli anomalii	✓	✓
Zarządzanie bezpieczeństwem zorientowane na urządzenie	✓	✓
Zarządzanie bezpieczeństwem zorientowane na użytkownika	✓	✓
Zarządzanie systemami		
Wdrażanie systemów operacyjnych na urządzeniach klienckich	✓	—
Zarządzanie licencjami stron trzecich	✓	—
Używanie Serwera administracyjnego jako serwera WSUS	✓	✓ (tylko w trybie pasywnego wyszukiwania w usłudze Windows Update)
Zarządzanie aplikacjami firm trzecich na urządzeniach klienckich		
Instalowanie aktualizacji oprogramowania innych firm i usuwanie luk w zabezpieczeniach oprogramowania innych firm	✓	✓
Monitorowanie, raportowanie i audyt		
Zarządzanie rewizjami obiektów	✓	✓
Porównanie rewizji zasad	✓	Do wdrożenia w 2026 roku
Wyświetlanie i praca z alertami wykrytymi przez Kaspersky Endpoint Detection and Response Optimum	✓	✓
Powiadomienia o zdarzeniach, które wystąpiły na zarządzanych urządzeniach	✓	✓
Monitorowanie statusu zasad i status zadań	✓	✓
Integracje		
Integracja z Kaspersky Managed Detection and Response	✓	✓
Integracja z systemami SIEM	✓	✓
Eksportowanie zdarzeń przy użyciu formatów CEF i LEEF	✓	✓
Agregowanie alertów i wykonywanie działań reagowania za pośrednictwem usługi Active Directory, KASAP i Kaspersky TIP Sandbox	—	✓ (począwszy od wersji 15.4) Musisz aktywować Serwer administracyjny w ramach licencji Kaspersky Next XDR Optimum, a następnie zainstalować klucz licencyjny Kaspersky Next XDR Optimum w Twoich zarządzanych aplikacjach

Informacje o Kaspersky Next Expert View

Używanie Kaspersky Security Center jako lokalnej aplikacji oznacza zainstalowanie Kaspersky Security Center, w tym Serwera administracyjnego, na urządzeniu lokalnym i zarządzanie systemem ochrony sieci za pośrednictwem Konsoli administracyjnej opartej o konsolę Microsoft Management Console (dostępnej wyłącznie w Kaspersky Security Center Windows) lub Kaspersky Security Center Web Console.

Jednakże możesz użyć Kaspersky Security Center jako usługi w chmurze. W tym przypadku Kaspersky Security Center jest instalowany i utrzymywany dla Ciebie przez ekspertów z Kaspersky w środowisku chmury, a Kaspersky zapewnia dostęp do Serwera administracyjnego jako usługi. Systemem ochrony sieci zarządza się za pośrednictwem działającej w chmurze Konsoli administracyjnej o nazwie Kaspersky Next Expert View. Ta konsola posiada interfejs podobny do interfejsu Kaspersky Security Center Web Console.

Interfejs i dokumentacja Kaspersky Next Expert View są dostępne w następujących językach:

- angielskim
- francuskim
- niemieckim
- włoskim
- japońskim
- portugalskim (Brazylijski)
- rosyjskim
- Chiński uproszczony
- hiszpańskim
- hiszpańskim (LATAM)
- Chiński tradycyjny

Więcej informacji o Kaspersky Next Expert View i jego funkcjach można znaleźć w dokumentacji Kaspersky Next Expert View oraz w dokumentacji Kaspersky Endpoint Security for Business.

Kaspersky Security Center 15.1

Ta sekcja zawiera informacje na temat korzystania z Kaspersky Security Center 15.1.

Informacje dostępne w pomocy online mogą różnić się od informacji w dokumentacji dołączonej do aplikacji. W tym przypadku, system pomocy online jest uznawany za aktualny. Internetowy system pomocy można otworzyć, klikając odnośniki w interfejsie aplikacji lub klikając odpowiedni odnośnik w dokumentacji. Internetowy system pomocy może być aktualizowany bez wcześniejszego powiadamiania o tym fakcie. W razie potrzeby możesz przełączać się między pomocą online i pomocą offline.

Podstawowe pojęcia

Ta sekcja wyjaśnia podstawowe pojęcia związane z Kaspersky Security Center.

Serwer administracyjny

Komponenty Kaspersky Security Center umożliwiają zdalne zarządzanie aplikacjami firmy Kaspersky zainstalowanymi na urządzeniach klienckich.

Urządzenia z zainstalowanym komponentem Serwer administracyjny będą nazywane *Serwerami administracyjnymi* (zwane również *Serwerami*). Serwery administracyjne muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

Serwer administracyjny jest instalowany na urządzeniu jako usługa z następującym zestawem atrybutów:

- Nosi nazwę „Serwer administracyjny Kaspersky Security Center”
- Ustawiony do automatycznego uruchamiania po załadowaniu systemu operacyjnego
- Posiada konto **SystemLokalny** lub konto użytkownika wybrane podczas instalacji Serwera administracyjnego

Serwer administracyjny pełni następujące funkcje:

- Przechowuje strukturę grup administracyjnych
- Przechowuje informacje o konfiguracji urządzeń klienckich
- Organizuje repozytoria dla pakietów dystrybucyjnych aplikacji
- Służy do zdalnej instalacji aplikacji na urządzeniach klienckich oraz do usuwania aplikacji
- Aktualizuje bazy danych i moduły aplikacji firmy Kaspersky
- Zarządza zasadami i zadaniami na urządzeniach klienckich
- Przechowuje informacje o zdarzeniach, które wystąpiły na urządzeniach klienckich

- Generuje raporty z działania aplikacji Kaspersky
- Wdraża klucze licencyjne na urządzenia klienckie oraz przechowuje informacje o kluczach licencyjnych
- Wysyła komunikaty o postępie zadań (na przykład o wykryciu wirusów na urządzeniu klienckim)

Nadawanie nazw Serwerom administracyjnym w interfejsie aplikacji

W interfejsie Konsoli administracyjnej opartej na MMC i w konsoli Kaspersky Security Center Web Console Serwery administracyjne mogą posiadać następujące nazwy:

- Nazwę urządzenia z Serwerem administracyjny, na przykład: „*nazwa_urządzenia*" lub „Serwer administracyjny: *nazwa_urządzenia*".
- Adres IP urządzenia z Serwerem administracyjny, na przykład: „*adres_IP*" lub „Serwer administracyjny: *adres_IP*".
- Podrzędne Serwery administracyjne i wirtualne Serwery administracyjne posiadają niestandardowe nazwy, które określasz podczas podłączania wirtualnego lub podrzędnego Serwera administracyjnego do głównego Serwera administracyjnego.
- Jeśli używasz konsoli Kaspersky Security Center Web Console zainstalowanej na urządzeniu z systemem Linux, aplikacja wyświetli nazwy Serwerów administracyjnych, które określiłeś jako zaufane w pliku odpowiedzi.

Możesz nawiązać połączenie z Serwerem administracyjnym poprzez Konsolę administracyjną lub Kaspersky Security Center Web Console.

Hierarchia Serwerów administracyjnych

Serwery administracyjne można zorganizować w hierarchię. Każdy Serwer administracyjny może mieć kilka podrzędnych Serwerów administracyjnych (zwanych *Serwerami podrzędnymi*) na różnych poziomach zagnieżdżenia w obrębie hierarchii. Poziom zagnieżdżenia Serwerów podrzędnych nie jest ograniczony. Grupy administracyjne głównego Serwera administracyjnego będą obejmować urządzenia klienckie wszystkich podrzędnych Serwerów administracyjnych. Z tego powodu odizolowane i niezależne sekcje sieci mogą być zarządzane przez różne Serwery administracyjne, które z kolei są zarządzane przez Serwer główny.

Wirtualne Serwery administracyjne są szczególnym przypadkiem podrzędnych Serwerów administracyjnych.

Hierarchii Serwerów administracyjnych można użyć w celu:

- Zmniejszenia obciążenia na Serwerze administracyjnym (w porównaniu do pojedynczego Serwera działającego dla całej sieci).
- Zmniejszenia ruchu w sieci wewnętrznej i uproszczenia pracy ze zdalnymi komputerami firmowymi. Nie ma konieczności nawiązywania połączenia pomiędzy głównym Serwerem administracyjnym a wszystkimi urządzeniami sieciowymi, które mogą znajdować się, na przykład, w innych regionach. W każdym segmencie sieci wystarczy zainstalować podrzędny Serwer administracyjny, przydzielić urządzenia do grup administracyjnych Serwerów podrzędnych i ustanowić połączenia między Serwerami podrzędnymi a Serwerem głównym na kanałach szybkiej komunikacji.

- Rozdzielenia obowiązków pomiędzy administratorami ochrony antywirusowej. Wszystkie możliwości scentralizowanego zarządzania i monitorowania stanu ochrony antywirusowej w sieciach korporacyjnych pozostają dostępne.

- Korzystaj z Kaspersky Security Center przez dostawców usług. Dostawca usługi musi tylko zainstalować Kaspersky Security Center i Kaspersky Security Center Web Console. Aby zarządzać dużą liczbą urządzeń klienckich różnych organizacji, dostawca usług może dodać pomocnicze Serwery administracyjne (w tym Serwery wirtualne) do hierarchii Serwerów administracyjnych.

Każde urządzenie wchodzące w skład hierarchii grup administracyjnych może być podłączone tylko do jednego Serwera administracyjnego. Należy monitorować połączenia urządzeń z Serwerami administracyjnymi. Użyj funkcji wyszukiwania urządzeń w grupach administracyjnych różnych Serwerów w oparciu o atrybuty sieciowe.

Wirtualny Serwer administracyjny

Wirtualny Serwer administracyjny (zwany również *Serwerem wirtualnym*) jest to moduł z Kaspersky Security Center służący do zarządzania ochroną antywirusową sieci organizacji klienta.

Wirtualny Serwer administracyjny jest szczególnym przypadkiem podrzędnego Serwera administracyjnego i ma następujące ograniczenia w porównaniu z fizycznym Serwerem administracyjnym:

- Wirtualny Serwer administracyjny można utworzyć tylko na głównym Serwerze administracyjnym.

- Podczas działania wirtualny Serwer administracyjny używa bazy danych głównego Serwera administracyjnego. Zadania tworzenia kopii zapasowych i przywracania danych, a także zadania pobierania i skanowania aktualizacji nie są obsługiwane na wirtualnym Serwerze administracyjnym.

- Serwer wirtualny nie obsługuje tworzenia podrzędnych Serwerów administracyjnych (łącznie z Serwerami wirtualnymi).

Dodatkowo, wirtualny Serwer administracyjny posiada następujące ograniczenia:

- W oknie właściwości wirtualnego Serwera administracyjnego ograniczona jest liczba sekcji.

- Aby zdalnie zainstalować aplikacje firmy Kaspersky na urządzeniach klienckich zarządzanych przez wirtualny Serwer administracyjny, upewnij się, że Agent sieciowy jest zainstalowany na jednym z urządzeń klienckich w celu zapewnienia komunikacji z wirtualnym Serwerem administracyjnym. Przy pierwszym połączeniu z wirtualnym Serwerem administracyjnym to urządzenie jest automatycznie przypisywane jako punkt dystrybucji, pełniąc rolę bramy połączenia pomiędzy urządzeniami klienckimi a wirtualnym Serwerem administracyjnym.

- Serwery wirtualne mogą odpytywać sieć wyłącznie za pośrednictwem punktów dystrybucji.

- Aby uruchomić ponownie nieprawidłowo działający Serwer wirtualny, Kaspersky Security Center uruchamia ponownie główny Serwer administracyjny i wszystkie wirtualne Serwery administracyjne.

- Użytkownikom utworzonym na Serwerze wirtualnym nie można przypisać roli na Serwerze administracyjnym.

Administrator wirtualnego Serwera administracyjnego posiada wszystkie uprawnienia na tym konkretnym Serwerze wirtualnym.

Serwer urządzeń mobilnych

Serwer urządzeń mobilnych jest to składnik Kaspersky Security Center umożliwiający dostęp do urządzeń mobilnych i zarządzanie nimi za pośrednictwem Konsoli administracyjnej. Serwer urządzeń mobilnych gromadzi informacje o urządzeniach mobilnych i przechowuje ich profile.

Kaspersky Security Center zawiera serwer iOS MDM pełniący funkcję serwera urządzeń mobilnych. Ten serwer urządzeń mobilnych jest używany do zarządzania urządzeniami mobilnymi, które obsługują usługę Apple® Push Notification (APNs).

Serwery urządzeń mobilnych Kaspersky Security Center umożliwiają zarządzanie następującymi obiektami:

- Pojedynczym urządzeniem mobilnym.
- Kilkoma urządzeniami mobilnymi.
- Kilkoma urządzeniami mobilnymi podłączonymi do klastra serwerów jednocześnie. Po podłączeniu do klastra serwerów, serwer urządzeń mobilnych, zainstalowany na tym klastrze, jest wyświetlany w Konsoli administracyjnej jako pojedynczy serwer.

Serwer sieciowy

Kaspersky Security Center *Web Server* (zwany również *serwer sieciowy, serwer WWW*) jest składnikiem Kaspersky Security Center, który jest instalowany wraz z Serwerem administracyjnym. Serwer WWW został zaprojektowany do przesyłania za pośrednictwem sieci autonomicznych pakietów instalacyjnych, profili iOS MDM oraz plików z folderu współdzielonego.

Po utworzeniu autonomicznego pakietu instalacyjnego, jest on automatycznie publikowany na serwerze sieciowym. Odnośnik do pobrania pakietu autonomicznego jest wyświetlany na liście utworzonych autonomicznych pakietów instalacyjnych. Jeśli jest to konieczne, możesz anulować publikację pakietu autonomicznego lub opublikować go ponownie na serwerze sieciowym.

Po utworzeniu profilu iOS MDM dla urządzenia mobilnego użytkownika, zostanie on również automatycznie opublikowany na serwerze sieciowym. Opublikowany profil jest automatycznie usuwany z serwera WWW, jak tylko zostanie pomyślnie zainstalowany na urządzeniu mobilnym użytkownika.

Folder współdzielony jest używany do przechowywania informacji dostępnych dla wszystkich użytkowników, których urządzenia są zarządzane poprzez Serwer administracyjny. Jeśli użytkownik nie ma bezpośredniego dostępu do folderu współdzielonego, nie może uzyskać informacji z folderu przy pomocy serwera sieciowego.

Aby udostępnić użytkownikom informacje z folderu współdzielonego przy pomocy serwera WWW, administrator musi utworzyć w folderze współdzielonym podfolder o nazwie "public" i wkleić do niego odpowiednie informacje.

Składnia odnośnika do przesłania informacji wygląda następująco:

```
https://<Web Server name>:<HTTPS port>/public/<object>
```

gdzie:

- `<Web Server name>` to nazwa serwera sieciowego Kaspersky Security Center Web Server.
- `<HTTPS port>` to port HTTPS serwera sieciowego, który został zdefiniowany przez Administratora. Port HTTPS można ustawić w sekcji **Serwer WWW** okna właściwości Serwera administracyjnego. Domyślny numer portu to 8061.
- `<object>` to podfolder lub plik, do którego użytkownik posiada dostęp.

Administrator może wysłać użytkownikowi nowy odnośnik w dowolny sposób, na przykład za pośrednictwem poczty elektronicznej.

Klikając odnośnik, użytkownik może pobrać żądane informacje na urządzenie lokalne.

Agent sieciowy

Interakcja między Serwerem administracyjnym a urządzeniami odbywa się przy użyciu komponentu *Agent sieciowy* programu Kaspersky Security Center. Agent sieciowy powinien być zainstalowany na wszystkich urządzeniach, na których do zarządzania aplikacjami Kaspersky wykorzystywany jest Kaspersky Security Center.

Agent sieciowy jest instalowany na urządzeniu jako usługa z następującym zestawem atrybutów:

- Nosi nazwę „Agent sieciowy Kaspersky Security Center"
- Ustawiony do automatycznego uruchamiania po załadowaniu systemu operacyjnego
- Korzysta z konta LocalSystem

Urządzenie, na którym jest zainstalowany Agent sieciowy, nazywa się *zarządzane urządzenie* lub *urządzenie*.

Agent sieciowy może zostać zainstalowany na urządzeniu z systemem Windows, Linux lub Mac. Możesz uzyskać komponent z jednego z następujących zasobów:

- Pakiet instalacyjny w magazynie Serwera administracyjnego (należy posiadać zainstalowany Serwer administracyjny)
- Pakiet instalacyjny znajduje się na serwerach sieciowych Kaspersky

Nie musisz instalować Agenta sieciowego na urządzeniu, na którym instalujesz Serwer administracyjny, ponieważ wersja serwerowa Agenta sieciowego jest automatycznie instalowana wraz z Serwerem administracyjnym.

Nazwa procesu, który jest uruchamiany przez Agenta sieciowego, to *klnagent.exe*.

Agent sieciowy synchronizuje zarządzane urządzenie z Serwerem administracyjnym. Zalecane jest ustawienie okresu synchronizacji (zwanego także *puls*) na 15 minut dla 10 000 zarządzanych urządzeń.

Grupy administracyjne

Grupa administracyjna (zwana dalej również *grupą*) jest logicznym zestawem zarządzanych urządzeń połączonych na podstawie pewnych cech w celu zarządzania pogrupowanymi urządzeniami jako pojedynczą jednostką w obrębie Kaspersky Security Center.

Wszystkie zarządzane urządzenia w danej grupie administracyjnej są tak skonfigurowane, aby:

- Używać tych samych ustawień aplikacji (które można określić w zasadach grupy).
- Używaj wspólnego trybu działania dla wszystkich aplikacji poprzez tworzenie zadań grupowych z określonymi ustawieniami. Przykłady zadań grupowych obejmują tworzenie i instalowanie takich samych pakietów instalacyjnych, aktualizowanie baz danych i modułów aplikacji, skanowanie urządzenia na żądanie i włączanie ochrony w czasie rzeczywistym.

Zarządzane urządzenie może należeć tylko do jednej grupy administracyjnej.

Możesz tworzyć hierarchie o dowolnym poziomie zagnieżdżenia Serwerów administracyjnych i grup. Pojedynczy poziom hierarchii może zawierać podrzędne i wirtualne Serwery administracyjne, grupy i zarządzane urządzenia. Możesz przenosić urządzenia z jednej grupy do innej bez przenoszenia ich fizycznie. Na przykład, jeśli pozycja pracownika w firmie zmieni się z księgowego na dewelopera, możesz przenieść urządzenie tego pracownika z grupy administracyjnej Księgowi do grupy administracyjnej Deweloperzy. Następnie urządzenie automatycznie pobierze ustawienia aplikacji wymagane dla deweloperów.

Zarządzane urządzenie

Zarządzane urządzenie to urządzenie z systemem Windows, Linux lub macOS, na którym zainstalowany jest Agent sieciowy, lub urządzenie mobilne, na którym zainstalowana jest aplikacja zabezpieczająca Kaspersky. Możesz zarządzać takimi urządzeniami poprzez utworzenie zadań i zasad dla aplikacji zainstalowanych na tych urządzeniach. Możesz także otrzymywać raporty z zarządzanych urządzeń.

Możesz sprawić, że zarządzane urządzenie niemobilne będzie działało jako punkt dystrybucji oraz jako brama połączenia.

Urządzenie może być zarządzane tylko przez jeden Serwer administracyjny. Jeden Serwer administracyjny może obsługiwać maksymalnie 100 000 urządzeń, w tym urządzenia mobilne.

Urządzenie nieprzypisane

Urządzenie nieprzypisane to urządzenie w sieci, które nie zostało uwzględnione w żadnej grupie administracyjnej. Na nieprzypisanych urządzeniach możesz wykonać różne działania, na przykład, przenieść je do grup administracyjnych lub zainstalować na nich aplikacje.

Jeśli nowe urządzenie zostanie wykryte w sieci, to urządzenie zostanie umieszczone w grupie administracyjnej **Urządzenia nieprzypisane**. Możesz skonfigurować reguły dla urządzeń, aby po wykryciu były przenoszone automatycznie do innych grup administracyjnych.

Stacja robocza administratora

Stacja robocza administratora to urządzenie, na którym zainstalowana jest konsola administracyjna lub które używane jest do otwierania Kaspersky Security Center Web Console. Administratorzy mogą używać tych urządzeń do scentralizowanego zdalnego zarządzania aplikacjami Kaspersky zainstalowanymi na urządzeniach klienckich.

Po zainstalowaniu Konsoli administracyjnej na urządzeniu, pojawi się jej ikona i będzie można jej użyć do uruchomienia Konsoli administracyjnej. Odszukaj ją w menu **Start** → **Programy** → **Kaspersky Security Center**.

Liczba stacji roboczych administratora jest nieograniczona. Z każdej stacji roboczej administratora możesz jednocześnie zarządzać grupami administracyjnymi kilku Serwerów administracyjnych w sieci. Możesz połączyć stację roboczą administratora z Serwerem administracyjnym (fizycznym lub wirtualnym) znajdującym się na dowolnym poziomie hierarchii.

Możesz dodać stację roboczą administratora do grupy administracyjnej jako urządzenie klienckie.

W obrębie grup administracyjnych dowolnego Serwera administracyjnego to samo urządzenie może funkcjonować jako klient Serwera administracyjnego, Serwer administracyjny lub stacja robocza administratora.

Wtyczka administracyjna

Aplikacje firmy Kaspersky są zarządzane poprzez Konsolę administracyjną przy użyciu dedykowanego komponentu o nazwie *wtyczka administracyjna*. Każda aplikacja firmy Kaspersky, która może zostać zarządzana poprzez Kaspersky Security Center, zawiera wtyczkę zarządzającą.

Przy pomocy wtyczki zarządzającej można wykonywać następujące czynności w Konsoli administracyjnej:

- Tworzyć i modyfikować zasady i ustawienia aplikacji, jak również ustawienia zadań aplikacji.
- Uzyskiwać informacje o zadaniach aplikacji, zdarzeniach występujących w trakcie jej pracy oraz statystyki z działania aplikacji odebrane od urządzeń klienckich.

Wtyczki do zarządzania można pobrać ze strony pomocy technicznej Kaspersky.

Webowa wtyczka administracyjna

Specjalny składnik — *webowa wtyczka administracyjna* — jest używany do zdalnego administrowania oprogramowaniem Kaspersky przy użyciu Kaspersky Security Center Web Console. W dalszej części dokumentu webowa wtyczka zarządzająca jest zwana również *wtyczką zarządzającą*. Wtyczka zarządzająca to interfejs między Kaspersky Security Center Web Console a określoną aplikacją firmy Kaspersky. Korzystając z wtyczki zarządzającej, możesz skonfigurować zadania i zasady dla aplikacji.

Webową wtyczkę administracyjna można pobrać ze strony internetowej Kaspersky.

Wtyczka zarządzająca oferuje:

- Interfejs do tworzenia i edytowania zadań i ustawień aplikacji
- Interfejs do tworzenia i edytowania zasad i profili zasad do zdalnej i scentralizowanej konfiguracji aplikacji Kaspersky i urządzeń
- Przesyłanie zdarzeń wygenerowanych przez aplikację
- Funkcje Kaspersky Security Center Web Console do wyświetlania danych operacyjnych i zdarzeń aplikacji, a także statystyk przekazanych z urządzeń klienckich

Zasady

Zasada to zbiór ustawień aplikacji Kaspersky, które są stosowane do grupy administracyjnej i jej podgrup. Możesz zainstalować kilka aplikacji Kaspersky na urządzeniach należących do grupy administracyjnej. Kaspersky Security Center zapewnia jedną zasadę dla każdej aplikacji Kaspersky w grupie administracyjnej. Zasada ma jeden z następujących stanów (patrz poniższa tabela):

Stan zasady

Stan	Opis
Aktywny	Bieżąca zasada, która jest stosowana do urządzenia. W każdej grupie administracyjnej dla aplikacji Kaspersky może być aktywna tylko jedna zasada. Urządzenia stosują wartości ustawień aktywnej zasady aplikacji Kaspersky.
Nieaktywna	Zasada, która nie jest obecnie stosowana do urządzenia.
Profil użytkownika mobilnego	Jeżeli ta opcja jest zaznaczona, zasada stanie się aktywna, gdy urządzenie znajdzie się poza siecią korporacyjną.

Zasady działają zgodnie z następującymi regułami:

- Dla jednej aplikacji można skonfigurować kilka zasad z różnymi wartościami.
- Tylko jedna zasada może być aktywna dla bieżącej aplikacji.
- Możesz aktywować nieaktywną zasadę, gdy wystąpi określone zdarzenie. Na przykład możesz wymusić bardziej rygorystyczne ustawienia ochrony antywirusowej podczas epidemii wirusów.
- Zasada może mieć zasady podrzędne.

Zazwyczaj można używać zasad w celu przygotowania się na sytuacje awaryjne, takie jak atak wirusa. Na przykład, jeśli wystąpi atak za pośrednictwem dysków flash, można aktywować zasadę blokującą dostęp do dysków flash. W takim przypadku bieżąca aktywna zasada automatycznie stanie się nieaktywna.

Aby zapobiec utrzymywaniu wielu zasad, na przykład, gdy przy różnych okazjach zakłada się zmianę tylko kilku ustawień, można użyć profili zasad.

Profil zasad to nazwany podzbiór wartości ustawień zasad, który zastępuje wartości ustawień zasady. Profil zasad wpływa na efektywne tworzenie ustawień na zarządzanym urządzeniu. *Obowiązujące ustawienia* to zbiory ustawień zasad, ustawień profilu zasad i lokalnych ustawień aplikacji, które są aktualnie zastosowane do urządzenia.

Profile zasad działają zgodnie z następującymi regułami:

- Profil zasad zaczyna obowiązywać, gdy wystąpi określony warunek aktywacji.
- Profile zasad zawierają wartości ustawień, które różnią się od ustawień zasad.

- Aktywacja profilu zasad zmienia obowiązujące ustawienia zarządzanego urządzenia.
- Zasada może zawierać maksymalnie 100 profili zasad.

Profile zasad

Czasami konieczne może być utworzenie kilku instancji jednej zasady dla różnych grup administracyjnych; możesz także zmodyfikować ustawienia tych zasad w sposób scentralizowany. Te instancje mogą różnić się jednym lub dwoma ustawieniami. Na przykład, wszyscy księgowi w firmie pracują pod kontrolą tego samej zasady—ale starsi księgowi mogą korzystać z dysków flash, a młodsi księgowi nie mają takich uprawnień. W tym przypadku, zastosowanie zasad do urządzeń tylko poprzez hierarchię grup administracyjnych może być niewygodne.

Aby uniknąć tworzenia kilku instancji jednej zasady, Kaspersky Security Center umożliwia utworzenie *profili zasad*. Profile zasad są niezbędne, jeśli chcesz, żeby urządzenia w jednej grupie administracyjnej były uruchamiane z ustawieniami innych zasad.

Profil zasad jest to inaczej podzbiór ustawień zasady. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z zasadą i uzupełnia ją zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowej" zasady, która jest aktywna na zarządzanym urządzeniu. Aktywacja profilu zmodyfikuje ustawienia „podstawowych" zasad, które były wstępnie aktywne na urządzeniu. Zmodyfikowane ustawienia przyjmują wartości określone w profilu.

Zadania

Kaspersky Security Center zarządza aplikacjami zabezpieczającymi Kaspersky, zainstalowanymi na urządzeniach poprzez tworzenie i uruchamianie *zadań*. Zadania są potrzebne do instalowania, uruchamiania i zatrzymywania działania aplikacji, skanowania plików, aktualizowania baz danych i modułów aplikacji, a także wykonywania innych działań na aplikacjach.

Zadania dla określonej aplikacji mogą być tworzone tylko wtedy, gdy zainstalowana jest wtyczka zarządzająca dla tej aplikacji.

Zadania mogą być wykonywane na Serwerze administracyjnym i na urządzeniach.

Na Serwerze administracyjnym wykonywane są następujące zadania:

- Automatyczne rozsyłanie raportów
- Pobieranie uaktualnień do repozytorium Serwera administracyjnego
- Tworzenie kopii zapasowych danych Serwera administracyjnego
- Obsługa baz danych
- Synchronizacja Windows Update
- Tworzenie pakietów instalacyjnych w oparciu o obraz systemu operacyjnego odpowiedniego urządzenia

Na urządzeniach wykonywane są następujące typy zadań:

- *Zadania lokalne*—zadania wykonywane na określonym urządzeniu

  Zadania lokalne mogą zostać zmodyfikowane przez administratora przy użyciu narzędzi Konsoli administracyjnej lub przez użytkownika zdalnego urządzenia (na przykład, z poziomu interfejsu aplikacji zabezpieczającej). Jeśli zadanie lokalne zostało zmodyfikowane jednocześnie przez administratora i użytkownika zarządzanego urządzenia, zostaną zastosowane zmiany wprowadzone przez administratora, ponieważ mają wyższy priorytet.

- *Zadania grupowe*—zadania wykonywane na wszystkich urządzeniach określonej grupy

  Dopóki nie określono inaczej we właściwościach zadania, zadanie grupowe także wpływa na wszystkie podgrupy wybranej grupy. Zadanie grupowe także może wpływać (opcjonalnie) na urządzenia, które zostały podłączone do podrzędnych i wirtualnych Serwerów administracyjnych zainstalowanych w grupie lub w jej dowolnej podgrupie.

- *Zadania globalne*—zadania wykonywane na zbiorze urządzeń, niezależnie od tego, czy znajdują się w jakiejkolwiek grupie

Dla każdej aplikacji można utworzyć dowolną liczbę zadań grupowych, zadań globalnych lub zadań lokalnych.

Możesz wprowadzać zmiany w ustawieniach zadań, przeglądać postęp ich wykonywania, a także kopiować, eksportować, importować i usuwać zadania.

Zadanie jest uruchamiane na urządzeniu tylko wtedy, gdy uruchomiona jest aplikacja, dla której utworzono zadanie.

Wyniki zadań są zapisywane w dzienniku zdarzeń systemu Microsoft Windows oraz w raporcie zdarzeń Kaspersky Security Center na Serwerze administracyjnym i lokalnie na każdym urządzeniu.

Nie używaj prywatnych danych w ustawieniach zadania. Na przykład, unikaj określania hasła administratora domeny.

Obszar zadania

Obszar zadania to zestaw urządzeń, na których wykonywane jest zadanie. Typy obszaru to:

- Dla *zadania lokalnego* obszarem jest samo urządzenie.
- Dla *zadania Serwera administracyjnego* obszarem jest Serwer administracyjny.
- Dla *zadania grupowego* obszarem jest lista urządzeń znajdujących się w grupie.

Podczas tworzenia *zadania globalnego* możesz użyć następujących metod do określenia jego obszaru:

- Ręcznie określ pewne urządzenia.

  Jako adresu urządzenia możesz użyć adresu IP (lub zakresu adresów IP), nazwy NetBIOS lub nazwy DNS.

- Zaimportuj listę urządzeń z pliku TXT zawierającego adresy dodawanych urządzeń (każdy adres powinien znajdować się w pojedynczej linii).

  Jeśli lista urządzeń jest importowana z pliku lub jest tworzona ręcznie, a urządzenia są identyfikowane po nazwie, lista może zawierać tylko urządzenia, o których informacje zostały już dodane do bazy danych Serwera administracyjnego. Co więcej, informacje musiały zostać wprowadzone, gdy te urządzenia były podłączone lub podczas wyszukiwania urządzeń.

- Utwórz wybór urządzeń.

  Obszar zadania zmienia się, gdy zmienia się zbiór urządzeń zawartych w wyborze. Wybór urządzeń można utworzyć w oparciu o atrybuty urządzeń, włączając w to oprogramowanie zainstalowane na urządzeniach, a także w oparciu o znaczniki przydzielone do urządzeń. Wybór urządzeń to najbardziej elastyczny sposób określania obszaru zadania.

  Zadania dla wyborów urządzeń są zawsze uruchamiane przez Serwer administracyjny zgodnie z terminarzem. Te zadania nie mogą zostać uruchomione na urządzeniach, które nie są połączone z Serwerem administracyjnym. Zadania, których obszar jest określony przy użyciu innych metod, są uruchamiane bezpośrednio na urządzeniach i dlatego nie zależą od połączenia urządzenia z Serwerem administracyjnym.

  Zadania dla wyborów urządzeń nie są uruchamiane zgodnie z czasem lokalnym urządzenia tylko z czasem lokalnym Serwera administracyjnego. Zadania, których obszar jest określony przy użyciu innych metod, są uruchamiane zgodnie z czasem lokalnym urządzenia.

Jak ustawienia lokalne aplikacji mają się do zasad

Za pomocą zasad możliwe jest ustawienie wspólnych wartości ustawień aplikacji dla wszystkich urządzeń należących do grupy.

Wartości ustawień określone w zasadzie mogą być zmieniane dla indywidualnych urządzeń znajdujących się w grupie przy użyciu lokalnych ustawień aplikacji. Możesz ustawić tylko te wartości ustawień, które zasada pozwala modyfikować, to znaczy odblokowanych ustawień.

Wartość ustawienia używana przez aplikację na urządzeniu klienckim jest wyznaczana przez pozycję zablokuj (🔒) dla tego ustawienia w zasadzie:

- Jeśli modyfikacja ustawienia jest zablokowana, wówczas ta sama wartość (określona w zasadzie) używana jest na wszystkich urządzeniach klienckich.

- Jeśli modyfikacja ustawienia jest odblokowana, wówczas na każdym urządzeniu klienckim aplikacja używa wartości lokalnej zamiast wartości określonej w zasadzie. W takiej sytuacji ustawienie może być zmieniane w lokalnych ustawieniach aplikacji.

Dlatego też, gdy zadanie jest uruchamiane na urządzeniu klienckim, aplikacja stosuje ustawienia określone na dwa różne sposoby:

- W ustawieniach zadania i lokalnych ustawieniach aplikacji, jeżeli modyfikowanie ustawienia nie jest zablokowane w zasadzie.

- W zasadzie grupy, jeżeli zablokowane jest modyfikowanie ustawienia.

Lokalne ustawienia aplikacji są zmieniane po pierwszym zastosowaniu zasady w zgodzie z jej ustawieniami.

Punkt dystrybucji

Punkt dystrybucji (wcześniej znany jako agent aktualizacji) to urządzenie z zainstalowanym Agentem sieciowym, które jest używane do dystrybucji aktualizacji, zdalnej instalacji aplikacji oraz pobierania informacji o urządzeniach w sieci. Punkty dystrybucji przyspieszają rozsyłanie uaktualnień i zwalniają zasoby Serwera administracyjnego.

Funkcje i przypadki użycia Agenta sieciowego zainstalowanego na urządzeniu pełniącym rolę punktu dystrybucji różnią się w zależności od systemu operacyjnego.

Punkt dystrybucji może wykonywać następujące funkcje:

- Dystrybucja plików otrzymanych z Serwera administracyjnego do urządzeń klienckich w obrębie grupy (w tym dystrybucja poprzez multiemisję z użyciem protokołu UDP).

  Lista plików, które można przesyłać za pośrednictwem punktów dystrybucji, obejmuje:

  - Aktualizacje baz danych i modułów oprogramowania Kaspersky
  - Instalowanie aktualizacji oprogramowania firm trzecich
  - Pakiety instalacyjne
  - Aktualizacje systemu Windows w przypadku używania Serwera administracyjnego jako serwera WSUS

  Uaktualnienia mogą być pobierane z Serwera administracyjnego lub z serwerów aktualizacji Kaspersky. W drugim przypadku należy utworzyć zadanie dla punktu dystrybucji. Urządzenia punktów dystrybucji działające pod kontrolą systemu operacyjnego macOS nie mogą pobierać uaktualnień z serwerów aktualizacji Kaspersky.

  W przypadku, gdy jedno lub więcej urządzeń działających pod kontrolą systemu operacyjnego macOS znajduje się w obszarze zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, zadanie zostaje zakończone ze stanem *Niepowodzenie* nawet wtedy, gdy zadanie zostaje zakończone pomyślnie na wszystkich urządzeniach z systemem Windows.

  Jeśli wszystkie punkty dystrybucji przypisane do urządzenia okażą się wadliwe, urządzenie nie będzie otrzymywać aktualizacji (baz wirusów i poprawek) ani pakietów instalacyjnych.

- Dystrybuować zasady i zadania grupowe poprzez multiemisję z użyciem protokołu UDP.
- Pełnić funkcję bramy połączenia z Serwerem administracyjnym dla urządzeń w grupie administracyjnej.

  Jeśli nie można nawiązać bezpośredniego połączenia między zarządzanymi urządzeniami w grupie a Serwerem administracyjnym, punkt dystrybucji może zostać użyty jako brama połączenia z Serwerem administracyjnym dla tej grupy. W tej sytuacji, zarządzane urządzenia zostaną podłączone do bramy połączenia, która połączy się z Serwerem administracyjnym.

  Obecność punktu dystrybucji, który działa jako brama połączenia, nie blokuje opcji bezpośredniego połączenia pomiędzy zarządzanymi urządzeniami a Serwerem administracyjnym. Jeśli brama połączenia nie jest dostępna, ale bezpośrednie połączenie z Serwerem administracyjnym jest technicznie możliwe, zarządzane urządzenia zostaną połączone bezpośrednio z Serwerem administracyjnym.

- Przeszukiwać sieć w celu odnalezienia nowych urządzeń i zaktualizowania informacji o tych istniejących. Punkt dystrybucji może stosować te same metody wykrywania urządzeń co Serwer administracyjny.

- Wykonaj zdalną instalację oprogramowania firm trzecich i aplikacji firmy Kaspersky przy użyciu narzędzi systemu operacyjnego punktu dystrybucji. Należy pamiętać, że punkt dystrybucji może przeprowadzić instalację na urządzeniach klienckich bez Agenta sieciowego.

  Ta funkcja umożliwia zdalne przesłanie pakietów instalacyjnych Agenta sieciowego na urządzenia klienckie znajdujące się w sieciach, do których Serwer administracyjny nie ma bezpośredniego dostępu.

- Pełni funkcję serwera proxy uczestniczącego w Kaspersky Security Network (KSN).

  Możesz włączyć serwer proxy KSN po stronie punktu dystrybucji, aby urządzenie pełniło rolę serwera proxy KSN. W tym przypadku usługa KSN proxy (ksnproxy) jest uruchomiona na urządzeniu.

Pliki są przesyłane z Serwera administracyjnego do punktu dystrybucji po protokole HTTP lub HTTPS (jeśli włączone jest połączenie SSL). W przeciwieństwie do SOAP, korzystanie z HTTP lub HTTPS zwiększa wydajność poprzez wyeliminowanie niezbędnego ruchu.

Urządzenia z zainstalowanym Agentem sieciowym mogą być wskazane do pełnienia roli punktów dystrybucji ręcznie (przez administratora) lub automatycznie (przez Serwer administracyjny). Pełna lista punktów dystrybucji dla określonych grup administracyjnych jest wyświetlana w raporcie na liście punktów dystrybucji.

Zakres punktu dystrybucji to grupa administracyjna, do której został przypisany przez administratora, a także jej podgrupy na wszystkich poziomach zagnieżdżenia. Jeśli w hierarchii grup administracyjnych przypisano kilka punktów dystrybucji, Agent sieciowy zarządzanego urządzenia nawiąże połączenie z najbliższym punktem dystrybucji w hierarchii.

Lokalizacja sieciowa także może należeć do zakresu punktów dystrybucji. Lokalizacja sieciowa jest wówczas używana do ręcznego tworzenia zbioru urządzeń, na które punkt dystrybucji roześle uaktualnienia. Lokalizacja sieciowa może zostać określona tylko dla urządzeń działających pod kontrolą systemu operacyjnego Windows.

Jeśli punkty dystrybucji są wskazywane automatycznie przez Serwer administracyjny, wskaże on je według domen rozgłoszeniowych, a nie według grup administracyjnych. Ma to miejsce wtedy, gdy znane są wszystkie domeny rozgłoszeniowe. Agent sieciowy wymienia wiadomości z innymi Agentami sieciowymi w tej samej podsieci, a następnie wysyła do Serwera administracyjnego informacje o sobie i innych Agentach sieciowych. Serwer administracyjny może użyć tych informacji do pogrupowania Agentów sieciowych według domen rozgłoszeniowych. Domeny rozgłoszeniowe są znane dla Serwera administracyjnego, gdy przeszuka on ponad 70% Agentów sieciowych w grupach administracyjnych. Serwer administracyjny wyszukuje domeny rozgłoszeniowe co dwie godziny. Po przypisaniu punktów dystrybucji według domen rozgłoszeniowych, nie mogą być one ponownie przypisane według grup administracyjnych.

Jeśli administrator ręcznie przypisuje punkty dystrybucji, można je przypisać do grup administracyjnych lub lokalizacji sieciowych.

Agenty sieciowe z aktywnym profilem połączenia nie uczestniczą w wykrywaniu domen rozgłoszeniowych.

Kaspersky Security Center przypisuje każdemu Agentowi sieciowemu unikatowy adres IP multicastu, który różni się od każdego innego adresu. Pozwala to uniknąć przeciążenia sieci, które może mieć miejsce w wyniku nakładania się adresów IP.

Jeśli w jednym obszarze sieci lub jednej grupie administracyjnej przypisanych jest więcej niż dwa punkty dystrybucji, jeden z nich staje się aktywnym punktem dystrybucji, a pozostałe stają się rezerwowymi punktami dystrybucji. Aktywny punkt dystrybucji pobiera uaktualnienia i pakiety instalacyjne bezpośrednio z Serwera administracyjnego, natomiast rezerwowe punkty dystrybucji pobierają uaktualnienia tylko z aktywnego punktu dystrybucji. W tym przypadku pliki zostają raz pobrane z Serwera administracyjnego, a następnie zostają rozdystrybuowane pośród punktów dystrybucji. Jeśli z jakiegoś powodu aktywny punkt dystrybucji stanie się niedostępny, jeden z rezerwowych punktów dystrybucji stanie się aktywny. Serwer administracyjny automatycznie wskaże punkt dystrybucji jako rezerwowy.

Stan punktu dystrybucji (*Aktywny*/*Rezerwowy*) jest wyświetlany z polem do zaznaczenia w raporcie narzędzia klnagchk.

Punkt dystrybucji wymaga przynajmniej 4 GB wolnej przestrzeni na dysku. Jeśli wolna przestrzeń na dysku punktu dystrybucji jest mniejsza niż 2 GB, Kaspersky Security Center tworzy problem bezpieczeństwa z poziomem istotności *Ostrzeżenie*. Problem bezpieczeństwa zostanie opublikowany we właściwościach urządzenia, w sekcji **Incydenty związane z bezpieczeństwem**.

Uruchamianie zadań zdalnej instalacji na urządzeniu wskazanym jako punkt dystrybucji wymaga dodatkowej wolnej przestrzeni na dysku. Ilość wolnego miejsca na dysku musi przekraczać całkowity rozmiar wszystkich pakietów instalacyjnych, które zostaną użyte do instalacji.

Uruchamianie dowolnych zadań aktualizacji i naprawiania luk na urządzeniu wskazanym jako punkt dystrybucji wymaga dodatkowej wolnej przestrzeni na dysku. Ilość wolnego miejsca na dysku musi być równa podwojonej wartości całkowitego rozmiaru wszystkich poprawek przeznaczonych do zainstalowania.

Urządzenia pełniące rolę punktów dystrybucji muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

Brama połączenia

Brama połączenia to Agent sieciowy działający w trybie specjalnym. Brama połączenia akceptuje połączenia z innych Agentów sieciowych i tuneluje je przez Serwer administracyjny poprzez własne połączenie z serwerem. W przeciwieństwie do zwykłego Agenta sieciowego brama połączenia oczekuje na połączenia z Serwerem administracyjnym bardziej niż nawiązuje te połączenia z Serwerem administracyjnym.

Brama połączenia może komunikować się z maksymalnie 10 000 urządzeń.

Masz dwie możliwości korzystania z bram połączeń:

- Zalecamy zainstalowanie bramy połączenia w strefie zdemilitaryzowanej (DMZ). W przypadku innych Agentów sieciowych zainstalowanych na urządzeniach mobilnych, musisz specjalnie skonfigurować połączenie z Serwerem administracyjnym przez bramę połączenia.

  Brama połączenia w żaden sposób nie modyfikuje ani nie przetwarza danych przesyłanych od Agentów sieciowych do Serwera administracyjnego. Co więcej, nie zapisuje tych danych w żadnym buforze i dlatego nie może zaakceptować danych od Agenta sieciowego i później przesyłać ich na Serwer administracyjny. Jeśli Agent sieciowy próbuje nawiązać połączenie z Serwerem administracyjnym przez bramę połączenia, ale brama połączenia nie może połączyć się z Serwerem administracyjnym, Agent sieciowy postrzega to tak, jakby Serwer administracyjny był niedostępny. Wszystkie dane pozostają na Agencie sieciowym (nie w bramie połączenia).

  Brama połączenia nie może nawiązać połączenia z Serwerem administracyjnym przez inną bramę połączenia. Oznacza to, że Agent sieciowy nie może być jednocześnie bramą połączenia i używać bramy połączenia do łączenia się z Serwerem administracyjnym.

Wszystkie bramy połączeń znajdują się na liście punktów dystrybucji we właściwościach Serwera administracyjnego.

- Możesz także używać bram połączeń w sieci. Na przykład, automatycznie przypisane punkty dystrybucji stają się również bramami połączeń w swoim własnym zakresie. Jednak w sieci wewnętrznej bramy połączeń nie zapewniają znaczących korzyści. Zmniejszają liczbę połączeń sieciowych odbieranych przez Serwer administracyjny, ale nie zmniejszają ilości przychodzących danych. Nawet bez bram połączeń wszystkie urządzenia mogą nadal łączyć się z Serwerem administracyjnym.

Główny scenariusz instalacji

Postępując zgodnie z tym scenariuszem możesz zainstalować Serwer administracyjny, a także zainstalować Agenta sieciowego i aplikacje zabezpieczające na urządzeniach w sieci. Możesz użyć tego scenariusza do przyjrzenia się aplikacji i do zainstalowania aplikacji.

Instalacja Kaspersky Security Center składa się na następujące etapy:

1. Prace przygotowawcze
2. Instalacja Kaspersky Security Center oraz aplikacji zabezpieczającej Kaspersky na urządzeniu z Serwerem administracyjnym
3. Scentralizowane wdrażanie aplikacji zabezpieczających Kaspersky na urządzeniach klienckich

Wdrożenie Kaspersky Security Center w środowiskach chmury oraz zdalna instalacja Kaspersky Security Center dla dostawców usługi są opisane w odpowiednich sekcjach Pomocy.

Zalecane jest poświęcenie przynajmniej godziny na zainstalowanie Serwera administracyjnego i przynajmniej jednego dnia roboczego na zakończenie scenariusza. Zalecane jest także zainstalowanie aplikacji zabezpieczającej, takiej jak Kaspersky Security for Windows Server lub Kaspersky Endpoint Security, na urządzeniu, które będzie pełniło rolę Serwera administracyjnego Kaspersky Security Center.

Po wykonaniu scenariusza, ochrona zostanie wdrożona w sieci organizacji w następujący sposób:

- System DBMS zostanie zainstalowany dla Serwera administracyjnego.
- Serwer administracyjny Kaspersky Security Center zostanie zainstalowany.
- Wszystkie wymagane zasady i zadania zostaną utworzone; domyślne ustawienia zasad i zadań zostaną określone.
- Aplikacje zabezpieczające (np. Kaspersky Endpoint Security for Windows) i Agent sieciowy zostaną zainstalowani na zarządzanych urządzeniach.
- Grupy administracyjne zostaną utworzone (i jeśli to możliwe, zostanie utworzona ich hierarchia).
- Jeśli to konieczne, ochrona urządzeń mobilnych zostanie wdrożona.
- Punkty dystrybucji zostaną przydzielone (jeśli to konieczne).

Instalacja Kaspersky Security Center odbywa się w krokach:

Prace przygotowawcze

1. **Pobieranie niezbędnych plików**

   Upewnij się, że posiadasz klucz licencyjny (kod aktywacyjny) do Kaspersky Security Center lub klucze licencyjne (kody aktywacyjne) do aplikacji zabezpieczających Kaspersky.

   Rozpakuj archiwum otrzymane od dostawcy. To archiwum zawiera klucze licencyjne (pliki KEY), kody aktywacyjne oraz listę aplikacji firmy Kaspersky, które można aktywować za pomocą każdego klucza licencyjnego.

   Jeśli najpierw chcesz wypróbować Kaspersky Security Center, możesz uzyskać bezpłatną, 30-dniową wersję testową na stronie internetowej Kaspersky.

   Aby uzyskać szczegółowe informacje na temat licencjonowania aplikacji zabezpieczających Kaspersky, które nie są zawarte w Kaspersky Security Center, możesz zapoznać się z dokumentacją tych aplikacji.

2. **Wybieranie struktury ochrony organizacji**

   Zapoznaj się ze szczegółowymi informacjami dotyczącymi komponentów Kaspersky Security Center. Wybierz strukturę ochrony i konfigurację sieci, które najbardziej odpowiadają Twojej organizacji. W oparciu o konfigurację sieci i przepustowość kanałów komunikacji, zdefiniuj liczbę używanych Serwerów administracyjnych oraz sposób ich dystrybucji pomiędzy biurami (jeśli pracujesz w sieci rozproszonej).

   Aby uzyskać i utrzymać optymalną wydajność w różnych warunkach pracy, należy wziąć pod uwagę liczbę urządzeń w sieci, topologię sieci oraz zestaw funkcji Kaspersky Security Center, jakich potrzebujesz (więcej informacji można znaleźć w Podręczniku szacowania rozmiaru Kaspersky Security Center).

   Zdefiniuj, czy hierarchia Serwerów administracyjnych będzie używana w organizacji. W tym celu należy oszacować, czy jest to możliwe i korzystne, aby wszystkie urządzenia kliencie były zarządzane przez jeden Serwer administracyjny i czy konieczne jest tworzenie hierarchii Serwerów administracyjnych. Konieczne może być też utworzenie hierarchii Serwerów administracyjnych, która jest taka sama, jak struktura organizacyjna firmy, której sieć chcesz chronić.

   Jeśli musisz zapewnić ochronę urządzeń mobilnych, wykonaj wszystkie wymagane wstępne działania niezbędne dla konfiguracji Serwera iOS MDM.

   Upewnij się, że urządzenia, które wybrałeś jako Serwery administracyjne, a także te do zainstalowania Konsoli administracyjnej, spełniają wszystkie wymagania sprzętowe i programowe.

3. **Przygotowanie do użycia certyfikatów niestandardowych**

   Jeśli infrastruktura kluczy publicznych (PKI) Twojej organizacji wymaga użycia certyfikatów niestandardowych opublikowanych przez określony Urząd certyfikacji (CA), przygotuj te certyfikaty i upewnij się, że spełniają wszystkie wymagania.

4. **Przygotowanie do licencjonowania Kaspersky Security Center**

   Jeśli panujesz korzystać z wersji Kaspersky Security Center z obsługą Zarządzania urządzeń mobilnych, Integracji systemów SIEM i/lub Zarządzania lukami i poprawkami, upewnij się, że posiadasz plik klucza lub kod aktywacyjny licencjonowania aplikacji.

5. **Przygotowanie do licencjonowania zarządzanych aplikacji zabezpieczających**

   Podczas wdrażania ochrony konieczne może być dostarczenie Kaspersky aktywnych kluczy licencyjnych dla aplikacji, którymi zamierzasz zarządzać za pośrednictwem Kaspersky Security Center (patrz lista zarządzanych aplikacji zabezpieczających). Szczegółowe informacje na temat licencjonowania każdej aplikacji zabezpieczającej można znaleźć w dokumentacji dla tej aplikacji.

6. **Wybieranie konfiguracji sprzętowej Serwera administracyjnego i systemu DBMS**

   Zaplanuj konfigurację sprzętową dla systemu DBMS i Serwera administracyjnego, biorąc pod uwagę liczbę urządzeń w sieci.

7 Wybieranie systemu zarządzania bazą danych

Podczas wybierania DBMS należy mieć na uwadze liczbę zarządzanych urządzeń, które obejmuje ten Serwer administracyjny. Jeśli Twoja sieć zawiera mniej niż 10 000 urządzeń i nie planujesz zwiększyć tej liczby, możesz wybrać bezpłatny system DBMS, taki jak SQL Express lub MySQL, i zainstalować go na tym samym urządzeniu co Serwer administracyjny. Alternatywnie możesz wybrać MariaDB DBMS, który pozwala na zarządzanie do 20 000 urządzeń. Jeśli Twoja sieć zawiera więcej niż 10 000 urządzeń (lub jeśli planujesz rozszerzyć sieć do tej liczby urządzeń), zalecane jest wybranie płatnego systemu SQL DBMS i zainstalowanie go na dedykowanym urządzeniu. Płatny system DBMS może pracować z kilkoma Serwerami administracyjnymi, ale darmowy system DBMS może pracować tylko z jednym.

Jeśli wybierzesz SQL Server DBMS, pamiętaj, że możesz migrować dane przechowywane w bazie danych do MySQL, MariaDB lub Azure SQL DBMS. Aby przeprowadzić migrację, utwórz kopię zapasową danych i przywróć je do nowego systemu DBMS.

> Jeśli wybierzesz MSSQL 2019, musisz użyć zbiorczej poprawki CU12 lub nowszej. Pozwoli to uniknąć błędów i przeciążenia systemu, które mogą wystąpić.

8 Instalowanie systemu DBMS i tworzenie bazy danych

Zapoznaj się z informacjami na temat kont do pracy z DBMS i zainstaluj swój system DBMS.

Przed instalacją wybierz obsługiwany system DBMS. Możesz wybrać na przykład PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL lub MariaDB.

Informacje o sposobie zainstalowania wybranego systemu DBMS znajdziesz w tym dokumencie.

Jeśli instalujesz MariaDB, MySQL, PostgreSQL lub Postgres Pro, użyj zalecanych ustawień, aby zapewnić prawidłowe działanie DBMS.

Zanotuj na kartce, a następnie zapisz ustawienia DBMS, ponieważ będziesz ich potrzebował podczas instalacji Serwera administracyjnego. Te ustawienia obejmują nazwę serwera SQL, numer portu używanego do łączenia z serwerem SQL, nazwę konta i hasło do uzyskania dostępu do serwera SQL.

> Jeśli zdecydujesz się zainstalować PostgreSQL lub Postgres Pro DBMS, upewnij się, że określone zostało hasło superużytkownika. Jeśli hasło nie zostanie określone, Serwer administracyjny może nie być w stanie połączyć się z bazą danych.

Domyślnie, instalator Kaspersky Security Center tworzy bazę danych do przechowywania informacji Serwera administracyjnego, ale możesz zrezygnować z utworzenia tej bazy danych i zamiast tego użyć innej bazy danych. W tym przypadku upewnij się, że baza danych została utworzona, znasz jej nazwę, a konto, z poziomu którego Serwer administracyjny uzyska dostęp do tej bazy, posiada dla niej rolę db_owner.

Jeśli to konieczne, skontaktuj się z administratorem DBMS w celu uzyskania dodatkowych informacji.

9 Konfigurowanie portów

Upewnij się, że wszystkie niezbędne porty są otwarte do interakcji pomiędzy komponentami zgodnie z wybraną strukturą bezpieczeństwa.

Jeśli musisz zapewnić Serwerowi administracyjnemu dostęp do internetu, skonfiguruj porty i określ ustawienia połączenia, w zależności od konfiguracji sieci.

10 Sprawdzanie kont

Upewnij się, że masz wszystkie uprawnienia lokalnego administratora, wymagane do pomyślnego zainstalowania Serwera administracyjnego Kaspersky Security Center i dalszego wdrażania ochrony na urządzeniach. Uprawnienia lokalnego administratora na urządzeniach klienckich są wymagane do zainstalowania Agenta sieciowego na tych urządzeniach. Po zainstalowaniu Agenta sieciowego możesz użyć go do zdalnego zainstalowania aplikacji na urządzeniach, bez użycia konta z uprawnieniami administratora urządzenia.

Domyślnie, na urządzeniu wybranym do zainstalowania Serwera administracyjnego, instalator Kaspersky Security Center tworzy trzy konta lokalne, z poziomu których zostanie uruchomiony Serwer administracyjny oraz usługi Kaspersky Security Center:

- KL-AK-*: konto usługi Serwera administracyjnego
- NT Service/KSC*: konto do innych usług z puli Serwera administracyjnego
- KlPxeUser: konto do zdalnej instalacji systemów operacyjnych

Możesz zrezygnować z tworzenia kont dla usług Serwera administracyjnego i innych usług. Zamiast tego użyj istniejących kont, takich jak konta domeny, jeśli planujesz zainstalować Serwer administracyjny na klastrze typu failover lub z jakiegoś powodu planujesz użyć kont domeny zamiast kont lokalnych. W tym przypadku upewnij się, że konta przeznaczone do działania Serwera administracyjnego i usług Kaspersky Security Center zostały utworzone, nie są uprzywilejowane i mają wszystkie uprawnienia, które są wymagane, żeby mieć dostęp do systemu DBMS. (Jeśli planujesz dalsze wdrożenie systemów operacyjnych na urządzeniach poprzez Kaspersky Security Center, nie wycofuj się z tworzenia kont.)

Instalacja Kaspersky Security Center oraz aplikacji zabezpieczającej Kaspersky na urządzeniu z Serwerem administracyjnym

1. **Instalowanie Serwera administracyjnego, Konsoli administracyjnej, Kaspersky Security Center Web Console i wtyczek administracyjnych dla aplikacji zabezpieczających**

   Pobierz Kaspersky Security Center ze strony internetowej Kaspersky. Możesz pobrać pełny pakiet, tylko konsolę Web Console lub tylko Konsolę administracyjną.

   Zainstaluj Serwer administracyjny na wybranym urządzeniu (lub kilku urządzeniach, jeśli planujesz używać kilku Serwerów administracyjnych). Możesz wybrać standardową lub niestandardową instalację Serwera administracyjnego. Konsola administracyjna zostanie zainstalowana wraz z Serwerem administracyjnym. Zaleca się zainstalowanie Serwera administracyjnego na serwerze dedykowanym zamiast na kontrolerze domeny.

   Instalacja standardowa jest zalecana, jeśli chcesz wypróbować Kaspersky Security Center, na przykład, poprzez przetestowanie działania aplikacji w małym obszarze wewnątrz sieci. Podczas instalacji standardowej konfigurujesz tylko bazę danych. Możesz także zainstalować tylko domyślny zestaw wtyczek administracyjnych dla aplikacji Kaspersky. Możesz także użyć standardowej instalacji, jeśli już masz doświadczenie w pracy z Kaspersky Security Center i jesteś w stanie określić wszystkie odpowiednie ustawienia po standardowej instalacji.

   Instalacja niestandardowa jest zalecana, jeśli planujesz zmodyfikować ustawienia Kaspersky Security Center, takie jak: ścieżka dostępu do folderu współdzielonego, konta i porty dla połączenia z Serwerem administracyjnym oraz ustawienia bazy danych. Instalacja niestandardowa umożliwia określenie, które wtyczki administracyjne Kaspersky mają zostać zainstalowane. Jeśli to konieczne, możesz uruchomić instalację niestandardową w trybie cichym.

   Konsola administracyjna i wersja serwerowa Agenta sieciowego są instalowane wraz z Serwerem administracyjnym. Podczas instalacji możesz także wybrać zainstalowanie Kaspersky Security Center Web Console.

   Jeśli chcesz, zainstaluj Konsolę administracyjną i/lub Kaspersky Security Center Web Console na stacji roboczej administratora oddzielnie, aby zarządzać Serwerem administracyjnym poprzez sieć.

2 Wstępna konfiguracja i licencjonowanie

Po zakończeniu instalacji Serwera administracyjnego, przy pierwszym połączeniu z Serwerem administracyjnym Kreator wstępnej konfiguracji zostanie uruchomiony automatycznie. Przeprowadź wstępną konfigurację Serwera administracyjnego zgodnie z istniejącymi wymaganiami. Na etapie wstępnej konfiguracji kreator używa domyślnych ustawień do tworzenia zasad i zadań, które są niezbędne do wdrażania ochrony. Jednakże ustawienia domyślne mogą być mniej niż optymalne dla potrzeb Twojej organizacji. Jeśli to konieczne, możesz edytować ustawienia zasad i zadań (Konfigurowanie ochrony w sieci organizacji klienta, Scenariusz: Konfigurowanie ochrony sieci).

Jeśli planujesz używać funkcji, które są poza podstawową funkcjonalnością, użyj licencji dla aplikacji. Możesz to zrobić w jednym z kroków kreatora wstępnej konfiguracji.

3 Sprawdzanie, czy instalacja Serwera administracyjnego została zakończona pomyślnie

Jeśli czynności ze wszystkich poprzednich kroków zostały wykonane, Serwer administracyjny jest zainstalowany i gotowy do użycia.

Upewnij się, że Konsola administracyjna jest uruchomiona i możesz połączyć się z Serwerem administracyjnym poprzez Konsolę administracyjną. Dodatkowo, upewnij się, że zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego jest dostępna na Serwerze administracyjnym (w folderze **Zadania** drzewa konsoli), a także dostępna jest zasada dla Kaspersky Endpoint Security (w folderze **Zasady** drzewa konsoli).

Po zakończeniu sprawdzania, przejdź do kroków poniżej.

Scentralizowane wdrażanie aplikacji zabezpieczających Kaspersky na urządzeniach klienckich

1 Wykrywanie urządzeń w sieci

Ten krok jest częścią kreatora wstępnej konfiguracji. Możesz także ręcznie uruchomić wykrywanie urządzeń. Kaspersky Security Center pobiera adresy i nazwy wszystkich urządzeń wykrytych w sieci. Następnie możesz użyć Kaspersky Security Center do zainstalowania aplikacji firmy Kaspersky i oprogramowania innych producentów na wykrytych urządzeniach. Kaspersky Security Center regularnie uruchamia wykrywanie urządzeń, co oznacza, że jeśli nowe instancje pojawią się w sieci, zostaną wykryte automatycznie.

2 Instalowanie Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci

Wdrożenie ochrony (Konfigurowanie ochrony w sieci organizacji klienta, Scenariusz: Konfigurowanie ochrony sieci) w sieci organizacji wiąże się z zainstalowaniem Agenta sieciowego i aplikacji zabezpieczających (na przykład: Kaspersky Endpoint Security) na urządzeniach, które zostały wykryte przez Serwer administracyjny podczas wykrywania urządzeń.

Aplikacje zabezpieczające chronią urządzenia przed wirusami i/lub innym programami stwarzającymi zagrożenie. Agent sieciowy zapewnienia komunikację pomiędzy urządzeniem a Serwerem administracyjnym. Domyślnie ustawienia Agenta sieciowego są konfigurowane automatycznie.

Jeśli chcesz, możesz zainstalować Agenta sieciowego w trybie cichym z plikiem odpowiedzi lub bez pliku odpowiedzi.

Przed rozpoczęciem instalacji Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci, upewnij się, że te urządzenia są dostępne (czyli są włączone). Możesz zainstalować Agenta sieciowego na maszynach wirtualnych, a także na urządzeniach fizycznych.

Aplikacje zabezpieczające i Agent sieciowy mogą zostać zainstalowani zdalnie lub lokalnie.

Zdalna instalacja — korzystając z kreatora wdrażania ochrony, możesz zdalnie zainstalować aplikację zabezpieczającą (np. Kaspersky Endpoint Security for Windows) i Agenta sieciowego na urządzeniach, które zostały wykryte przez Serwer administracyjny w sieci organizacji. Zazwyczaj zadanie Zdalna instalacja pomyślnie wdraża ochronę na większości urządzeń w sieci. Jednakże może zwrócić błąd na niektórych urządzeniach, jeśli, na przykład, urządzenie jest wyłączone lub z jakiegoś powodu nie można uzyskać do niego dostępu. W tym przypadku zalecane jest ręczne nawiązanie połączenia z urządzeniem i skorzystanie z instalacji lokalnej.

Lokalna instalacja—używana na urządzeniach w sieci, na których ochrona nie mogła zostać wdrożona przy użyciu zadania zdalnej instalacji. Aby wdrożyć ochronę na takich urządzeniach, utwórz autonomiczny pakiet instalacyjny, który możesz uruchomić lokalnie na tych urządzeniach.

Instalacja Agenta sieciowego na urządzeniach działających pod kontrolą systemów operacyjnych Linux i macOS została opisana w dokumentacji do Kaspersky Endpoint Security for Linux i Kaspersky Endpoint Security for Mac. Chociaż urządzenia działające pod kontrolą systemów operacyjnych Linux i macOS są uważane za mniej podatne na zagrożenia i ataki niż urządzenia z systemem Windows, zalecane jest zainstalowanie aplikacji zabezpieczających na tych urządzeniach.

Po zainstalowaniu, upewnij się, że aplikacja zabezpieczająca jest zainstalowana na zarządzanych urządzeniach. Otwórz raport o wersjach oprogramowania Kaspersky i przejrzyj jego wyniki.

3. **Rozsyłanie kluczy licencyjnych na urządzenia klienckie**

   Roześlij klucze licencyjne na urządzenia klienckie, aby aktywować zarządzane aplikacje zabezpieczające na tych urządzeniach.

4. **Konfigurowanie ochrony urządzeń mobilnych**

   Ten krok jest częścią kreatora wstępnej konfiguracji.

   Jeśli chcesz zarządzać firmowymi urządzeniami mobilnymi, podejmij odpowiednie kroki w celu przygotowania i wdrożenia Zarządzania urządzeniami mobilnymi.

5. **Tworzenie struktury grupy administracyjnej**

   W niektórych przypadkach, wdrożenie ochrony na urządzeniach w sieci w najbardziej wygodny sposób może wymagać podzielenia całej puli urządzeń na grupy administracyjne, z uwzględnieniem struktury organizacji. Możesz utworzyć reguły przenoszenia urządzeń pomiędzy grupami lub możesz ręcznie przenieść urządzenia. Możesz przypisać zadania grupowe dla grup administracyjnych, zdefiniować obszar zasad oraz przypisać punkty dystrybucji.

   Upewnij się, że wszystkie zarządzane urządzenia zostały poprawnie przydzielone do odpowiednich grup administracyjnych i że w sieci nie ma żadnego nieprzypisanego urządzenia.

6. **Przypisywanie punktów dystrybucji**

   Kaspersky Security Center przypisuje punkty dystrybucji do grup administracyjnych automatycznie, ale w razie potrzeby możesz przypisać je ręcznie. Zalecane jest użycie punktów dystrybucji w sieciach dużej skali w celu zmniejszenia obciążenia na Serwerze administracyjnym, a także w sieciach, które posiadają strukturę rozproszoną, aby zapewnić Serwerowi administracyjnemu dostęp do urządzeń (lub grup urządzeń) komunikujących się przez kanały o niskiej przepustowości. Możesz używać urządzeń działających pod kontrolą systemu Linux jako punktów dystrybucji, a także urządzeń działających pod kontrolą systemu Windows.

Porty używane przez Kaspersky Security Center

Poniższe tabele przedstawiają domyślne porty używane przez Serwery administracyjne i urządzenia klienckie. Jeśli chcesz, możesz zmienić domyślne numery portów.

Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server, port 1433 dla Microsoft SQL Server, lub port 5432 dla PostgreSQL i Postgres Pro). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

Porty używane przez Serwer administracyjny

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
8060	klcsweb	TCP	Przesyłanie opublikowanych pakietów instalacyjnych na urządzenia klienckie	Publikowanie pakietów instalacyjnych. Możesz zmienić domyślny numer portu w sekcji **Serwer internetowy** okna właściwości Serwera administracyjnego w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console. Ten parametr jest opcjonalny. Ze względów bezpieczeństwa zalecamy używanie portu TCP 8061.
8061	klcsweb	TCP (TLS)	Przesyłanie opublikowanych pakietów instalacyjnych na urządzenia klienckie	Publikowanie pakietów instalacyjnych. Możesz zmienić domyślny numer portu w sekcji **Serwer internetowy** okna właściwości Serwera administracyjnego w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
13000	klserver	TCP (TLS)	Odbieranie połączeń od Agentów sieciowych i podrzędnych Serwerów administracyjnych; używany także na podrzędnych Serwerach administracyjnych do odbierania połączeń od głównego Serwera administracyjnego (na przykład, jeśli podrzędny Serwer administracyjny znajduje się w strefie DMZ)	Zarządzanie urządzeniami klienckimi i podrzędnymi Serwerami administracyjnymi. Możesz zmienić numer domyślnego portu do odbierania połączeń od Agentów sieciowych podczas konfigurowania portów połączeń; możesz zmienić numer domyślnego portu do odbierania połączeń z podrzędnych Serwerów administracyjnych podczas tworzenia hierarchii Serwerów administracyjnych w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
13000	klserver	UDP	Pobieranie informacji o urządzeniach, które zostały wyłączone, z Agentów sieciowych	Zarządzanie urządzeniami klienckimi. Możesz zmienić numer domyślnego portu w ustawieniach zasad Agenta sieciowego w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
13291	klserver	TCP (TLS)	Odbieranie połączeń od Konsoli administracyjnej do Serwera administracyjnego	Zarządzanie Serwerem administracyjnym. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego w Konsoli administracyjnej.
13299	klserver	TCP (TLS)	Odbieranie połączeń od Kaspersky Security Center Web Console do Serwera administracyjnego; odbieranie połączeń do Serwera administracyjnego poprzez OpenAPI	Kaspersky Security Center Web Console, OpenAPI. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego (sekcja **Ustawienia połączenia z Serwerem administracyjnym** → podsekcja **Porty połączenia**) w Konsoli administracyjnej lub podczas tworzenia hierarchii Serwerów administracyjnych w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
14000	klserver	TCP	Odbieranie połączeń od Agentów sieciowych	Zarządzanie urządzeniami klienckimi. Możesz zmienić numer domyślnego portu, gdy konfigurowanie portów połączeń podczas instalacji Kaspersky Security Center lub podczas ręcznego łączenia urządzenia klienckiego z Serwerem administracyjnym. Ten parametr jest opcjonalny. Ze względów bezpieczeństwa zalecamy używanie portu TCP 13000.
13111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	TCP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.
15111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	UDP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
17000	klactprx	TCP (TLS)	Odbieranie połączeń dla aktywacji aplikacji od zarządzanych urządzeń (za wyjątkiem urządzeń mobilnych)	Serwer proxy aktywacji używany przez urządzenia inne niż mobilne do aktywacji aplikacji Kaspersky za pomocą kodów aktywacyjnych. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.
17100 (tylko wtedy, gdy zarządzasz urządzeniami mobilnymi)	klactprx	TCP (TLS)	Odbieranie połączeń dla aktywacji aplikacji od urządzeń mobilnych	Aktywacja przy użyciu serwera proxy dla urządzeń mobilnych. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.
19170	klserver	HTTPS (TLS)	Tunelowanie połączeń z zarządzanymi urządzeniami przy użyciu narzędzia klsctunnel	Zdalne nawiązywanie połączenia z zarządzanymi urządzeniami przy użyciu Kaspersky Security Center Web Console. Domyślny numer portu można zmienić tylko w oknie właściwości serwera administracyjnego w Konsoli administracyjnej (sekcja **Ustawienia połączenia z Serwerem administracyjnym** → podsekcja **Porty połączenia** → opcja **Otwórz port RDP dla Kaspersky Security Center Web Console**).
13292 (tylko wtedy, gdy zarządzasz urządzeniami mobilnymi)	klserver	TCP (TLS)	Obieranie połączeń od urządzeń mobilnych	Zarządzanie urządzeniami mobilnymi. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
13294 (tylko wtedy, gdy zarządzasz urządzeniami mobilnymi)	klserver	TCP (TLS)	Odbieranie połączeń od urządzeń chronionych UEFI	Zarządzanie urządzeniami klienckimi chronionymi UEFI. Możesz zmienić domyślny numer portu podczas podłączania urządzeń mobilnych lub później, w oknie właściwości Serwera administracyjnego (sekcja **Ustawienia połączenia z Serwerem administracyjnym** → podsekcja **Porty połączenia**) w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
13296	klserver	TCP (TLS)	Publikowanie metryk Kaspersky Security Center dla Prometheus	Publikowanie metryk Kaspersky Security Center, które będą dalej pozyskiwane przez Prometheus. Metryki możesz zobaczyć pod następującym odnośnikiem: https://<`adres_serwera`>:13296/metrics. W polu <`server_address`>, określ adres IP lub nazwę domeny Serwera administracyjnego. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego w konsoli administracyjnej.
30522, 30523 (porty na interfejsie localhost)	klnagent	TCP	Przesyłanie aktualizacji aplikacji z Agenta sieciowego do lokalnie zainstalowanych aplikacji Kaspersky za pomocą komponentu FileTransferBridge	Urządzenie Serwera administracyjnego, które odbiera aktualizacje aplikacji Kaspersky.

Poniższa tabela wyświetla port, który musi zostać otwarty na serwerze iOS MDM Server (tylko wtedy, gdy zarządzasz urządzeniami mobilnymi).

Port używany przez serwer iOS MDM

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
443	kliosmdmservicesrv	TCP (TLS)	Obieranie połączeń od urządzeń mobilnych iOS	Zarządzanie urządzeniami mobilnymi. Możesz zmienić numer domyślnego portu podczas instalowania serwera iOS MDM.

Poniższa tabela wyświetla port, który musi zostać otwarty na serwerze Kaspersky Security Center Web Console Server. To może być to samo urządzenie, na którym jest zainstalowany Serwer administracyjny, lub inne urządzenie.

Port używany przez Kaspersky Security Center Web Console Server

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
8080	Node.js: Server-side JavaScript	TCP (TLS)	Odbieranie połączeń z przeglądarki do Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. Możesz zmienić numer domyślnego portu podczas instalacji Kaspersky Security Center Web Console na urządzeniu z systemem Windows lub na platformie Linux. Jeśli instalujesz konsolę Kaspersky Security Center Web Console w systemie operacyjnym Linux ALT, musisz określić numer portu inny niż 8080, ponieważ port 8080 jest używany przez system operacyjny.

Poniższa tabela wyświetla port, który musi być otwarty na zarządzanych urządzeniach, na których jest zainstalowany Agent sieciowy.

Porty używane przez Agenta sieciowego

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
15000	klnagent	UDP	Sygnały zarządzania z Serwera administracyjnego lub punktów dystrybucji do Agentów sieciowych	Zarządzanie urządzeniami klienckimi. Możesz zmienić numer domyślnego portu w ustawieniach zasad Agenta sieciowego w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
15000	klnagent	Transmisja UDP	Uzyskiwanie danych o innych Agentach sieciowych w obrębie tej samej domeny broadcastowej (dane są następnie wysyłane do Serwera administracyjnego)	Dostarczanie uaktualnień i pakietów instalacyjnych.
15001	klnagent	UDP	Odbieranie żądań multiemisji z punktu dystrybucji (jeśli jest używany)	Odbieranie aktualizacji i pakietów instalacyjnych z punktu dystrybucji. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
30522, 30523 (porty na interfejsie localhost)	klnagent	TCP	Odbieranie aktualizacji aplikacji Kaspersky z Serwera administracyjnego przy użyciu komponentu FileTransferBridge	Zarządzane urządzenia, które otrzymują aktualizacje aplikacji Kaspersky z Serwera administracyjnego określonego jako źródło aktualizacji bazy danych.
161	klnagent	SNMP	Monitorowanie i wykrywanie urządzeń sieciowych.	Możliwość wykrycia urządzenia.

Należy pamiętać, że proces klnagent może również żądać wolnych portów z dynamicznego zakresu portów systemu operacyjnego punktu końcowego. Porty te są automatycznie przydzielane procesowi klnagent przez system operacyjny, więc proces klnagent może korzystać z niektórych portów używanych przez inne oprogramowanie. Jeśli proces klnagent wpływa na działanie tego oprogramowania, zmień ustawienia portu w tym oprogramowaniu lub zmień domyślny dynamiczny zakres portów w systemie operacyjnym, aby wykluczyć port używany przez oprogramowanie, którego dotyczy problem.

Należy również wziąć pod uwagę, że zalecenia dotyczące kompatybilności Kaspersky Security Center z oprogramowaniem innych firm zostały opisane wyłącznie w celach informacyjnych i mogą nie mieć zastosowania do nowych wersji oprogramowania innych firm. Opisane zalecenia dotyczące konfiguracji portów zostały oparte na doświadczeniach działu pomocy technicznej i naszych najlepszych praktykach.

Poniższa tabela wyświetla porty, które muszą być otwarte na zarządzanym urządzeniu z zainstalowanym Agentem sieciowym pełniącym rolę punktu dystrybucji. Wymienione porty muszą być otwarte na urządzeniach punktu dystrybucji oprócz portów używanych przez Agentów sieciowych (patrz tabela powyżej).

Porty używane przez Agenta sieciowego pełniącego rolę punktu dystrybucji

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
13000	klnagent	TCP (TLS)	Odbieranie połączeń od Agentów sieciowych i od Kaspersky Security Center, gdy punkt dystrybucji działa jako brama połączenia w DMZ. Jeśli urządzenie z zainstalowanym serwerem administracyjnym zostało określone jako punkt dystrybucji, do połączenia SSL domyślnie używany jest port 13 001 zamiast 13 000.	Zarządzanie urządzeniami klienckimi, dostarczanie uaktualnień i pakietów instalacyjnych. Aby uzyskać szczegółowe informacje, zobacz następujący temat: Serwer administracyjny, brama połączenia w segmencie sieci i urządzenie klienckie. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
13111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	TCP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
15111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	UDP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
17111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	HTTPS	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
13295 (tylko wtedy, gdy używasz punktu dystrybucji jako serwera push)	klnagent	TCP (TLS)	Obieranie połączeń od urządzeń klienckich	Serwer push. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.

Poniższa tabela przedstawia porty używane na urządzeniu kontrolera domeny.

Porty używane na urządzeniu kontrolera domeny

Numer portu	Protokół	Przeznaczenie portu	Obszar
389	LDAP przez TCP lub UDP	Łączenie z serwerem LDAP	Przeszukiwanie kontrolera domeny
636	LDAP przez TLS	Łączenie z serwerem LDAP	Przeszukiwanie kontrolera domeny

Poniższa tabela zawiera port, który musi być otwarty na urządzeniach klienckich, na których jest zainstalowany Agent sieciowy.

Port używany na nieprzypisanym urządzeniu klienckim

Numer portu	Protokół	Przeznaczenie portu	Obszar
22	SSH	Łączenie się z urządzeniem klienckim przez SSH	Tylko dla urządzeń klienckich z systemem Linux. Instalacja zdalna aplikacji Kaspersky za pośrednictwem punktu dystrybucji Linux.

Certyfikaty do pracy z Kaspersky Security Center

Ta sekcja zawiera informacje o certyfikatach Kaspersky Security Center i opisuje, jak wystawić niestandardowy certyfikat dla serwera administracyjnego.

Informacje o certyfikatach Kaspersky Security Center

Kaspersky Security Center używa następujących typów certyfikatów w celu włączenia interakcji między składnikami aplikacji:

- Certyfikatu Serwera administracyjnego
- Certyfikat mobilny
- Certyfikat serwera iOS MDM
- Certyfikat Kaspersky Security Center Web Server
- Certyfikat Kaspersky Security Center Web Console

Domyślnie, Kaspersky Security Center używa certyfikatów z podpisem własnym (czyli takich, które zostały opublikowane przez sam program Kaspersky Security Center), ale możesz zastąpić je z certyfikatami niestandardowymi, aby lepiej spełniały wymagania sieci w Twojej organizacji i były zgodne ze standardami bezpieczeństwa. Po zweryfikowaniu przez Serwer administracyjny, czy certyfikat niestandardowy spełnia wszystkie odpowiednie wymagania, ten certyfikat obejmuje ten sam obszar funkcyjny jak certyfikat z podpisem własnym. Jedyna różnica to taka, że certyfikat niestandardowy nie jest ponownie publikowany automatycznie po wygaśnięciu. Możesz zastąpić certyfikaty certyfikatami niestandardowymi przy użyciu narzędzia klsetsrvcert lub poprzez sekcję Właściwości Serwera administracyjnego w Konsoli administracyjnej, w zależności od typu certyfikatu. Podczas korzystania z narzędzia klsetsrvcert należy określić typ certyfikatu przy użyciu jednej z następujących wartości:

- C – typowy certyfikat dla portów 13000 i 13291
- CR – typowy rezerwowy certyfikat dla portów 13000 i 13291
- M – certyfikat mobilny dla portu 13292

- MR – rezerwowy certyfikat mobilny dla portu 13292
- MCA – mobilny urząd certyfikacji dla automatycznie wygenerowanych certyfikatów użytkowników

Nie ma konieczności pobierania narzędzia klsetsrvcert. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center. Narzędzie nie jest kompatybilne z poprzednimi wersjami Kaspersky Security Center.

Maksymalny okres ważności dowolnego certyfikatu Serwera administracyjnego nie może przekraczać 397 dni.

Certyfikaty Serwera administracyjnego

Certyfikat Serwera administracyjnego jest wymagany do autoryzacji Serwera administracyjnego, a także do bezpiecznej interakcji między Serwerem administracyjnym a Agentem sieciowym na zarządzanych urządzeniach lub między głównym Serwerem administracyjnym a podrzędnymi Serwerami administracyjnymi. Po podłączeniu Konsoli administracyjnej do Serwera administracyjnego po raz pierwszy, zostanie wyświetlony komunikat z potwierdzeniem użycia bieżącego certyfikatu Serwera administracyjnego. Takie potwierdzenie jest również wymagane za każdym razem, gdy certyfikat Serwera administracyjnego zostanie wymieniony, po każdej ponownej instalacji Serwera administracyjnego, a także podczas podłączania podrzędnego Serwera administracyjnego do głównego Serwera administracyjnego. Ten certyfikat jest nazywany standardowym („C").

Wspólny certyfikat („C") jest tworzony automatycznie podczas instalacji komponentu Serwer administracyjny. Certyfikat składa się z dwóch części:

- pliku klserver.cer; domyślnie znajduje się na komputerze, na którym zainstalowany jest komponent Serwer administracyjny, w folderze C:\ProgramData\KasperskyLab\adminkit\1093\cert.
- Tajny klucz znajdujący się w magazynie chronionym systemu Windows.

Oprócz tego istnieje wspólny certyfikat rezerwowy („CR"). Kaspersky Security Center automatycznie generuje ten certyfikat na 90 dni przed wygaśnięciem certyfikatu standardowego. Wspólny certyfikat rezerwowy jest dalej używany dla bezproblemowego zastąpienia certyfikat Serwera administracyjnego. Jeśli certyfikat standardowy wkrótce wygaśnie, wspólny certyfikat rezerwowy jest używany do zachowania połączenia z instancjami Agenta sieciowego, zainstalowanymi na zarządzanych urządzeniach. Wspólny certyfikat rezerwowy automatycznie staje się nowym certyfikatem standardowym na 24 godziny przed wygaśnięciem starego certyfikatu standardowego.

Możesz utworzyć kopię zapasową certyfikatu Serwera administracyjnego oddzielnie od innych ustawień Serwera administracyjnego w celu usunięcia Serwera administracyjnego z jednego urządzenia na inne bez utraty danych.

Certyfikaty mobilne

Certyfikat mobilny („M") jest wymagany do autoryzacji Serwera administracyjnego na urządzeniu mobilnym. Możesz skonfigurować użycie certyfikatu mobilnego w dedykowanym kroku Kreator wstępnej konfiguracji.

Poza tym, dostępny jest zapasowy certyfikat mobilny („MR"): jest on używany dla bezproblemowego zastąpienia certyfikatu mobilnego. Kaspersky Security Center automatycznie generuje ten certyfikat na 60 dni przed wygaśnięciem certyfikatu standardowego. Jeśli certyfikat mobilny wkrótce wygaśnie, zapasowy certyfikat mobilny jest używany do zachowania połączenia z instancjami Agenta sieciowego, zainstalowanymi na zarządzanych urządzeniach mobilnych. Zapasowy certyfikat mobilny automatycznie staje się nowym certyfikatem standardowym na 24 godziny przed wygaśnięciem starego certyfikatu mobilnego.

Jeśli scenariusz połączenia wymaga użycia certyfikatu klienckiego na urządzeniach mobilnych (połączenie obejmujące dwuetapową autoryzację SSL), możesz wygenerować te certyfikaty przy użyciu urzędu certyfikacji dla automatycznie wygenerowanych certyfikatów używanych („MCA"). Poza tym Kreator wstępnej konfiguracji włącza uruchamianie niestandardowych certyfikatów klienckich opublikowanych przez inny urząd certyfikacji, podczas integracji z domeną infrastrukturą kluczy publicznych (PKI) Twojej organizacji włącza publikację certyfikatów klienckich przy użyciu urzędu certyfikacji domeny.

Certyfikat serwera iOS MDM

Certyfikat serwera iOS MDM jest wymagany do autoryzacji Serwera administracyjnego na urządzeniach mobilnych działających pod kontrolą systemu operacyjnego iOS. Interakcja z tymi urządzeniami odbywa się za pośrednictwem protokołu Apple mobile device management (MDM), który nie obejmuje Agenta sieciowego. Zamiast tego instalujesz specjalnego profilu iOS MDM, zawierający certyfikat kliencki, na każdym urządzeniu, aby zapewnić dwuetapową autoryzację SSL.

Poza tym Kreator wstępnej konfiguracji włącza uruchamianie niestandardowych certyfikatów klienckich opublikowanych przez inny urząd certyfikacji, podczas integracji z domeną infrastrukturą kluczy publicznych (PKI) Twojej organizacji włącza publikację certyfikatów klienckich przy użyciu urzędu certyfikacji domeny.

Certyfikaty klienckie są transmitowane na urządzenia iOS, gdy pobierzesz ten profil iOS MDM. Certyfikat klienta iOS MDM Server jest unikalny w przypadku każdego zarządzanego urządzenia z systemem iOS. Wygenerujesz wszystkie certyfikaty klienckie serwera iOS MDM przy użyciu urzędu certyfikacji dla automatycznie wygenerowanych certyfikatów użytkownika („MCA").

Certyfikat Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (zwany dalej Serwerem sieciowym), składnik Serwera administracyjnego Kaspersky Security Center, używa specjalnego typu certyfikatu. Ten certyfikat jest wymagany do publikowania pakietów instalacyjnych Agenta sieciowego, które są następnie pobierane na zarządzane urządzenia, a także do publikowania profili iOS MDM, aplikacji iOS i pakietów instalacyjnych Kaspersky Security for Mobile. W tym celu serwer sieciowy może użyć różnych certyfikatów.

Jeśli obsługa urządzenia mobilnego jest wyłączona, serwer sieciowy używa jednego z następujących certyfikatów w kolejności priorytetów:

1. Niestandardowy certyfikat serwer sieciowy, który określiłeś ręcznie przy użyciu Konsoli administracyjnej

2. Niestandardowy certyfikat Serwera administracyjnego („C")

Jeśli obsługa urządzenia mobilnego jest włączona, serwer sieciowy używa jednego z następujących certyfikatów w kolejności priorytetów:

1. Niestandardowy certyfikat serwer sieciowy, który określiłeś ręcznie przy użyciu Konsoli administracyjnej
2. Niestandardowy certyfikat mobilny
3. Certyfikat mobilny z podpisem własnym („M")
4. Niestandardowy certyfikat Serwera administracyjnego („C")

Certyfikat Kaspersky Security Center Web Console

Serwer Kaspersky Security Center Web Console (zwany dalej Web Console) posiada własny certyfikat. Po otwarciu witryny przeglądarka sprawdza, czy połączenie jest zaufane. Certyfikat Web Console umożliwia uwierzytelnianie Web Console i jest używany do szyfrowania ruchu między przeglądarką a Web Console.

Po otworzeniu Web Console przeglądarka informuje użytkownika, że połączenie z Web Console nie jest prywatne oraz że certyfikat Web Console jest nieprawidłowy. Takie ostrzeżenie pojawia się, ponieważ certyfikat Web Console jest certyfikatem z podpisem własnym i jest automatycznie generowany przez Kaspersky Security Center. Aby usunąć to ostrzeżenie, możesz wykonać jedną z następujących czynności:

- Zastąp certyfikat Web Console certyfikatem niestandardowym (opcja zalecana). Utwórz certyfikat, który jest zaufany w Twojej infrastrukturze i spełnia wymagania certyfikatów niestandardowych.
- Dodaj certyfikat Web Console do listy zaufanych certyfikatów przeglądarki. Zalecamy korzystanie z tej opcji tylko wtedy, gdy nie można utworzyć certyfikatu niestandardowego.

Informacje o certyfikacie Serwera administracyjnego

Dwie operacje wykonywane są w oparciu o *Certyfikat Serwera administracyjnego:* Uwierzytelnianie Serwera administracyjnego podczas połączenia przez Konsolę administracyjną i wymianę danych z urządzeniami. Certyfikat jest także używany do uwierzytelniania, gdy główne Serwery administracyjne nawiązują połączenie z podrzędnymi Serwerami administracyjnymi.

Certyfikat wydany przez Kaspersky

Certyfikat Serwera administracyjnego jest tworzony automatycznie w trakcie instalacji modułu Serwera administracyjnego i jest przechowywany w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Certyfikat Serwera administracyjnego jest ważny przez pięć lat, jeśli został wygenerowany przez Serwer administracyjny w wersji 12.2 lub wcześniejszej. W przeciwnym razie okres ważności certyfikatu jest ograniczony 397 dni. Nowy certyfikat jest generowany na Serwerze administracyjnym jako zapasowy certyfikat na 90 dni przed datą wygaśnięcia bieżącego certyfikatu. Następnie, nowy certyfikat automatycznie zastępuje bieżący certyfikat dzień przed datą wygaśnięcia. Wszystkie Agenty sieciowe na urządzeniach klienckich są automatycznie ponownie konfigurowane do autoryzacji na Serwerze administracyjnym przy użyciu nowego certyfikatu.

Certyfikaty niestandardowe

Jeśli to konieczne, możesz przypisać certyfikat innej firmy dla Serwera administracyjnego. Na przykład, to może być konieczne w celu zapewnienia lepszej integracji z istniejącą PKI Twojej firmy lub w celu przeprowadzenia konfiguracji niestandardowej pól certyfikatu.

Maksymalny okres ważności dowolnego certyfikatu Serwera administracyjnego nie może przekraczać 397 dni.

Podczas zamiany certyfikatu, wszystkie Agenty sieciowe, które wcześniej były połączone z Serwerem administracyjnym za pomocą protokołu SSL, utracą połączenie i zwrócą "Błąd autoryzacji Serwera administracyjnego". Aby wyeliminować ten błąd, będziesz musiał przywrócić połączenie po zastąpieniu certyfikatu.

Jeśli certyfikat Serwera administracyjnego zostanie utracony, aby go odzyskać, musisz ponownie zainstalować moduł Serwera administracyjnego, a następnie przywrócić dane.

Jeżeli otworzysz Kaspersky Security Center Web Console w różnych przeglądarkach i pobierzesz plik certyfikatu Serwera administracyjnego w oknie właściwości Serwera administracyjnego, pobrane pliki będą miały różne nazwy.

Wymagania dotyczące niestandardowych certyfikatów stosowanych w Kaspersky Security Center

Poniższa tabela wyświetla wymagania odnośnie niestandardowych certyfikatów określonych dla różnych komponentów Kaspersky Security Center.

Wymagania wobec certyfikatów Kaspersky Security Center

Typ certyfikatu	Wymagania	Komentarze
Wspólny certyfikat, wspólny certyfikat rezerwowy („C", „CR")	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Ograniczenie długości ścieżki: brak Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie klucza • Podpisywanie CRL Rozszerzone użycie klucza (opcjonalnie): uwierzytelnianie serwera, uwierzytelnianie klienta. Certyfikat musi zawierać prawidłową Alternatywną nazwę podmiotu (SAN), która zawiera adres pętli zwrotnej Serwera administracyjnego: • Dla IPv4: 127.0.0.1 • Dla IPv6: 0:0:0:0:0:0:0:1	Parametr Rozszerzone użycie klucza jest opcjonalny. Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak", ale nie mniejsza niż „1".

Typ certyfikatu	Wymagania	Komentarze
Certyfikat mobilny, mobilny certyfikat rezerwowy („M", „MR")	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Urząd certyfikacji (CA): prawda • Ograniczenie długości ścieżki: brak Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie klucza • Podpisywanie CRL Rozszerzone użycie klucza (opcjonalnie): uwierzytelnianie serwera.	Parametr Rozszerzone użycie klucza jest opcjonalny. Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak", jeśli wspólny certyfikat ma wartość ograniczenia długości ścieżki nie mniejszą niż „1".
Certyfikat Urzędu certyfikacji (CA) dla automatycznie generowanych certyfikatów użytkowników („MCA")	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Urząd certyfikacji (CA): prawda • Ograniczenie długości ścieżki: brak Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie klucza • Podpisywanie CRL Rozszerzone użycie klucza (opcjonalnie): uwierzytelnianie serwera, uwierzytelnianie klienta.	Parametr Rozszerzone użycie klucza jest opcjonalny. Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak", jeśli wspólny certyfikat ma wartość ograniczenia długości ścieżki nie mniejszą niż „1".
Certyfikat serwera sieciowego	Rozszerzone użycie klucza: uwierzytelnianie serwera. Kontener PKCS #12 / PEM, z którego certyfikat jest określony, zawiera cały łańcuch kluczy publicznych. Alternatywna nazwa podmiotu (SAN) certyfikatu jest obecna; czyli wartość pola `subjectAltName` jest ważna. Certyfikat spełnia faktyczne wymagania przeglądarek nałożone na certyfikaty serwera, a także bieżące podstawowe wymagania CA/Browser Forum.	—
Certyfikat Kaspersky Security Center Web Console	Kontener PEM, z którego certyfikat jest określony, zawiera cały łańcuch kluczy publicznych. Alternatywna nazwa podmiotu (SAN) certyfikatu jest obecna; czyli wartość pola `subjectAltName` jest ważna. Certyfikat spełnia faktyczne wymagania przeglądarek nałożone na certyfikaty serwera, a także bieżące podstawowe wymagania CA/Browser Forum.	Zaszyfrowane certyfikaty nie są obsługiwane przez Kaspersky Security Center Web Console.

Scenariusz: Określanie niestandardowego certyfikatu Serwera administracyjnego

Możesz przypisać niestandardowy certyfikat Serwera administracyjnego, na przykład, w celu lepszej integracji z istniejącą infrastrukturą kluczy publicznych (PKI) przedsiębiorstwa lub w celu niestandardowej konfiguracji pól certyfikatu. Dobrym rozwiązaniem jest zastąpienie certyfikatu natychmiast po zainstalowaniu Serwera administracyjnego, a przed zakończeniem działania kreatora wstępnej konfiguracji.

Maksymalny okres ważności dowolnego certyfikatu Serwera administracyjnego nie może przekraczać 397 dni.

Wymagania wstępne

Muszą być spełnione następujące warunki:

- Nowy certyfikat musi zostać utworzony w formacie PKCS#12 (na przykład za pomocą infrastruktury klucza publicznego (PKI) organizacji).
- W przypadku nowego certyfikatu należy spełnić wymagania wymienione w poniższej tabeli.

  W poniższej tabeli zwróć uwagę na wymaganie „CA: true", które oznacza, że nowy certyfikat musi zostać wydany przez zaufany urząd certyfikacji (CA). Nowy certyfikat z wymaganiem „CA: true", musi zawierać cały łańcuch zaufania oraz klucz prywatny, który musi być przechowywany w pliku z rozszerzeniem pfx lub p12.

Wymagania dotyczące certyfikatów Serwera administracyjnego

Typ certyfikatu	Wymagania
Certyfikat standardowy, standardowy certyfikat zapasowy („C", „CR")	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Ograniczenie długości ścieżki: brak Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak", ale nie mniejsza niż „1". Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie klucza • Podpisywanie CRL Rozszerzone użycie klucza (EKU): uwierzytelnianie serwera i uwierzytelnianie klienta. Jednostka EKU jest opcjonalna, ale jeśli zawiera ją certyfikat, dane uwierzytelniania serwera i klienta muszą być określone w jednostce EKU. Certyfikat musi zawierać prawidłową Alternatywną nazwę podmiotu (SAN). Pole `subjectAltName` musi zawierać adres pętli zwrotnej Serwera administracyjnego: • Dla IPv4: 127.0.0.1 • Dla IPv6: 0:0:0:0:0:0:0:1
Certyfikat mobilny, zapasowy certyfikat mobilny („M", „MR")	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Urząd certyfikacji (CA): prawda • Ograniczenie długości ścieżki: brak Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak", jeśli standardowy certyfikat ma wartość ograniczenia długości ścieżki nie mniejszą niż 1. Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie klucza • Podpisywanie CRL Rozszerzone użycie klucza (EKU): uwierzytelnianie serwera. Jednostka EKU jest opcjonalna, ale jeśli zawiera ją certyfikat, dane uwierzytelniania serwera muszą być określone w jednostce EKU.

Typ certyfikatu	Wymagania
Certyfikat Urzędu certyfikacji (CA) dla automatycznie generowanych certyfikatów użytkowników („MCA")	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Urząd certyfikacji (CA): prawda • Ograniczenie długości ścieżki: brak Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak", jeśli Standardowy certyfikat ma wartość ograniczenia długości ścieżki nie mniejszą niż 1. Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie klucza • Podpisywanie CRL Rozszerzone użycie klucza (EKU): uwierzytelnianie klienta. Jednostka EKU jest opcjonalna, ale jeśli zawiera ją certyfikat, dane uwierzytelniania klienta muszą być określone w jednostce EKU.

Certyfikaty wystawione przez publiczny urząd certyfikacji nie mają uprawnień do podpisywania certyfikatów. Aby korzystać z takich certyfikatów, upewnij się, że zainstalowałeś Agenta sieciowego w wersji 13 lub nowszej w punktach dystrybucji lub bramach połączeń w swojej sieci. W przeciwnym razie nie będziesz mógł korzystać z certyfikatów bez pozwolenia na podpisywanie.

Etapy

Określanie certyfikatu Serwera administracyjnego odbywa się w etapach:

1. **Zastępowanie certyfikatu Serwera administracyjnego**

   W tym celu użyj polecenia narzędzie klsetsrvcert.

2. **Określanie nowego certyfikatu i przywracanie połączenia Agentów sieciowych z Serwerem administracyjnym**

   Podczas zamiany certyfikatu, wszystkie Agenty sieciowe, które wcześniej były połączone z Serwerem administracyjnym za pomocą protokołu SSL, utracą połączenie i zwrócą „Błąd autoryzacji Serwera administracyjnego". Aby określić nowy certyfikat i przywrócić połączenie, użyj polecenia narzędzia klmover.

3. **Określenie nowego certyfikatu w ustawieniach Kaspersky Security Center Web Console**

   Po wymianie certyfikatu określ go w ustawieniach Kaspersky Security Center Web Console. W przeciwnym razie Kaspersky Security Center Web Console nie będzie mógł nawiązać połączenia z Serwerem administracyjnym.

Wyniki

Po zakończeniu scenariusza, certyfikat Serwera administracyjnego jest zastępowany i serwer zostaje uwierzytelniony przez Agentów sieciowych na zarządzanych urządzeniach.

Zastępowanie certyfikatu Serwera administracyjnego za pomocą narzędzia klsetsrvcert

W celu zastąpienia certyfikatu Serwera administracyjnego:

W wierszu polecenia uruchom następujące narzędzie:

```
klsetsrvcert [-t <typ certyfikatu> {-i <ścieżka do nowego certyfikatu> [-p <hasło>] [-o <parametry>] | -g <nazwa DNS>}][-f <czas zastąpienia>][-r <certyfikaty główne>][-l <ścieżka do pliku dziennika>]
```

Nie ma konieczności pobierania narzędzia klsetsrvcert. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center. Nie jest kompatybilne z poprzednimi wersjami Kaspersky Security Center.

Opis parametrów narzędzia klsetsrvcert przedstawia poniższa tabela.

Wartości parametrów narzędzia klsetsrvcert

Parametr	Wartość
`-t < typ certyfikatu >`	Typ zastępowanego certyfikatu. Możliwe wartości parametru `< typ certyfikatu >` to: • `C` – zastępuje certyfikat standardowy dla portów 13000 i 13291. • `CR` – zastępuje zapasowy certyfikat standardowy dla portów 13000 i 13291. • `M` – Zastępuje certyfikat dla urządzeń mobilnych na porcie 13292. • `MR` – Zastępuje zapasowy certyfikat mobilny dla portu 13292. • `MCA` – Mobilny urząd certyfikacji dla automatycznie wygenerowanych certyfikatów użytkowników.
`-f < czas zastąpienia >`	Terminarz zmiany certyfikatu w formacie „DD-MM-YYYY hh:mm" (dla portów: 13000 i 13291). Użyj tego parametru, jeśli chcesz zastąpić certyfikat standardowy zapasowym certyfikatem standardowym przed wygaśnięciem certyfikatu standardowego. Określ czas, w którym zarządzane urządzenia muszą synchronizować się z Serwerem administracyjnym na nowym certyfikacie.
`-i < ścieżka do nowego certyfikatu >`	Kontener z certyfikatem i kluczem prywatnym w formacie PKCS#12 (plik z rozszerzeniem .p12 lub .pfx).
`-p < hasło >`	Hasło używane do ochrony kontenera p12. Certyfikat i klucz prywatny są przechowywane w kontenerze, dlatego do odszyfrowania pliku z kontenerem wymagane jest hasło.
`-o < parametry walidacji >`	Parametry legalizacji certyfikatu (oddzielone średnikiem). Aby użyć certyfikatu niestandardowego bez uprawnień do podpisywania, określ `-o NoCA` w narzędziu klsetsrvcert. Jest to przydatne w przypadku certyfikatów wydanych przez publiczny urząd certyfikacji. Aby zmienić długość klucza szyfrowania dla certyfikatów typu C lub CR, w narzędziu klsetsrvcert określ parametr `-o RsaKeyLen:< długość klucza >`, gdzie parametr `< długość klucza >` jest wymaganą wartością długości klucza. W przeciwnym razie używana jest bieżąca długość klucza certyfikatu.
`-g < nazwa DNS >`	Nowy certyfikat zostanie utworzony dla określonej nazwy DNS.
`-r < certyfikaty główne >`	Lista zaufanych urzędów certyfikacji w formacie PEM.
`-l < ścieżka do pliku dziennika >`	Zapisuje dane wynikowe. Domyślnie dane wynikowe są przekierowywane do standardowego strumienia wyjściowego.

Na przykład, aby określić niestandardowy certyfikat Serwera administracyjnego, użyj następującego polecenia:

```
klsetsrvcert -t C -i <ścieżka do nowego certyfikatu> -p <hasło> -o NoCA
```

Po zastąpieniu certyfikatu wszystkie Agenty sieciowe połączone z Serwerem administracyjnym przez SSL tracą połączenie. Aby je przywrócić, użyj polecenia narzędzia klmover.

Aby uniknąć utraty połączeń z Agentami sieciowymi, użyj następującego polecenia:

1. Aby zainstalować nowy certyfikat,

```
klsetsrvcert.exe -t CR -i <ścieżka do nowego certyfikatu> -p <hasło> -o NoCA
```

2. Aby określić datę stosowania nowego certyfikatu,

```
klsetsrvcert.exe -f "DD-MM-YYYY hh:mm"
```

gdzie „`DD-MM-YYYY hh:mm`" to data 3–4 tygodnie po dacie bieżącej. Przesunięcie czasowe zmiany certyfikatu na nowy pozwoli na rozesłanie nowego certyfikatu do wszystkich Agentów sieciowych.

Podłączanie Agentów sieciowych do Serwera administracyjnego przy użyciu narzędzia klmover

Po zastąpieniu certyfikatu Serwera administracyjnego za pomocą polecenia narzędzia klsetsrvcert, musisz nawiązać połączenie SSL między Agentami sieciowymi a Serwerem administracyjnym, ponieważ połączenie jest zerwane.

W celu określenia nowego certyfikatu Serwera administracyjnego i przywrócenia połączenia:

W wierszu polecenia uruchom następujące narzędzie:

```
klmover [-address <adres serwera>] [-pn <numer portu>] [-ps <numer portu SSL>] [-nossl] [-cert <ścieżka do pliku certyfikatu>]
```

Do uruchomienia narzędzia wymagane są uprawnienia administratora.

To narzędzie jest automatycznie kopiowane do folderu instalacyjnego Agenta sieciowego, gdy Agent sieciowy jest instalowany na urządzeniu klienckim.

Aby uniemożliwić intruzom przeniesienie urządzeń poza Serwer administracyjny kontrolujący, zdecydowanie zalecamy włączenie ochrony hasłem podczas uruchamiania narzędzia klmover. Aby włączyć ochronę hasłem, wybierz opcję **Użyj hasła dezinstalacyjnego** w ustawieniach zasady Agenta sieciowego.

Narzędzie klmover wymaga uprawnień administratora lokalnego. Zabezpieczenie hasłem do uruchomienia narzędzia klmover można pominąć w przypadku urządzeń obsługiwanych bez uprawnień administratora lokalnego.

Włączenie opcji **Użyj hasła dezinstalacyjnego** umożliwia również ochronę hasłem narzędzia Cleaner (cleaner.exe).

Narzędzia klmover nie można używać w przypadku urządzeń klienckich podłączonych do Serwera administracyjnego poprzez bramy połączeń. W przypadku takich urządzeń należy albo ponownie skonfigurować Agenta sieciowego, albo ponownie zainstalować Agenta sieciowego i określić bramę połączenia.

Opis parametrów narzędzia klmover przedstawia poniższa tabela.

Wartości parametrów narzędzia klmover

Parametr	Wartość
`-address < adres serwera >`	Adres Serwera administracyjnego do nawiązania połączenia. Można określić adres IP, nazwę NetBIOS lub nazwę DNS.
`-pn < numer portu >`	Numer portu użytego do nawiązania nieszyfrowanego połączenia z Serwerem administracyjnym. Domyślny numer portu to 14000.
`-ps < numer portu SSL >`	Numer portu SSL, przez który nawiązywane jest połączenie szyfrowane z Serwerem administracyjnym (przy użyciu protokołu SSL). Domyślny numer portu to 13000.
`-nossl`	Użycie nieszyfrowanego połączenia z Serwerem administracyjnym. Jeżeli klucz ten nie zostanie użyty, Agent sieciowy nawiąże z Serwerem administracyjnym połączenie szyfrowane przy użyciu szyfrowanego protokołu SSL.
`-cert < ścieżka do pliku certyfikatu >`	Użycie określonego pliku certyfikatu do autoryzacji podczas uzyskiwania dostępu do Serwera administracyjnego.
`-virtserv`	Nazwa wirtualnego Serwera administracyjnego.
`-cloningmode`	Tryb klonowania dysku Agenta sieciowego. Użyj jednego z następujących parametrów, aby skonfigurować tryb klonowania dysku: • `-cloningmode` — Zażądaj stanu trybu klonowania dysku. • `-cloningmode 1` — Włącz tryb klonowania dysku. • `-cloningmode 0` — Wyłącz tryb klonowania dysku.
`-nauninstpwd < hasło >`	Użyj tego parametru, aby określić hasło dezinstalacyjne Agenta sieciowego. Parametr nie jest obowiązkowy.

Na przykład, aby połączyć Agenta sieciowego z Serwerem administracyjnym, uruchom następującą komendę:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Ponowne wystawianie certyfikatu serwera sieciowego

Certyfikat serwera sieciowego używany w Kaspersky Security Center jest wymagany do publikowania pakietów instalacyjnych Agenta sieciowego, które są następnie pobierane na zarządzane urządzenia, a także do publikowania profili iOS MDM, aplikacji iOS oraz pakietów instalacyjnych Kaspersky Endpoint Security for Mobile. W zależności od bieżącej konfiguracji aplikacji różne certyfikaty mogą funkcjonować jako certyfikat serwera sieciowego (aby uzyskać więcej informacji, zobacz Informacje o certyfikatach Kaspersky Security Center).

Ponowne wystawienie certyfikatu serwera sieciowego może być konieczne w celu spełnienia określonych wymagań bezpieczeństwa organizacji lub utrzymania ciągłego połączenia z zarządzanymi urządzeniami przed rozpoczęciem aktualizacji aplikacji. Kaspersky Security Center zapewnia dwa sposoby ponownego wystawienia certyfikatu serwera sieciowego. Wybór między tymi dwiema metodami zależy od tego, czy masz podłączone urządzenia mobilne i zarządzane za pośrednictwem protokołu mobilnego (tj. przy użyciu certyfikatu mobilnego).

Jeśli nigdy nie określono własnego certyfikatu niestandardowego jako certyfikatu serwera sieciowego w sekcji **Serwer WWW** właściwości Serwera administracyjnego, certyfikat mobilny działa jako certyfikat serwera sieciowego. W tym przypadku ponowne wystawienie certyfikatu serwera sieciowego odbywa się poprzez ponowne wystawienie samego protokołu mobilnego.

Aby ponownie wystawić certyfikat serwera sieciowego, gdy nie masz żadnych urządzeń mobilnych zarządzanych za pośrednictwem protokołu mobilnego:

1. W drzewie konsoli kliknij prawym przyciskiem myszy nazwę odpowiedniego Serwera administracyjnego i z menu kontekstowego wybierz **Właściwości**.

2. W otwartym oknie właściwości Serwera administracyjnego, w lewym panelu wybierz sekcję **Ustawienia połączenia z Serwerem administracyjnym**.

3. Na liście podsekcji wybierz **Certyfikaty**.

4. Jeśli planujesz nadal używać certyfikatu wystawionego przez Kaspersky Security Center, wykonaj następujące czynności:

   a. W prawym okienku, w grupie ustawień **Uwierzytelnianie Serwera administracyjnego przez urządzenia mobilne** wybierz opcję **Certyfikat wydany przez Serwer administracyjny** i kliknij przycisk **Wydaj ponownie**.

   b. W otwartym oknie **Wydaj certyfikat ponownie**, w grupach ustawień **Adres połączenia** i **Czas aktywacji** wybierz odpowiednie opcje i kliknij przycisk **OK**.

   c. W oknie potwierdzenia kliknij przycisk **Tak**.

   Alternatywnie, jeśli planujesz używać własnego certyfikatu niestandardowego, wykonaj następujące czynności:

   a. Sprawdź, czy Twój certyfikat niestandardowy spełnia wymagania Kaspersky Security Center Linux. W razie potrzeby zmodyfikuj certyfikat.

   b. Wybierz opcję **Inny certyfikat** i kliknij przycisk **Przeglądaj**.

   c. W otwartym oknie **Certyfikat**, w polu **Typ certyfikatu** wybierz typ swojego certyfikatu, a następnie określ lokalizację i ustawienia certyfikatu:

      - Jeśli został wybrany typ **Kontener PKCS #12**, kliknij przycisk **Przeglądaj** obok pola **Plik certyfikatu** i określ plik certyfikatu na dysku twardym. Jeśli plik certyfikatu jest chroniony hasłem, wprowadź hasło w polu **Hasło (jeśli istnieje)**.

      - Jeśli został wybrany typ **Certyfikat X.509**, kliknij przycisk **Przeglądaj** obok pola **Klucz prywatny (.prk, .pem)** i określ klucz prywatny na dysku twardym. Jeśli klucz prywatny jest chroniony hasłem, wprowadź hasło w polu **Hasło (jeśli istnieje)**. Następnie kliknij przycisk **Przeglądaj** obok pola **Klucz publiczny (.cer)** i określ klucz prywatny na dysku twardym.

   d. W oknie **Certyfikat** kliknij **OK**.

   e. W oknie potwierdzenia kliknij przycisk **Tak**.

   Certyfikat mobilny został ponownie wystawiony w celu używania go jako certyfikat serwera sieciowego.

Aby ponownie wystawić certyfikat serwera sieciowego, gdy masz jakiekolwiek urządzenia mobilne zarządzane za pośrednictwem protokołu mobilnego:

1. Wygeneruj swój certyfikat niestandardowy i przygotuj go do użycia w Kaspersky Security Center. Sprawdź, czy Twój certyfikat niestandardowy spełnia wymagania Kaspersky Security Center Linux. W razie potrzeby zmodyfikuj certyfikat.

2. W drzewie konsoli kliknij prawym przyciskiem myszy nazwę odpowiedniego Serwera administracyjnego i z menu kontekstowego wybierz **Właściwości**.

3. W otwartym oknie właściwości Serwera administracyjnego, w lewym panelu wybierz sekcję **Serwer WWW**.

4. W menu **Przez HTTPS** wybierz opcję **Określ inny certyfikat**.

5. W menu **Przez HTTPS** kliknij przycisk **Zmień**.

6. W otwartym oknie **Certyfikat**, w polu **Typ certyfikatu** wybierz typ swojego certyfikatu:

   - Jeśli został wybrany typ **Kontener PKCS #12**, kliknij przycisk **Przeglądaj** obok pola **Plik certyfikatu** i określ plik certyfikatu na dysku twardym. Jeśli plik certyfikatu jest chroniony hasłem, wprowadź hasło w polu **Hasło (jeśli istnieje)**.

   - Jeśli został wybrany typ **Certyfikat X.509**, kliknij przycisk **Przeglądaj** obok pola **Klucz prywatny (.prk, .pem)** i określ klucz prywatny na dysku twardym. Jeśli klucz prywatny jest chroniony hasłem, wprowadź hasło w polu **Hasło (jeśli istnieje)**. Następnie kliknij przycisk **Przeglądaj** obok pola **Klucz publiczny (.cer)** i określ klucz prywatny na dysku twardym.

7. W oknie **Certyfikat** kliknij przycisk **OK**.

8. Jeśli to konieczne, w oknie właściwości Serwera administracyjnego, w polu **Port HTTPS serwera WWW** zmień numer portu HTTPS dla serwera sieciowego. Kliknij **OK**.

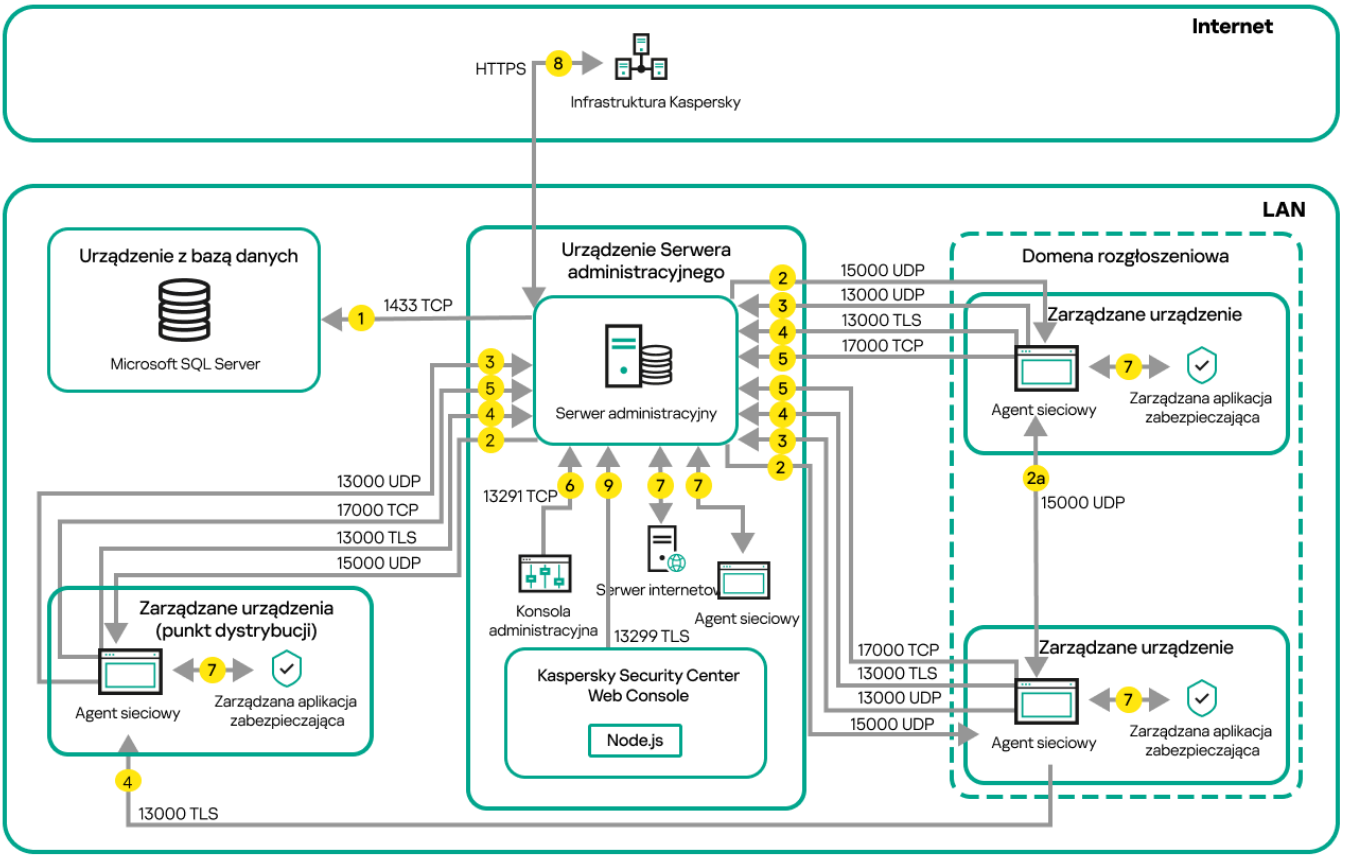
   Certyfikat serwera sieciowego został ponownie wystawiony.

Schematy ruchu sieciowego danych i użycia portów

Ta sekcja zawiera schematy ruchu sieciowego danych między komponentami Kaspersky Security Center, zarządzanymi aplikacjami zabezpieczającymi i serwerami zewnętrznymi w różnych konfiguracjach. Schematy są dostarczane z numerami portów, które muszą być dostępne na urządzeniach lokalnych.

Serwer administracyjny i zarządzane urządzenia w sieci LAN

Poniższy rysunek przedstawia ruch sieciowy danych, gdy Kaspersky Security Center jest zainstalowany tylko w sieci lokalnej (LAN).



Serwer administracyjny i zarządzane urządzenia w sieci lokalnej (LAN)

Rysunek przedstawia sposób, w jaki różne zarządzane urządzenia nawiązują połączenie z Serwerem administracyjnym na różne sposoby: bezpośrednio lub poprzez punkt dystrybucji. Punkty dystrybucji zmniejszają obciążenie na Serwerze administracyjnym podczas dystrybucji aktualizacji i optymalizowania ruchu sieciowego. Jednakże punkty dystrybucji są potrzebne tylko wtedy, gdy liczba zarządzanych urządzeń jest wystarczająco duża. Jeśli liczba zarządzanych urządzeń jest mała, wszystkie zarządzane urządzenia mogą pobierać uaktualnienia bezpośrednio z Serwera administracyjnego.

Strzałki wskazują inicjowanie ruchu sieciowego: każda strzałka wskazuje kierunek z urządzenia, które inicjuje połączenie, do urządzenia, które „odpowiada" na połączenie. Dostarczony jest numer portu oraz nazwa protokołu użytego do przesyłania danych. Każda strzałka posiada etykietę liczby, a szczegóły dotyczące odpowiedniego ruchu danych wyglądają następująco:

1. Serwer administracyjny wysyła dane do bazy danych. Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server lub port 1433 dla Microsoft SQL Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2. Żądania komunikacji od Serwera administracyjnego są przesyłane do wszystkich niemobilnych zarządzanych urządzeń poprzez port UDP o numerze 15000.

   Agenty sieciowe wysyłają żądania do siebie nawzajem w obrębie jednej domeny broadcastowej. Dane są następnie wysyłane do Serwera administracyjnego i są używane do określenia ograniczeń domeny broadcastowej i do automatycznego przydzielenia punktów dystrybucji (jeśli ta opcja jest włączona).

Jeżeli Serwer administracyjny nie ma bezpośredniego dostępu do zarządzanych urządzeń, żądania komunikacji z Serwera administracyjnego nie są wysyłane bezpośrednio do tych urządzeń.

3. Informacje o zamknięciu zarządzanych urządzeń są przesyłane z Agenta sieciowego do Serwera administracyjnego poprzez port UDP o numerze 13000.

4. Serwer administracyjny odbiera połączenie od Agentów sieciowych i podrzędnych Serwerów administracyjnych poprzez port TLS o numerze 13000.

   Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port inny niż TLS o numerze 14000. Kaspersky Security Center obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu TLS o numerze 13000.

   > We wcześniejszych wersjach Kaspersky Security Center punkt dystrybucji nosił nazwę „Agent aktualizacji".

5. Zarządzane urządzenia (za wyjątkiem urządzeń mobilnych) żądają aktywacji poprzez port TCP o numerze 17000. Nie jest to konieczne, jeśli urządzenie posiada własny dostęp do Internetu; w tym przypadku urządzenie wysyła dane do serwerów Kaspersky bezpośrednio przez Internet.

6. Dane z Konsoli administracyjnej opartej na konsoli MMC zostaną przesłane do Serwera administracyjnego poprzez port 13291 (Konsola administracyjna może zostać zainstalowana na tym samym lub na innym urządzeniu).

7. Lokalny ruch sieciowy aplikacji na pojedynczym urządzeniu (na Serwerze administracyjnym lub na zarządzanym urządzeniu). Żadne porty zewnętrzne nie muszą być otwarte.

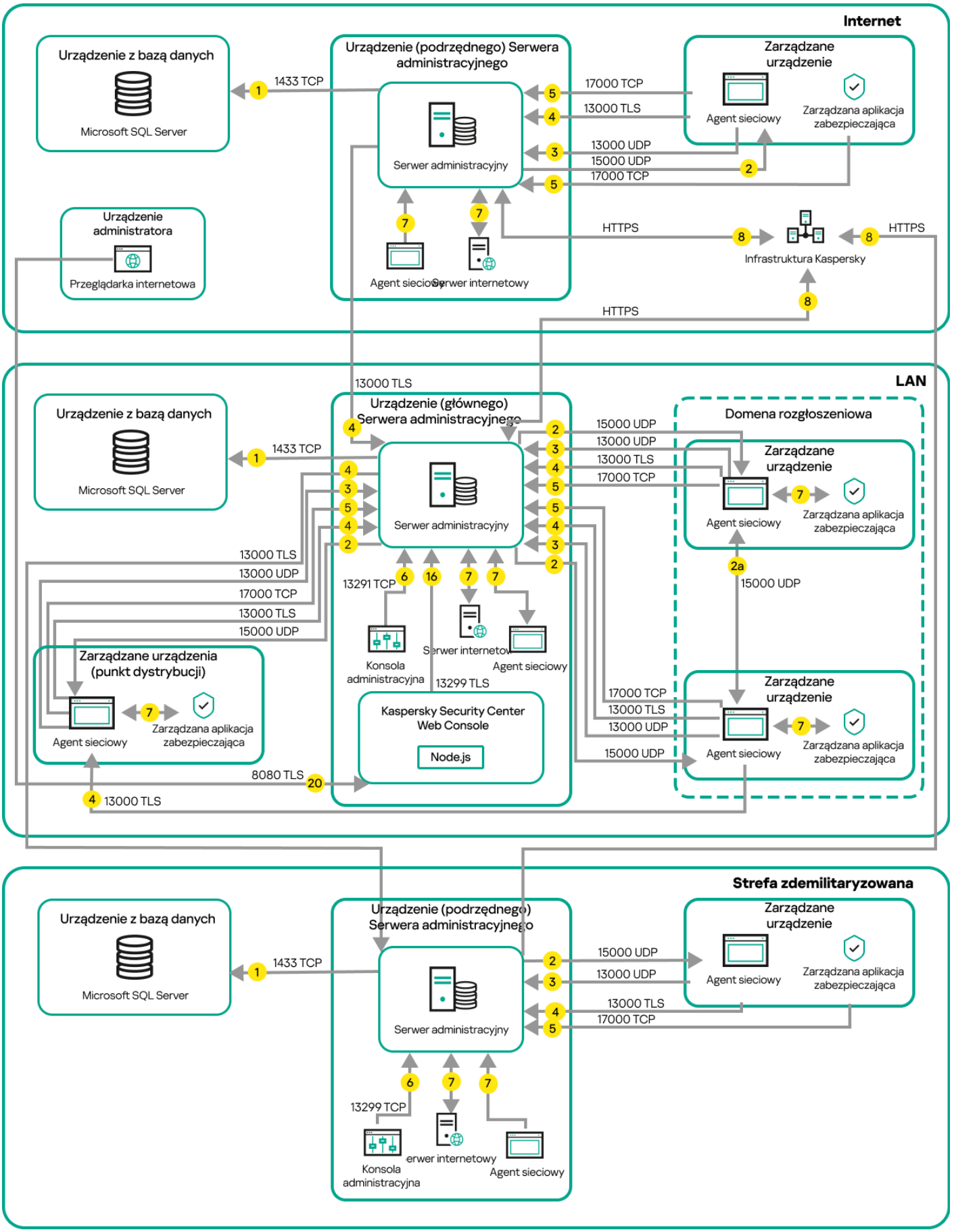
8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do Internetu, musisz ręcznie zarządzać tymi danymi.

9. Kaspersky Security Center Web Console Server wysyła dane na Serwer administracyjny, który może być zainstalowany na tym samym lub innym urządzeniu, poprzez port TLS o numerze 13299.

Główny Serwer administracyjny w sieci LAN i dwa podrzędne Serwery administracyjne

Poniższy rysunek przedstawia hierarchię Serwerów administracyjnych: główny Serwer administracyjny znajduje się w sieci lokalnej (LAN). Podrzędny Serwer administracyjny znajduje się w strefie zdemilitaryzowanej (DMZ); inny podrzędny Serwer administracyjny znajduje się w Internecie.



Hierarchia Serwerów administracyjnych: główny Serwer administracyjny i dwa podrzędne Serwery administracyjne

Strzałki wskazują inicjowanie ruchu sieciowego: każda strzałka wskazuje kierunek z urządzenia, które inicjuje połączenie, do urządzenia, które „odpowiada" na połączenie. Dostarczony jest numer portu oraz nazwa protokołu użytego do przesyłania danych. Każda strzałka posiada etykietę liczby, a szczegóły dotyczące odpowiedniego ruchu danych wyglądają następująco:

1. Serwer administracyjny wysyła dane do bazy danych. Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server lub port 1433 dla Microsoft SQL Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2. Żądania komunikacji od Serwera administracyjnego są przesyłane do wszystkich niemobilnych zarządzanych urządzeń poprzez port UDP o numerze 15000.

   Agenty sieciowe wysyłają żądania do siebie nawzajem w obrębie jednej domeny broadcastowej. Dane są następnie wysyłane do Serwera administracyjnego i są używane do określenia ograniczeń domeny broadcastowej i do automatycznego przydzielenia punktów dystrybucji (jeśli ta opcja jest włączona).

   Jeżeli Serwer administracyjny nie ma bezpośredniego dostępu do zarządzanych urządzeń, żądania komunikacji z Serwera administracyjnego nie są wysyłane bezpośrednio do tych urządzeń.

3. Informacje o zamknięciu zarządzanych urządzeń są przesyłane z Agenta sieciowego do Serwera administracyjnego poprzez port UDP o numerze 13000.

4. Serwer administracyjny odbiera połączenie od Agentów sieciowych i podrzędnych Serwerów administracyjnych poprzez port TLS o numerze 13000.

   Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port inny niż TLS o numerze 14000. Kaspersky Security Center obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu TLS o numerze 13000.

   > We wcześniejszych wersjach Kaspersky Security Center punkt dystrybucji nosił nazwę „Agent aktualizacji".

5. Zarządzane urządzenia (za wyjątkiem urządzeń mobilnych) żądają aktywacji poprzez port TCP o numerze 17000. Nie jest to konieczne, jeśli urządzenie posiada własny dostęp do Internetu; w tym przypadku urządzenie wysyła dane do serwerów Kaspersky bezpośrednio przez Internet.

6. Dane z Konsoli administracyjnej opartej na konsoli MMC zostaną przesłane do Serwera administracyjnego poprzez port 13291 (Konsola administracyjna może zostać zainstalowana na tym samym lub na innym urządzeniu).

7. Lokalny ruch sieciowy aplikacji na pojedynczym urządzeniu (na Serwerze administracyjnym lub na zarządzanym urządzeniu). Żadne porty zewnętrzne nie muszą być otwarte.

8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

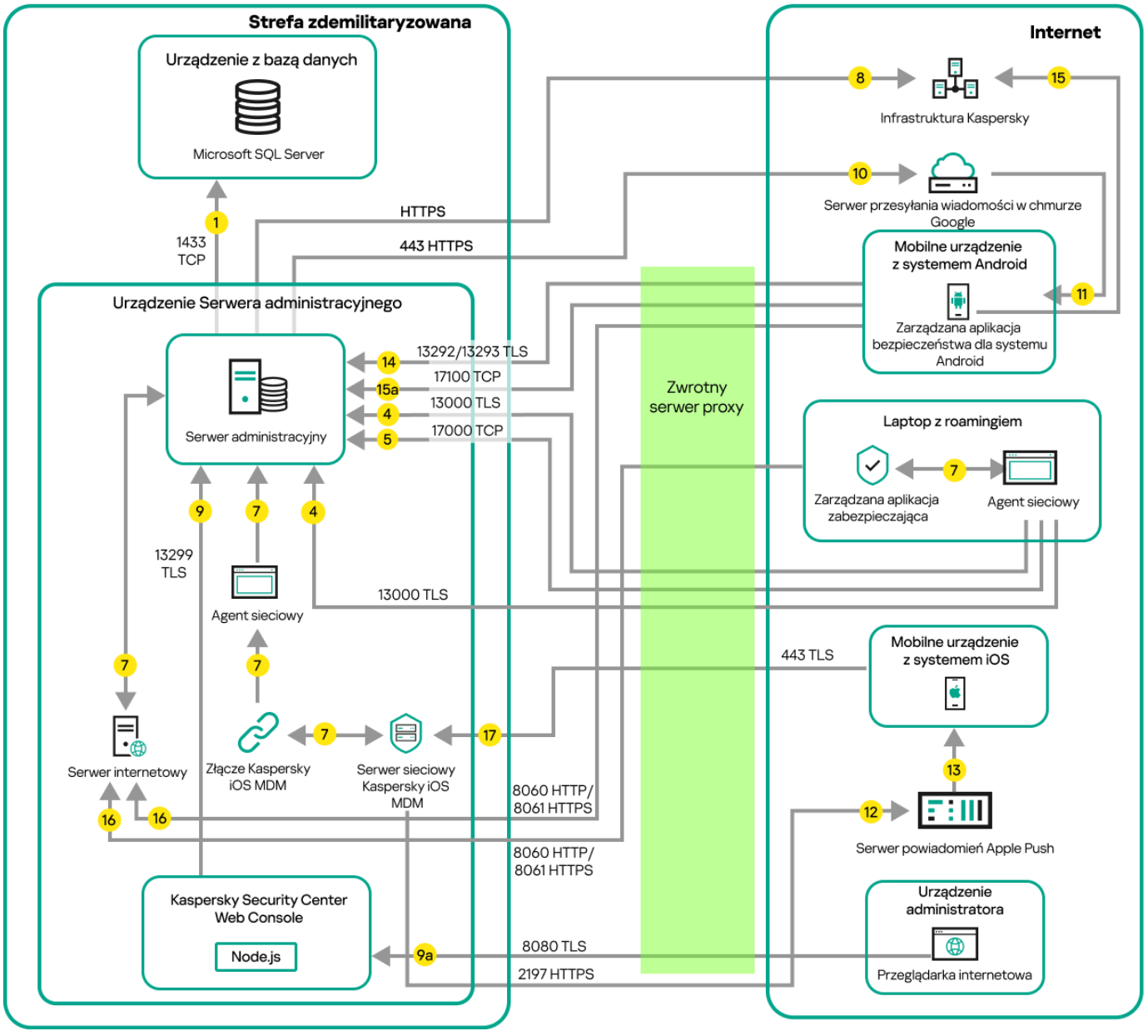
   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do Internetu, musisz ręcznie zarządzać tymi danymi.

9. Kaspersky Security Center Web Console Server wysyła dane na Serwer administracyjny, który może być zainstalowany na tym samym lub innym urządzeniu, poprzez port TLS o numerze 13299.

   9a. Dane z przeglądarki, która jest zainstalowana na oddzielnym urządzeniu administratora, są przesyłane do Kaspersky Security Center Web Console Server poprzez port TLS o numerze 8080. Kaspersky Security Center Web Console Server może zostać zainstalowany na Serwerze administracyjnym lub na innym urządzeniu.

Serwer administracyjny w sieci LAN, zarządzane urządzenia w Internecie, odwrotny serwer proxy w użyciu

Poniższy rysunek przedstawia ruch sieciowy danych, gdy Serwer administracyjny jest w sieci lokalnej (LAN), a zarządzane urządzenia, w tym urządzenia mobilne, są w internecie. Na tym rysunku używany jest wybrany przez Ciebie odwrotny serwer proxy. Więcej informacji można znaleźć w dokumentacji aplikacji.



Serwer administracyjny w sieci lokalnej; zarządzane urządzenia nawiązują połączenie z Serwerem administracyjnym poprzez odwrotny serwer proxy

Ten schemat wdrażania jest zalecany, jeśli nie chcesz, żeby urządzenia mobilne nawiązywały połączenie bezpośrednio z Serwerem administracyjnym i nie chcesz przypisać bramy połączenia w DMZ.

Strzałki wskazują inicjowanie ruchu sieciowego: każda strzałka wskazuje kierunek z urządzenia, które inicjuje połączenie, do urządzenia, które „odpowiada" na połączenie. Dostarczony jest numer portu oraz nazwa protokołu użytego do przesyłania danych. Każda strzałka posiada etykietę liczby, a szczegóły dotyczące odpowiedniego ruchu danych wyglądają następująco:

1. Serwer administracyjny wysyła dane do bazy danych. Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server lub port 1433 dla Microsoft SQL Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2. Żądania komunikacji od Serwera administracyjnego są przesyłane do wszystkich niemobilnych zarządzanych urządzeń poprzez port UDP o numerze 15000.

   Agenty sieciowe wysyłają żądania do siebie nawzajem w obrębie jednej domeny broadcastowej. Dane są następnie wysyłane do Serwera administracyjnego i są używane do określenia ograniczeń domeny broadcastowej i do automatycznego przydzielenia punktów dystrybucji (jeśli ta opcja jest włączona).

   Jeżeli Serwer administracyjny nie ma bezpośredniego dostępu do zarządzanych urządzeń, żądania komunikacji z Serwera administracyjnego nie są wysyłane bezpośrednio do tych urządzeń.

3. Informacje o zamknięciu zarządzanych urządzeń są przesyłane z Agenta sieciowego do Serwera administracyjnego poprzez port UDP o numerze 13000.

4. Serwer administracyjny odbiera połączenie od Agentów sieciowych i podrzędnych Serwerów administracyjnych poprzez port TLS o numerze 13000.

   Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port inny niż TLS o numerze 14000. Kaspersky Security Center obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu TLS o numerze 13000.

   > We wcześniejszych wersjach Kaspersky Security Center punkt dystrybucji nosił nazwę „Agent aktualizacji".

5. Zarządzane urządzenia (za wyjątkiem urządzeń mobilnych) żądają aktywacji poprzez port TCP o numerze 17000. Nie jest to konieczne, jeśli urządzenie posiada własny dostęp do Internetu; w tym przypadku urządzenie wysyła dane do serwerów Kaspersky bezpośrednio przez Internet.

6. Dane z Konsoli administracyjnej opartej na konsoli MMC zostaną przesłane do Serwera administracyjnego poprzez port 13291 (Konsola administracyjna może zostać zainstalowana na tym samym lub na innym urządzeniu).

7. Lokalny ruch sieciowy aplikacji na pojedynczym urządzeniu (na Serwerze administracyjnym lub na zarządzanym urządzeniu). Żadne porty zewnętrzne nie muszą być otwarte.

8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do Internetu, musisz ręcznie zarządzać tymi danymi.

9. Kaspersky Security Center Web Console Server wysyła dane na Serwer administracyjny, który może być zainstalowany na tym samym lub innym urządzeniu, poprzez port TLS o numerze 13299.

   9a. Dane z przeglądarki, która jest zainstalowana na oddzielnym urządzeniu administratora, są przesyłane do Kaspersky Security Center Web Console Server poprzez port TLS o numerze 8080. Kaspersky Security Center Web Console Server może zostać zainstalowany na Serwerze administracyjnym lub na innym urządzeniu.

10. Tylko dla urządzeń mobilnych z systemem Android: dane z Serwera administracyjnego są przesyłane na serwery Google. To połączenie jest używane do informowania urządzeń mobilnych Android, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym. Powiadomienia push są wysyłane na urządzenia mobilne.

11. Tylko dla urządzeń mobilnych z systemem Android: powiadomienia push z serwerów Google są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym.

12. Tylko dla urządzeń mobilnych z systemem iOS: dane z serwera iOS MDM są przesyłane do serwerów Apple Push Notification. Powiadomienia push są wysyłane na urządzenia mobilne.

13. Tylko dla urządzeń mobilnych z systemem iOS: powiadomienia push z serwerów Apple są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych iOS, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym.

14. Tylko dla urządzeń mobilnych: dane z zarządzanej aplikacji są przesyłane do Serwera administracyjnego (lub do bramy połączenia) poprzez port TLS o numerze 13292 / 13293—bezpośrednio lub poprzez odwrotny serwer proxy.

15. Tylko dla urządzeń mobilnych: dane z urządzenia mobilnego są przesyłane do infrastruktury Kaspersky.

    Jeśli urządzenie mobilne nie ma dostępu do Internetu, dane są przesyłane do Serwera administracyjnego poprzez port o numerze 17100, a Serwer administracyjny wysyła je do infrastruktury Kaspersky; jednakże ten scenariusz jest stosowany bardzo rzadko.

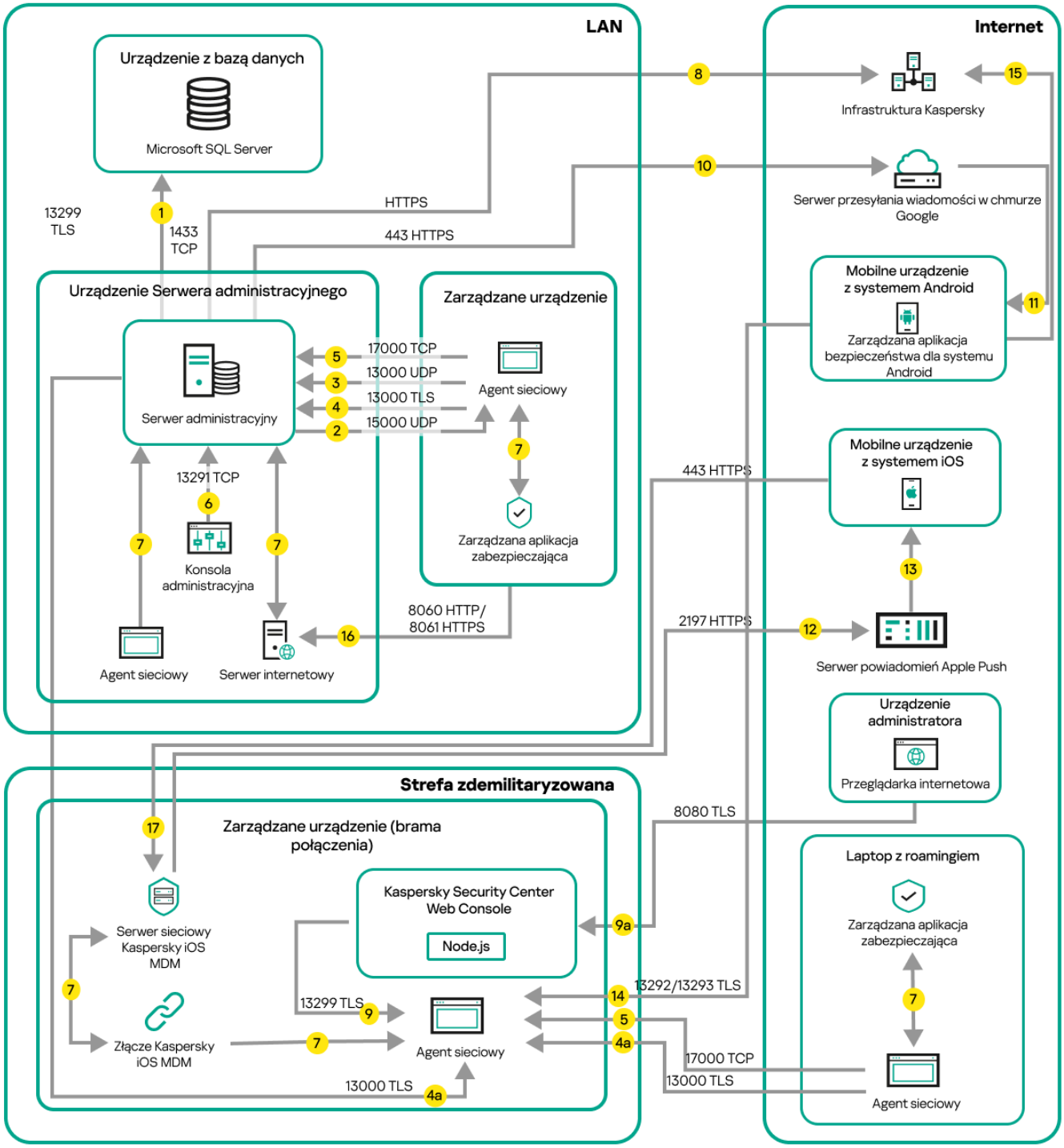
16. Żądania dla pakietów z zarządzanych urządzeń, w tym urządzeń mobilnych, są przesyłane do serwera WWW, który znajduje się na tym samym urządzeniu co Serwer administracyjny.

17. Tylko dla urządzeń mobilnych z systemem iOS: dane z urządzenia mobilnego są przesyłane za pośrednictwem portu TLS o numerze 443 na serwer iOS MDM, który znajduje się na tym samym urządzeniu co Serwer administracyjny, lub na bramie połączenia.

Serwer administracyjny w sieci LAN, zarządzane urządzenia w internecie, brama połączenia w użyciu

Poniższy rysunek przedstawia ruch sieciowy danych, gdy Serwer administracyjny jest w sieci lokalnej (LAN), a zarządzane urządzenia, w tym urządzenia mobilne, są w internecie. Używana jest brama połączenia.

Ten schemat wdrażania jest zalecany, jeśli nie chcesz, żeby urządzenia mobilne nawiązywały połączenie bezpośrednio z Serwerem administracyjnym i nie chcesz używać odwrotnego serwera proxy lub firmowej zapory sieciowej.



Zarządzane urządzenia mobilne połączone z Serwerem administracyjnym poprzez bramę połączenia

Na tym rysunku zarządzane urządzenia są połączone z Serwerem administracyjnym poprzez bramę połączenia, która znajduje się w strefie DMZ. Nie jest używany odwrotny serwer proxy ani firmowa zapora sieciowa.

Strzałki wskazują inicjowanie ruchu sieciowego: każda strzałka wskazuje kierunek z urządzenia, które inicjuje połączenie, do urządzenia, które „odpowiada" na połączenie. Dostarczony jest numer portu oraz nazwa protokołu użytego do przesyłania danych. Każda strzałka posiada etykietę liczby, a szczegóły dotyczące odpowiedniego ruchu danych wyglądają następująco:

1. Serwer administracyjny wysyła dane do bazy danych. Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server lub port 1433 dla Microsoft SQL Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2. Żądania komunikacji od Serwera administracyjnego są przesyłane do wszystkich niemobilnych zarządzanych urządzeń poprzez port UDP o numerze 15000.

   Agenty sieciowe wysyłają żądania do siebie nawzajem w obrębie jednej domeny broadcastowej. Dane są następnie wysyłane do Serwera administracyjnego i są używane do określenia ograniczeń domeny broadcastowej i do automatycznego przydzielenia punktów dystrybucji (jeśli ta opcja jest włączona).

   Jeżeli Serwer administracyjny nie ma bezpośredniego dostępu do zarządzanych urządzeń, żądania komunikacji z Serwera administracyjnego nie są wysyłane bezpośrednio do tych urządzeń.

3. Informacje o zamknięciu zarządzanych urządzeń są przesyłane z Agenta sieciowego do Serwera administracyjnego poprzez port UDP o numerze 13000.

4. Serwer administracyjny odbiera połączenie od Agentów sieciowych i podrzędnych Serwerów administracyjnych poprzez port TLS o numerze 13000.

   Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port inny niż TLS o numerze 14000. Kaspersky Security Center obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu TLS o numerze 13000.

   > We wcześniejszych wersjach Kaspersky Security Center punkt dystrybucji nosił nazwę „Agent aktualizacji".

   4a. Brama połączenia w strefie DMZ odbiera również połączenie z Serwera administracyjnego przez port TLS 13000. Ponieważ brama połączenia w strefie DMZ nie obejmuje portów Serwera administracyjnego, Serwer administracyjny utworzy i zachowa ciągłe połączenie sygnałowe z bramą połączenia. Połączenie sygnałowe nie jest używane do przesyłania danych; jest używane tylko do wysyłania zaproszenia do interakcji z siecią. Jeśli brama połączenia musi nawiązać połączenie z Serwerem, poinformuje Serwer za pośrednictwem połączenia sygnałowego, a następnie Serwer utworzy wymagane połączenie do przesyłania danych.

   Urządzenia spoza biura nawiązują także połączenie z bramą połączenia za pośrednictwem portu TLS o numerze 13000.

5. Zarządzane urządzenia (za wyjątkiem urządzeń mobilnych) żądają aktywacji poprzez port TCP o numerze 17000. Nie jest to konieczne, jeśli urządzenie posiada własny dostęp do Internetu; w tym przypadku urządzenie wysyła dane do serwerów Kaspersky bezpośrednio przez Internet.

6. Dane z Konsoli administracyjnej opartej na konsoli MMC zostaną przesłane do Serwera administracyjnego poprzez port 13291 (Konsola administracyjna może zostać zainstalowana na tym samym lub na innym urządzeniu).

7. Lokalny ruch sieciowy aplikacji na pojedynczym urządzeniu (na Serwerze administracyjnym lub na zarządzanym urządzeniu). Żadne porty zewnętrzne nie muszą być otwarte.

8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do Internetu, musisz ręcznie zarządzać tymi danymi.

9. Kaspersky Security Center Web Console Server wysyła dane na Serwer administracyjny, który może być zainstalowany na tym samym lub innym urządzeniu, poprzez port TLS o numerze 13299.

   9a. Dane z przeglądarki, która jest zainstalowana na oddzielnym urządzeniu administratora, są przesyłane do Kaspersky Security Center Web Console Server poprzez port TLS o numerze 8080. Kaspersky Security Center Web Console Server może zostać zainstalowany na Serwerze administracyjnym lub na innym urządzeniu.

10. Tylko dla urządzeń mobilnych z systemem Android: dane z Serwera administracyjnego są przesyłane na serwery Google. To połączenie jest używane do informowania urządzeń mobilnych Android, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym. Powiadomienia push są wysyłane na urządzenia mobilne.

11. Tylko dla urządzeń mobilnych z systemem Android: powiadomienia push z serwerów Google są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym.

12. Tylko dla urządzeń mobilnych z systemem iOS: dane z serwera iOS MDM są przesyłane do serwerów Apple Push Notification. Powiadomienia push są wysyłane na urządzenia mobilne.

13. Tylko dla urządzeń mobilnych z systemem iOS: powiadomienia push z serwerów Apple są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych iOS, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym.

14. Tylko dla urządzeń mobilnych: dane z zarządzanej aplikacji są przesyłane do Serwera administracyjnego (lub do bramy połączenia) poprzez port TLS o numerze 13292 / 13293—bezpośrednio lub poprzez odwrotny serwer proxy.

15. Tylko dla urządzeń mobilnych: dane z urządzenia mobilnego są przesyłane do infrastruktury Kaspersky.

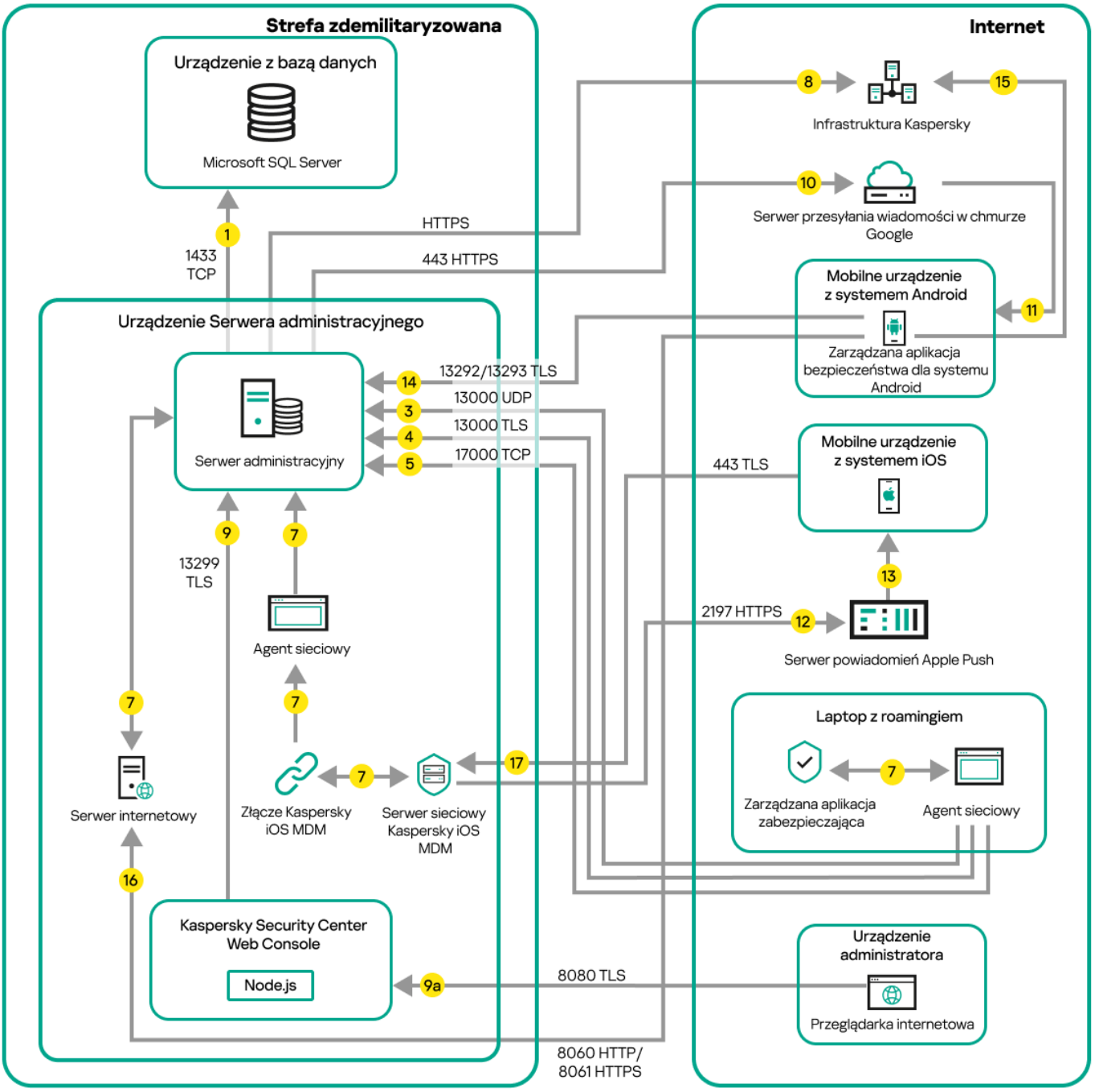
    Jeśli urządzenie mobilne nie ma dostępu do Internetu, dane są przesyłane do Serwera administracyjnego poprzez port o numerze 17100, a Serwer administracyjny wysyła je do infrastruktury Kaspersky; jednakże ten scenariusz jest stosowany bardzo rzadko.

16. Żądania dla pakietów z zarządzanych urządzeń, w tym urządzeń mobilnych, są przesyłane do serwera WWW, który znajduje się na tym samym urządzeniu co Serwer administracyjny.

17. Tylko dla urządzeń mobilnych z systemem iOS: dane z urządzenia mobilnego są przesyłane za pośrednictwem portu TLS o numerze 443 na serwer iOS MDM, który znajduje się na tym samym urządzeniu co Serwer administracyjny, lub na bramie połączenia.

Serwer administracyjny w strefie DMZ, zarządzane urządzenia w Internecie

Poniższy rysunek przedstawia ruch sieciowy danych, gdy Serwer administracyjny jest w strefie zdemilitaryzowanej (DMZ), a zarządzane urządzenia, w tym urządzenia mobilne, są w Internecie.



Serwer administracyjny w strefie DMZ, zarządzane urządzenia mobilne w Internecie

Na tym rysunku brama połączenia nie jest używana: urządzenia mobilne nawiązują połączenie bezpośrednio z Serwerem administracyjnym.

Strzałki wskazują inicjowanie ruchu sieciowego: każda strzałka wskazuje kierunek z urządzenia, które inicjuje połączenie, do urządzenia, które „odpowiada" na połączenie. Dostarczony jest numer portu oraz nazwa protokołu użytego do przesyłania danych. Każda strzałka posiada etykietę liczby, a szczegóły dotyczące odpowiedniego ruchu danych wyglądają następująco:

1. Serwer administracyjny wysyła dane do bazy danych. Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server lub port 1433 dla Microsoft SQL Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2. Żądania komunikacji od Serwera administracyjnego są przesyłane do wszystkich niemobilnych zarządzanych urządzeń poprzez port UDP o numerze 15000.

   Agenty sieciowe wysyłają żądania do siebie nawzajem w obrębie jednej domeny broadcastowej. Dane są następnie wysyłane do Serwera administracyjnego i są używane do określenia ograniczeń domeny broadcastowej i do automatycznego przydzielenia punktów dystrybucji (jeśli ta opcja jest włączona).

   Jeżeli Serwer administracyjny nie ma bezpośredniego dostępu do zarządzanych urządzeń, żądania komunikacji z Serwera administracyjnego nie są wysyłane bezpośrednio do tych urządzeń.

3. Informacje o zamknięciu zarządzanych urządzeń są przesyłane z Agenta sieciowego do Serwera administracyjnego poprzez port UDP o numerze 13000.

4. Serwer administracyjny odbiera połączenie od Agentów sieciowych i podrzędnych Serwerów administracyjnych poprzez port TLS o numerze 13000.

   Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port inny niż TLS o numerze 14000. Kaspersky Security Center obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu TLS o numerze 13000.

   > We wcześniejszych wersjach Kaspersky Security Center punkt dystrybucji nosił nazwę „Agent aktualizacji".

5. Zarządzane urządzenia (za wyjątkiem urządzeń mobilnych) żądają aktywacji poprzez port TCP o numerze 17000. Nie jest to konieczne, jeśli urządzenie posiada własny dostęp do Internetu; w tym przypadku urządzenie wysyła dane do serwerów Kaspersky bezpośrednio przez Internet.

6. Dane z Konsoli administracyjnej opartej na konsoli MMC zostaną przesłane do Serwera administracyjnego poprzez port 13291 (Konsola administracyjna może zostać zainstalowana na tym samym lub na innym urządzeniu).

7. Lokalny ruch sieciowy aplikacji na pojedynczym urządzeniu (na Serwerze administracyjnym lub na zarządzanym urządzeniu). Żadne porty zewnętrzne nie muszą być otwarte.

8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do Internetu, musisz ręcznie zarządzać tymi danymi.

9. Kaspersky Security Center Web Console Server wysyła dane na Serwer administracyjny, który może być zainstalowany na tym samym lub innym urządzeniu, poprzez port TLS o numerze 13299.

   9a. Dane z przeglądarki, która jest zainstalowana na oddzielnym urządzeniu administratora, są przesyłane do Kaspersky Security Center Web Console Server poprzez port TLS o numerze 8080. Kaspersky Security Center Web Console Server może zostać zainstalowany na Serwerze administracyjnym lub na innym urządzeniu.

10. Tylko dla urządzeń mobilnych z systemem Android: dane z Serwera administracyjnego są przesyłane na serwery Google. To połączenie jest używane do informowania urządzeń mobilnych Android, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym. Powiadomienia push są wysyłane na urządzenia mobilne.

11. Tylko dla urządzeń mobilnych z systemem Android: powiadomienia push z serwerów Google są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym.

12. Tylko dla urządzeń mobilnych z systemem iOS: dane z serwera iOS MDM są przesyłane do serwerów Apple Push Notification. Powiadomienia push są wysyłane na urządzenia mobilne.

13. Tylko dla urządzeń mobilnych z systemem iOS: powiadomienia push z serwerów Apple są wysyłane na urządzenie mobilne. To połączenie jest używane do informowania urządzeń mobilnych iOS, że są niezbędne do nawiązania połączenia z Serwerem administracyjnym.

14. Tylko dla urządzeń mobilnych: dane z zarządzanej aplikacji są przesyłane do Serwera administracyjnego (lub do bramy połączenia) poprzez port TLS o numerze 13292 / 13293—bezpośrednio lub poprzez odwrotny serwer proxy.

15. Tylko dla urządzeń mobilnych: dane z urządzenia mobilnego są przesyłane do infrastruktury Kaspersky.

    Jeśli urządzenie mobilne nie ma dostępu do Internetu, dane są przesyłane do Serwera administracyjnego poprzez port o numerze 17100, a Serwer administracyjny wysyła je do infrastruktury Kaspersky; jednakże ten scenariusz jest stosowany bardzo rzadko.

16. Żądania dla pakietów z zarządzanych urządzeń, w tym urządzeń mobilnych, są przesyłane do serwera WWW, który znajduje się na tym samym urządzeniu co Serwer administracyjny.

17. Tylko dla urządzeń mobilnych z systemem iOS: dane z urządzenia mobilnego są przesyłane za pośrednictwem portu TLS o numerze 443 na serwer iOS MDM, który znajduje się na tym samym urządzeniu co Serwer administracyjny, lub na bramie połączenia.

Interakcja komponentów Kaspersky Security Center i aplikacji zabezpieczających: więcej informacji

Ta sekcja opisuje schematy interakcji komponentów Kaspersky Security Center z zarządzanymi aplikacjami zabezpieczającymi. Schematy zawierają numery portów, które muszą być dostępne, oraz nazwy procesów, które otwierają te porty.

Konwencje stosowane w schematach interakcji

Poniższa tabela przedstawia konwencje stosowane w schematach.

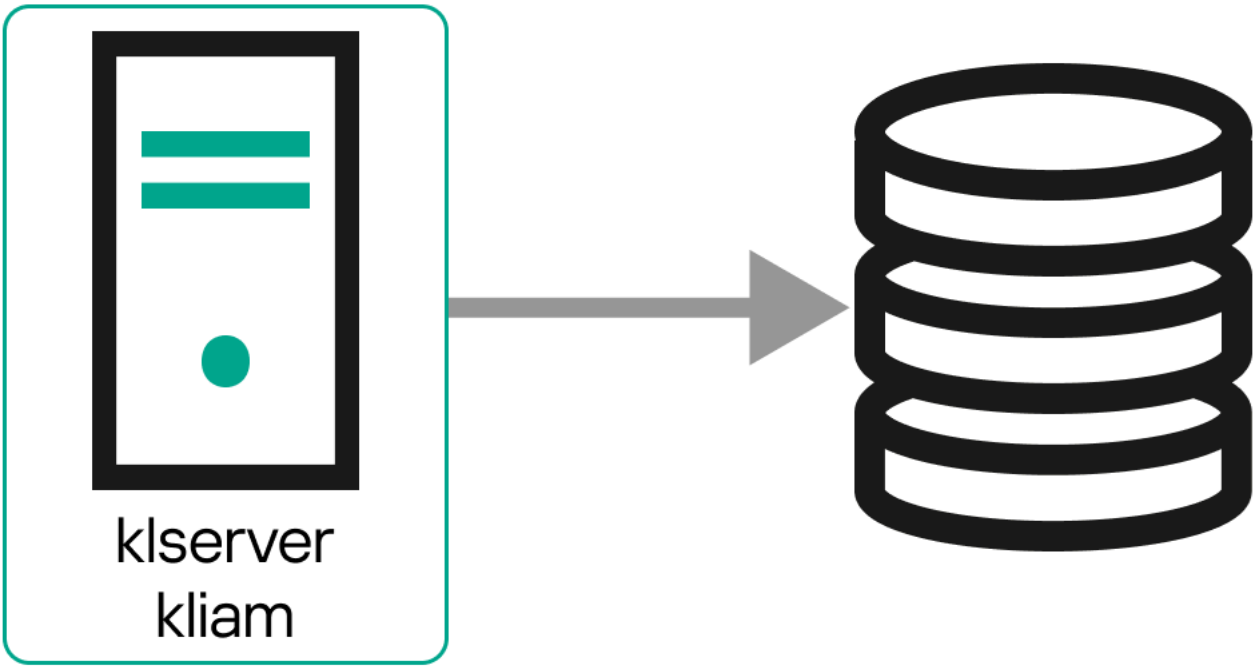
Oznaczenia stosowane w dokumencie

Ikona	Znaczenie
	Serwer administracyjny

	Podrzędny Serwer administracyjny
	DBMS
	Urządzenie klienckie (na którym jest zainstalowany Agent sieciowy oraz aplikacja z rodziny Kaspersky Endpoint Security lub inna aplikacja zabezpieczająca, którą może zarządzać Kaspersky Security Center)
	Brama połączenia
	Punkt dystrybucji
	Mobilne urządzenie klienckie z programem Kaspersky Security for Mobile
	Przeglądarka na urządzeniu użytkownika
	Proces uruchomiony na urządzeniu i otwierający port
	Port i jego numer
	Ruch TCP (kierunek strzałki przedstawia kierunek przepływu ruchu)
	Ruch UDP (kierunek strzałki przedstawia kierunek przepływu ruchu)
	Wywoływanie COM
	Transport DBMS
	Granica strefy DMZ

Serwer administracyjny i DBMS

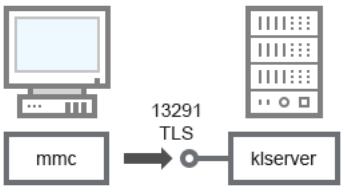
Dane z Serwera administracyjnego wprowadź w bazie danych serwera SQL, MySQL lub MariaDB.



Serwer administracyjny i DBMS

Jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server lub port 1433 dla Microsoft SQL Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

Serwer administracyjny i Konsola administracyjna



Serwer administracyjny i Konsola administracyjna

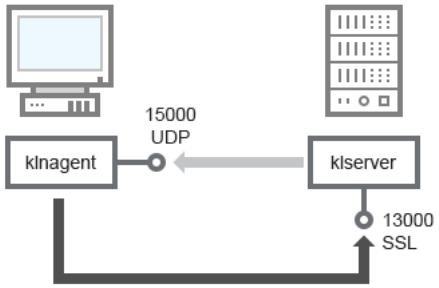
Klasyfikacje schematu są dostępne w tabeli poniżej.

Serwer administracyjny i Konsola administracyjna (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	TLS	Przeznaczenie portu
Serwer administracyjny	13291	klserver	TCP	Tak	Odbieranie połączeń z Konsoli administracyjnej

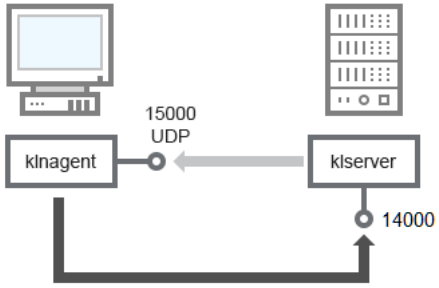
Serwer administracyjny i urządzenie klienckie: zarządzanie aplikacją zabezpieczająca

Serwer administracyjny odbiera połączenie od Agentów sieciowych za pośrednictwem portu SSL o numerze 13000 (patrz rysunek poniżej).



Serwer administracyjny i urządzenie klienckie: zarządzanie aplikacją zabezpieczająca, połączenie poprzez port 13000 (zalecane)

Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port bez szyfrowania SSL o numerze 14000 (patrz rysunek poniżej). Kaspersky Security Center 15.1 obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu SSL o numerze 13000.



Serwer administracyjny i urządzenie klienckie: zarządzanie aplikacją zabezpieczająca, połączenie poprzez port 14000 (mniejsze bezpieczeństwo)

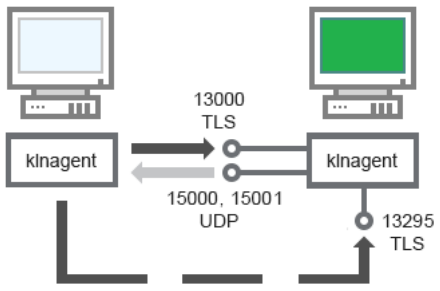
Wyjaśnienie schematów jest dostępne w tabeli poniżej.

Serwer administracyjny i urządzenie klienckie: zarządzanie aplikacją zabezpieczająca (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	TLS (tylko dla TCP)	Przeznaczenie portu
Agent sieciowy	15000	klnagent	UDP	Null	Multiemisja dla Agentów sieciowych
Serwer administracyjny	13000	klserver	TCP	Tak	Odbieranie połączeń od Agentów sieciowych
Serwer administracyjny	14000	klserver	TCP	Nie	Odbieranie połączeń od Agentów sieciowych

Aktualizowanie oprogramowania na urządzeniu klienckim poprzez punkt dystrybucji

Urządzenie klienckie nawiązuje połączenie z punktem dystrybucji poprzez port 13000, a jeśli używasz punktu dystrybucji jako serwera push, także poprzez port 13295; punkt dystrybucji wykonuje multiemisję do Agentów sieciowych poprzez port 15000 (patrz rysunek poniżej). Aktualizacje i pakiety instalacyjne są odbierane z punktu dystrybucji przez port 15001.



Aktualizowanie oprogramowania na urządzeniu klienckim poprzez punkt dystrybucji

Klasyfikacje schematu są dostępne w tabeli poniżej.

Aktualizowanie oprogramowania za pośrednictwem punktu dystrybucji (ruch sieciowy)

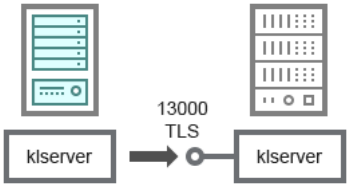
Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	TLS (tylko dla TCP)	Przeznaczenie portu
Agent sieciowy	15000	klnagent	UDP	Null	Multiemisja dla Agentów sieciowych
Agent sieciowy	15001	klnagent	UDP	Null	Odbieranie aktualizacji i pakietów instalacyjnych z punktu dystrybucji
Punkt dystrybucji	13000	klnagent	TCP	Tak	Odbieranie połączeń od Agentów sieciowych
Punkt dystrybucji	13295	klnagent	TCP	Tak	Odbieranie połączeń z urządzeń klienckich (przez serwer push)

Hierarchia Serwerów administracyjnych: główny Serwer administracyjny i podrzędny Serwer administracyjny

Schemat (patrz rysunek poniżej) przedstawia korzystanie z portu 13000 do zapewnienia interakcji pomiędzy Serwerami administracyjnymi połączonymi w hierarchię.

Podczas łączenia dwóch Serwerów administracyjnych w hierarchię upewnij się, że port 13291 jest dostępny na obu Serwerach administracyjnych. Konsola administracyjna nawiązuje połączenie z Serwerem administracyjnym poprzez port 13291.

Następnie, gdy Serwery administracyjne zostaną połączone w hierarchię, będziesz mógł zarządzać nimi przy użyciu Konsoli administracyjnej połączonej z głównym Serwerem administracyjnym. Dlatego też, dostępność portu 13291 głównego Serwera administracyjnego jest niezbędnym wymaganiem.



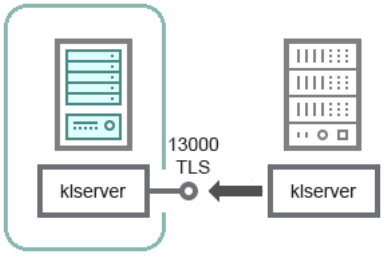
Hierarchia Serwerów administracyjnych: główny Serwer administracyjny i podrzędny Serwer administracyjny

Klasyfikacje schematu są dostępne w tabeli poniżej.

Hierarchia Serwerów administracyjnych (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	TLS	Przeznaczenie portu
Główny Serwer administracyjny	13000	klserver	TCP	Tak	Odbieranie połączeń z podrzędnych Serwerów administracyjnych

Hierarchia Serwerów administracyjnych z podrzędnym Serwerem administracyjnym w strefie DMZ



Hierarchia Serwerów administracyjnych z podrzędnym Serwerem administracyjnym w strefie DMZ

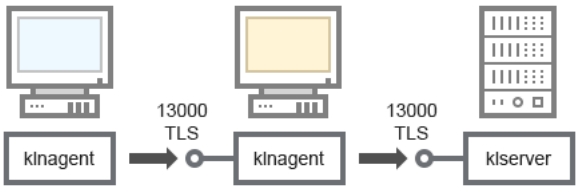
Schemat przedstawia hierarchię Serwerów administracyjnych, w której podrzędny Serwer administracyjny, znajdujący się w strefie DMZ, odbiera połączenie z głównego Serwera administracyjnego (patrz tabela poniżej dla wyjaśnienia schematu). Podczas łączenia dwóch Serwerów administracyjnych w hierarchię upewnij się, że port 13291 jest dostępny na obu Serwerach administracyjnych. Konsola administracyjna nawiązuje połączenie z Serwerem administracyjnym poprzez port 13291.

Następnie, gdy Serwery administracyjne zostaną połączone w hierarchię, będziesz mógł zarządzać nimi przy użyciu Konsoli administracyjnej połączonej z głównym Serwerem administracyjnym. Dlatego też, dostępność portu 13291 głównego Serwera administracyjnego jest niezbędnym wymaganiem.

Hierarchia Serwerów administracyjnych z podrzędnym Serwerem administracyjnym w strefie DMZ (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	TLS	Przeznaczenie portu
Podrzędny Serwer administracyjny	13000	klserver	TCP	Tak	Odbieranie połączeń z głównego Serwera administracyjnego

Serwer administracyjny, brama połączenia w segmencie sieci i urządzenie klienckie



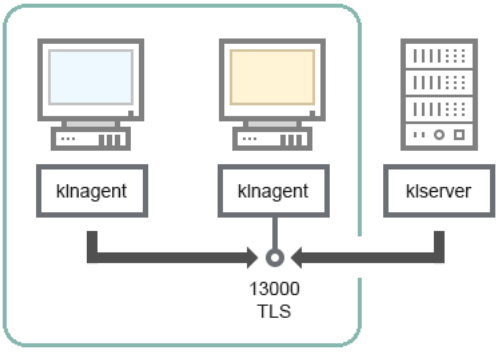
Serwer administracyjny, brama połączenia w segmencie sieci i urządzenie klienckie

Klasyfikacje schematu są dostępne w tabeli poniżej.

Serwer administracyjny, brama połączenia w segmencie sieci i urządzenie klienckie (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	TLS	Przeznaczenie portu
Serwer administracyjny	13000	klserver	TCP	Tak	Odbieranie połączeń od Agentów sieciowych
Agent sieciowy	13000	klnagent	TCP	Tak	Odbieranie połączeń od Agentów sieciowych

Serwer administracyjny i dwa urządzenia w strefie DMZ: brama połączenia i urządzenie klienckie



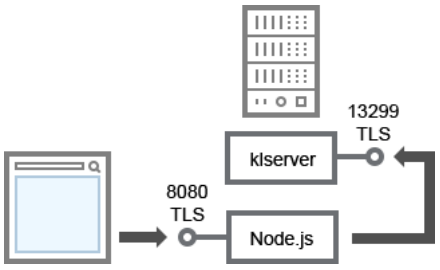
Serwer administracyjny z bramą połączenia i urządzeniem klienckim w strefie DMZ

Klasyfikacje schematu są dostępne w tabeli poniżej.

Serwer administracyjny z bramą połączenia w segmencie sieci i urządzenie klienckie (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	TLS	Przeznaczenie portu
Agent sieciowy	13000	klnagent	TCP	Tak	Odbieranie połączeń od Agentów sieciowych

Serwer administracyjny i Kaspersky Security Center Web Console



Serwer administracyjny i Kaspersky Security Center Web Console

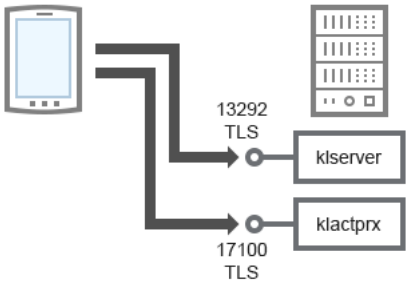
Klasyfikacje schematu są dostępne w tabeli poniżej.

Serwer administracyjny i Kaspersky Security Center Web Console (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	TLS	Przeznaczenie portu
Serwer administracyjny	13299	klserver	TCP	Tak	Odbieranie połączeń od Kaspersky Security Center Web Console do Serwera administracyjnego poprzez OpenAPI
Kaspersky Security Center Web Console Server lub Serwer administracyjny	8080	Node.js: Server-side JavaScript	TCP	Tak	Odbieranie połączeń od Kaspersky Security Center Web Console

Konsola Kaspersky Security Center Web Console może zostać zainstalowana na Serwerze administracyjnym lub na innym urządzeniu.

Aktywowanie i zarządzanie aplikacją zabezpieczającą na urządzeniu mobilnym



Aktywowanie i zarządzanie aplikacją zabezpieczającą na urządzeniu mobilnym

Klasyfikacje schematu są dostępne w tabeli poniżej.

Aktywowanie i zarządzanie aplikacją zabezpieczającą na urządzeniu mobilnym (ruch sieciowy)

Urządzenie	Numer portu	Nazwa procesu, który otwiera port	Protokół	TLS	Przeznaczenie portu
Serwer administracyjny	13292	klserver	TCP	Tak	Odbieranie połączeń od Konsoli administracyjnej do Serwera administracyjnego
Serwer administracyjny	17100	klactprx	TCP	Tak	Odbieranie połączeń dla aktywacji aplikacji od urządzeń mobilnych

Wdrażanie praktycznego zastosowania aplikacji

Kaspersky Security Center jest aplikacją oferującą wiele funkcji. Kaspersky Security Center zawiera następujące komponenty:

- Serwer administracyjny—główny komponent, zaprojektowany do zarządzania urządzeniami w organizacji i przechowywania danych w DBMS.
- Konsola administracyjna—podstawowe narzędzie administratora. Konsola administracyjna jest dostarczana wraz z Serwerem administracyjnym, ale można ją także zainstalować oddzielnie na jednym lub kilku urządzeniach administratora.
- Agent sieciowy — zaprojektowany do zarządzania aplikacją zabezpieczającą, zainstalowaną na urządzeniu, a także do uzyskiwania informacji o tym urządzeniu i przesyłania tych informacji na Serwer administracyjny. Agenty sieciowe są instalowane na urządzeniach w organizacji.

Instalacja Kaspersky Security Center w sieci organizacji odbywa się w następujący sposób:

- Instalacja Serwera administracyjnego
- Instalacja Konsoli administracyjnej na urządzeniu administratora
- Instalacja Agenta sieciowego i aplikacji zabezpieczającej na urządzeniach w firmie

Przewodnik po zwiększaniu odporności

Kaspersky Security Center służy do scentralizowanego wykonywania podstawowych zadań dotyczących administracji i zarządzania w sieci firmy. Aplikacja zapewnia administratorowi dostęp do szczegółowych informacji o poziomie bezpieczeństwa sieci organizacji. Kaspersky Security Center umożliwia skonfigurowanie wszystkich komponentów ochrony zbudowanych przy użyciu aplikacji Kaspersky.

Serwer administracyjny Kaspersky Security Center ma pełny dostęp do zarządzania ochroną urządzeń klienckich i jest najważniejszym komponentem systemu bezpieczeństwa organizacji. Dlatego dla Serwera administracyjnego wymagane są zwiększone metody ochrony.

Przed rozpoczęciem konfiguracji utwórz kopię zapasową Serwera administracyjnego Kaspersky Security Center za pomocą zadania Kopia zapasowa danych Serwera administracyjnego lub narzędzia klbackup i zapisz ją w bezpiecznym miejscu.

Przewodnik zwiększania bezpieczeństwa opisuje zalecenia i funkcje konfigurowania Kaspersky Security Center i jego komponentów, mające na celu zmniejszenie ryzyka związanego z jego włamaniem.

Przewodnik po zwiększaniu odporności zawiera następujące informacje:

- Wybór architektury Serwera administracyjnego
- Konfigurowanie bezpiecznego połączenia z Serwerem administracyjnym
- Konfigurowanie kont w celu uzyskania dostępu do Serwera administracyjnego

- Zarządzanie ochroną Serwera administracyjnego
- Zarządzanie ochroną urządzeń klienckich
- Konfigurowanie ochrony dla zarządzanych aplikacji
- Konserwacja Serwera administracyjnego
- Przesyłanie informacji do aplikacji firm trzecich
- Zalecenia dotyczące bezpieczeństwa systemów informatycznych innych firm

Wdrożenie Serwera administracyjnego

Architektura Serwera administracyjnego

Ogólnie rzecz biorąc, wybór scentralizowanej architektury zarządzania zależy od lokalizacji chronionych urządzeń, dostępu z sąsiednich sieci, schematów dostarczania aktualizacji baz danych i tak dalej.

Na początkowym etapie rozwoju architektury zalecamy zapoznanie się z komponentami Kaspersky Security Center i ich wzajemną interakcją, a także ze schematami ruchu danych i wykorzystania portów.

Na podstawie tych informacji można utworzyć architekturę, która określa:

- Lokalizacja Serwera administracyjnego i połączenia sieciowe
- Organizacja obszarów roboczych administratora i metody łączenia się z Serwerem administracyjnym
- Metody wdrożenia agenta sieciowego i oprogramowania zabezpieczającego
- Korzystanie z punktów dystrybucji
- Korzystanie z wirtualnych Serwerów administracyjnych
- Użycie hierarchii Serwerów administracyjnych
- Schemat aktualizacji antywirusowej bazy danych
- Inne przepływy informacji

Wybieranie urządzenia do instalacji Serwera administracyjnego

Zalecamy zainstalowanie Serwera administracyjnego na serwerze dedykowanym w infrastrukturze organizacji. Jeśli na serwerze nie jest zainstalowane żadne inne oprogramowanie innych firm, możesz skonfigurować ustawienia bezpieczeństwa w oparciu o wymagania Kaspersky Security Center, bez zależności od wymagań oprogramowania innych firm.

Możesz zainstalować Serwer administracyjny na serwerze fizycznym lub na serwerze wirtualnym. Prosimy upewnić się, że wybrane urządzenie spełnia wymagania sprzętowe i programowe.

Lokalizacja Serwera administracyjnego

Urządzenia zarządzane przez Serwer administracyjny można zlokalizować w następujący sposób:

- W sieci lokalnej (LAN)
- W Internecie
- W strefie zdemilitaryzowanej (DMZ)

Jednocześnie Serwer administracyjny może być zlokalizowany w różnych segmentach: przemysłowym, korporacyjnym i DMZ.

Jeśli używasz Kaspersky Security Center do zarządzania ochroną izolowanego segmentu sieci, zalecamy zainstalowanie Serwera administracyjnego w segmencie strefy zdemilitaryzowanej (DMZ). Pozwala to na zorganizowanie odpowiedniej segmentacji sieci i zminimalizowanie przepływu ruchu do chronionego segmentu, przy jednoczesnym zachowaniu pełnych możliwości zarządzania i dostarczania aktualizacji.

Ograniczenie instalacji Serwera administracyjnego na kontrolerze domeny, serwerze terminali lub urządzeniu użytkownika

Zdecydowanie nie zalecamy instalowania Serwera administracyjnego na kontrolerze domeny, serwerze terminali lub urządzeniu użytkownika.

Zalecamy zapewnienie funkcjonalnej separacji kluczowych węzłów sieci. Takie podejście pozwala zachować funkcjonalność różnych systemów, gdy węzeł ulegnie awarii lub zostanie naruszony. Jednocześnie możesz tworzyć różne zasady zabezpieczeń dla każdego węzła.

Przykładowo ograniczenia zabezpieczeń stosowane zwykle do kontrolera domeny mogą znacznie zmniejszyć wydajność Serwera administracyjnego i uniemożliwić korzystanie z niektórych funkcji Serwera administracyjnego. Jeśli intruz uzyska uprzywilejowany dostęp do kontrolera domeny, bazy danych Active Directory Domain Services (AD DS). mogą być modyfikowane, uszkadzane lub niszczone. Ponadto wszystkie systemy i konta zarządzane przez usługę Active Directory mogą zostać naruszone.

Konta do instalowania i uruchamiania Serwera administracyjnego

Zalecamy uruchomienie instalacji Serwera administracyjnego z konta administratora lokalnego, aby uniknąć korzystania z kont domeny w celu uzyskania dostępu do bazy danych Serwera administracyjnego. Zestaw wymaganych kont i ich uprawnień zależy od wybranego typu DBMS, lokalizacji DBMS oraz metody tworzenia bazy danych Serwera administracyjnego.

Podczas instalacji Kaspersky Security Center automatycznie tworzone są grupy KLAdmins i KLOperators. Grupom tym nadawane są uprawnienia do nawiązywania połączeń z Serwerem administracyjnym i do przetwarzania jego obiektów.

W zależności od typu konta użytego przy instalacji Kaspersky Security Center, grupy KLAdmins i KLOperators są tworzone w następujący sposób:

- Jeżeli aplikacja jest zainstalowana z poziomu konta użytkownika znajdującego się w domenie, grupy są tworzone na urządzeniu Serwera administracyjnego oraz w domenie zawierającej Serwer administracyjny.
- Jeśli aplikacja jest zainstalowana z poziomu konta systemowego, grupy są tworzone tylko na urządzeniu Serwera administracyjnego.

Aby uniknąć tworzenia grup KLAdmins i KLOperators w domenie i w rezultacie **nadawania uprawnień do zarządzania Serwerem administracyjnym kontu spoza urządzenia Serwera administracyjnego**, zalecamy zainstalowanie Kaspersky Security Center z poziomu konta lokalnego.

Podczas instalacji Serwera administracyjnego wybierz konto, które zostanie użyte do uruchomienia Serwera administracyjnego jako usługi. Domyślnie aplikacja tworzy konto lokalne o nazwie KL-AK-*, w ramach którego będzie działać usługa Serwera administracyjnego (usługa klserver).

W razie potrzeby usługę Serwera administracyjnego można uruchomić z poziomu wybranego konta. To konto musi mieć wymagane uprawnienia dostępu do DBMS. Ze względów bezpieczeństwa użyj konta bez uprawnień, aby uruchomić usługę Serwera administracyjnego.

Aby uniknąć korzystania z nieprawidłowych ustawień konta, zalecamy automatyczne generowanie konta.

Wykluczanie Serwera administracyjnego z domeny

Jeśli używasz Serwera administracyjnego do ochrony grup urządzeń systemów o dużym znaczeniu, nie zalecamy dołączania urządzenia Serwera administracyjnego do domeny. Pozwala to rozróżnić uprawnienia zarządzania Kaspersky Security Center i uniemożliwić dostęp do Serwera administracyjnego w przypadku naruszenia bezpieczeństwa konta domeny.

Weź pod uwagę, że jeśli zainstalujesz Serwer administracyjny na urządzeniu znajdującym się w grupie roboczej, nie będą dostępne następujące scenariusze pracy z Serwerem administracyjnym:

- Korzystanie z klastra awaryjnego Kaspersky Security Center
- Korzystanie z klastra trybu failover systemu Windows Server
- Korzystanie z SQL Server systemu Windows na oddzielnym urządzeniu

  Możesz używać SQL Server systemu Windows na oddzielnym urządzeniu tylko jeśli Serwer administracyjny i SQL Server znajdują się w tej samej domenie lub w zaufanych domenach. Jeśli Serwer administracyjny, Serwer SQL i udział UNC na potrzeby kopii zapasowych znajdują się w grupie roboczej, nie można bezpiecznie skonfigurować praw dostępu ani praw odczytu i zapisu między Serwerem SQL a udziałem.
- Zdalna instalacja przy użyciu narzędzi Serwera administracyjnego poprzez zasady grupy Active Directory

Jeśli musisz odłączyć Serwer administracyjny od domeny Active Directory, wykonaj czynności opisane w temacie: Jak zmienić nazwę Kaspersky Security Center.

Jeśli konieczna jest instalacja Serwera administracyjnego na urządzeniu należącym do grupy roboczej, możesz również użyć Kaspersky Security Center Linux zamiast Kaspersky Security Center Windows.

Bezpieczeństwo połączenia

Użycie TLS

Zalecamy zablokowanie niezabezpieczonych połączeń z Serwerem administracyjnym. Na przykład, możesz zabronić połączeń korzystających z HTTP w ustawieniach Serwera administracyjnego.

Należy pamiętać, że domyślnie kilka portów HTTP Serwera administracyjnego jest zamkniętych. Pozostały port jest używany przez serwer WWW Serwera administracyjnego (8060). Ten port może być ograniczony przez ustawienia zapory sieciowej urządzenia Serwera administracyjnego.

Ścisłe ustawienia TLS

Zalecamy korzystanie z protokołu TLS w wersji 1.2 lub nowszej oraz ograniczanie lub blokowanie niezabezpieczonych algorytmów szyfrowania.

Możesz skonfigurować protokoły szyfrowania (TLS) używane przez Serwer administracyjny. Należy pamiętać, że w momencie wydania wersji Serwera administracyjnego ustawienia protokołu szyfrowania są domyślnie skonfigurowane w celu zapewnienia bezpiecznego przesyłania danych.

Zakaz zdalnego uwierzytelniania przy użyciu kont Windows

Możesz użyć flagi LP_RestrictRemoteOsAuth, aby zabronić połączeń SSPI ze zdalnych adresów. Ta flaga umożliwia zablokowanie zdalnego uwierzytelniania na Serwerze administracyjnym przy użyciu lokalnych lub domenowych kont Windows.

Aby przełączyć flagę LP_RestrictRemoteOsAuth w tryb blokowania połączeń ze zdalnych adresów:

1. Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Wykonaj następujące polecenie w wierszu poleceń, aby określić wartość flagi LP_RestrictRemoteOsAuth:

   ```
   klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
   ```

3. Uruchom ponownie usługę Serwera administracyjnego.

Flaga LP_RestrictRemoteOsAuth nie działa, jeśli przeprowadzana jest zdalna autoryzacja poprzez Kaspersky Security Center Web Console lub Konsolę administracyjną zainstalowaną na urządzeniu Serwera administracyjnego.

Ograniczanie dostępu do bazy danych Serwera administracyjnego

Zalecamy ograniczenie dostępu do bazy danych Serwera administracyjnego. Na przykład, udzielasz dostępu tylko z urządzenia Serwera administracyjnego. Zmniejsza to prawdopodobieństwo naruszenia bezpieczeństwa bazy danych Serwera administracyjnego z powodu znanych luk w zabezpieczeniach.

Możesz skonfigurować parametry zgodnie z instrukcją obsługi używanej bazy danych, a także udostępnić zamknięte porty na zaporach ogniowych.

Autoryzacja Microsoft SQL Server

Jeśli Kaspersky Security Center używa Microsoft SQL Server jako DBMS, konieczna jest ochrona danych Kaspersky Security Center przesyłanych do lub z bazy danych oraz danych przechowywanych w bazie danych przed nieautoryzowanym dostępem. Aby to zrobić, musisz zapewnić bezpieczną komunikację między Kaspersky Security Center a SQL Server. Najbardziej rozsądny sposób zapewnienia bezpiecznej komunikacji to zainstalowanie Kaspersky Security Center i SQL Server na tym samym urządzeniu i używanie mechanizmu pamięci współużytkowanej dla obu aplikacji. We wszystkich pozostałych przypadkach zalecane jest użycie certyfikatu SSL/TLS do uwierzytelniania instancji SQL Server.

Ogólnie rzecz biorąc, Serwer administracyjny może kontaktować się z serwerem SQL Server za pośrednictwem następujących dostawców:

- SQLOLEDB przy użyciu protokołu TCP/IP lub Named Pipes

  Ten dostawca jest instalowany w systemie operacyjnym Windows i używany domyślnie.

- MSOLEDBSQL przy użyciu protokołu TCP/IP, Named Pipes lub Shared memory

  Jeśli chcesz korzystać z tego dostawcy, musisz zainstalować go na urządzeniu z Serwerem administracyjnym, a następnie ustawić wartość `1` w globalnej zmiennej środowiskowej `KLDBADO_UseMSOLEDBSQL`.

- MSOLEDBSQL19 przy użyciu protokołu TCP/IP, Named Pipes lub Shared memory

  Jeśli chcesz korzystać z tego dostawcy, musisz zainstalować go na urządzeniu z Serwerem administracyjnym, a następnie ustaw wartość `1` w globalnej zmiennej środowiskowej `KLDBADO_UseMSOLEDBSQL` i wartość `MSOLEDBSQL19` w globalnej zmiennej środowiskowej `KLDBADO_ProviderName`.

Ponadto przed użyciem protokołu TCP/IP, Named Pipes lub Shared memory upewnij się, że wymagany protokół jest włączony.

Interakcja bezpieczeństwa z zewnętrznym systemem DBMS

Jeżeli system DBMS jest instalowany na oddzielnym urządzeniu podczas instalacji Serwera administracyjnego (zewnętrzny system DBMS), zalecamy skonfigurowanie parametrów bezpiecznej interakcji i uwierzytelniania z tym systemem DBMS. Aby uzyskać więcej informacji na temat konfigurowania uwierzytelniania SSL, zobacz Uwierzytelnianie serwera PostgreSQL i Scenariusz: Uwierzytelnianie serwera MySQL.

Konfigurowanie listy zezwolonych adresów IP do łączenia się z Serwerem administracyjnym

Domyślnie użytkownicy Kaspersky Security Center Linux mogą logować się do Kaspersky Security Center z dowolnego urządzenia, na którym zainstalowano Konsolę administracyjną opartą na MMC, Kaspersky Security Center Web Console lub aplikacje OpenAPI. Możesz skonfigurować serwer administracyjny tak, aby użytkownicy mogli łączyć się z nim tylko z urządzeń o dozwolonych adresach IP. Na przykład, jeśli intruz spróbuje nawiązać połączenie z Kaspersky Security Center za pośrednictwem Kaspersky Security Center Web Console Server zainstalowanego na urządzeniu, które nie znajduje się na liście zezwolonych, nie będzie mógł zalogować się do Kaspersky Security Center.

Konfigurowanie listy zezwolonych adresów IP do łączenia się z Kaspersky Security Center Web Console

Domyślnie użytkownicy Kaspersky Security Center mogą łączyć się z Kaspersky Security Center Web Console z dowolnego urządzenia. Na urządzeniu z Kaspersky Security Center Web Console należy skonfigurować zaporę sieciową (wbudowaną w system operacyjny lub innej firmy), aby użytkownicy mogli łączyć się z Kaspersky Security Center Web Console wyłącznie z dozwolonych adresów IP.

Bezpieczeństwo połączenia z kontrolerem domeny podczas przeszukiwania

Serwer administracyjny lub punkt dystrybucji systemu Linux łączy się z kontrolerem domeny za pośrednictwem protokołu LDAPS w celu przeszukania domeny. Domyślnie weryfikacja certyfikatu nie jest wymagana podczas łączenia. Aby wymusić weryfikację certyfikatu, należy ustawić flagę `KLNAG_LDAP_TLS_REQCERT` na 1. Można również określić niestandardową ścieżkę do urzędu certyfikacji (CA) w celu uzyskania dostępu do łańcucha certyfikatów, korzystając z flagi `KLNAG_LDAP_SSL_CACERT`.

Konta i uwierzytelnianie

Przed wykonaniem poniższych kroków utwórz kopię zapasową serwera administracyjnego Kaspersky Security Center za pomocą narzędzi Kopia zapasowa danych serwera administracyjnego lub klbackup i zapisz ją w bezpiecznym miejscu.

Używanie weryfikacji dwuetapowej z Serwerem administracyjnym

Kaspersky Security Center zapewnia weryfikację dwuetapową dla użytkowników Kaspersky Security Center Web Console i Konsoli administracyjnej w oparciu o standard RFC 6238 (TOTP: algorytm jednorazowych haseł czasowych).

Jeśli weryfikacja dwuetapowa jest włączona dla Twojego konta, za każdym razem, gdy logujesz się do Kaspersky Security Center Web Console lub Konsolę administracyjną, wprowadzasz swoją nazwę użytkownika, hasło i dodatkowy jednorazowy kod zabezpieczający. Jeśli korzystasz z uwierzytelniania domeny na swoim koncie, wystarczy wprowadzić dodatkowy jednorazowy kod zabezpieczający. Aby otrzymać jednorazowy kod zabezpieczający, musisz zainstalować aplikację uwierzytelniającą na swoim komputerze lub urządzeniu mobilnym.

Istnieją zarówno programowe, jak i sprzętowe uwierzytelniacze (tokeny), które obsługują standard RFC 6238. Na przykład uwierzytelniacze oprogramowania obejmują Google Authenticator, Microsoft Authenticator, FreeOTP.

Zdecydowanie nie zalecamy instalowania aplikacji uwierzytelniającej na tym samym urządzeniu, z którego nawiązywane jest połączenie z Serwerem administracyjnym. Możesz zainstalować aplikację uwierzytelniającą na swoim urządzeniu mobilnym.

Ograniczenie nowym użytkownikom możliwości konfigurowania dla siebie weryfikacji dwuetapowej

Aby jeszcze bardziej zwiększyć bezpieczeństwo dostępu do Kaspersky Security Center Web Console, możesz

uniemożliwienie nowym użytkownikom konfigurowania dla siebie weryfikacji dwuetapowej.

Jeśli ta opcja jest włączona, użytkownik z wyłączoną weryfikacją dwuetapową, na przykład nowy administrator domeny, nie może skonfigurować dla siebie weryfikacji dwuetapowej. W związku z tym takiego użytkownika nie można uwierzytelnić na Serwerze administracyjnym ani zalogować się do Kaspersky Security Center Web Console bez zgody innego administratora Kaspersky Security Center, który ma już włączoną weryfikację dwuetapową.

Używanie uwierzytelniania dwuskładnikowego dla systemu operacyjnego

Zalecamy używanie uwierzytelniania wieloskładnikowego (MFA) do uwierzytelniania na urządzeniu Serwera administracyjnego przy użyciu tokena, karty inteligentnej lub innej metody (jeśli to możliwe).

Ograniczenie możliwości zapisywania hasła administratora

Jeśli korzystasz z Konsoli administracyjnej, nie zalecamy zapisywania hasła administratora w oknie dialogowym połączenia z Serwerem administracyjnym.

Jeśli korzystasz z Kaspersky Security Center Web Console, nie zalecamy zapisywania hasła administratora w przeglądarce zainstalowanej na urządzeniu użytkownika.

Uwierzytelnianie wewnętrznego konta użytkownika

Domyślnie hasło do konta użytkownika wewnętrznego Serwera administracyjnego musi być zgodne z następującymi zasadami:

- Hasło musi zawierać od 8 do 256 znaków.
- Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
  - Wielkie litery (A-Z)
  - Małe litery (a-z)
  - Cyfry (0-9)
  - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków „.” i „@”, gdy „.” jest umieszczane przed „@”.

Domyślnie, maksymalna liczba dozwolonych prób wprowadzenia hasła to 10. Możesz zmienić liczby dozwolonych prób wprowadzenia hasła.

Użytkownik Kaspersky Security Center może wprowadzić niepoprawne hasło ograniczoną liczbę razy. Po osiągnięciu limitu, konto użytkownika zostaje zablokowane na godzinę.

Konfigurowanie opcji zmiany hasła konta użytkownika wewnętrznego

Zalecamy skonfigurowanie następujących opcji w celu zmiany hasła konta użytkownika wewnętrznego:

- Okres rotacji hasła
- Konfigurowanie czasu wstępnego ostrzeżenia o konieczności zmiany hasła
- Wartość opcji **Użytkownik musi zmienić hasło przy pierwszym logowaniu**

Ochrona przed nieautoryzowaną modyfikacją

Zalecamy włączenie dodatkowej opcji chroniącej konto użytkownika wewnętrznego Serwera administracyjnego przed nieautoryzowaną modyfikacją. Tę ochronę należy skonfigurować osobno dla każdego użytkownika wewnętrznego.

Dedykowana grupa administracyjna dla Serwera administracyjnego

Zalecamy utworzenie dedykowanej grupy administracyjnej dla Serwera administracyjnego. Przyznaj tej grupie specjalne prawa dostępu i utwórz dla niej specjalną zasadę zabezpieczeń.

Aby uniknąć celowego obniżania poziomu bezpieczeństwa Serwera administracyjnego, zalecamy ograniczenie listy kont, które mogą zarządzać dedykowaną grupą administracyjną.

Grupy KLAdmins i KLOperators

Podczas instalacji Kaspersky Security Center automatycznie tworzone są grupy KLAdmins i KLOperators. Grupa KLAdmins otrzymuje wszystkie prawa dostępu. Grupa KLOperators ma tylko uprawnienia do odczytu i wykonywania. Uprawnienia nadane grupie KLAdmins są **zablokowane**.

Możesz przeglądać grupy KLAdmins i KLOperators oraz wprowadzać w nich zmiany, używając standardowych narzędzi administracyjnych systemu operacyjnego.

Podczas opracowywania regulaminu pracy z Serwerem administracyjnym konieczne jest określenie, czy specjalista ds. bezpieczeństwa informacji potrzebuje pełnego dostępu (i przynależności do grupy KLAdmins) do wykonywania standardowych zadań.

Większość podstawowych zadań administracyjnych można rozdzielić między działy firmy (lub różnych pracowników tego samego działu), a co za tym idzie, między różne konta. Możesz także skonfigurować zróżnicowanie dostępu grup administracyjnych w Kaspersky Security Center. Dzięki temu możliwe jest zaimplementowanie scenariusza, w którym autoryzacja w ramach kont z grupy KLAdmins będzie nieprawidłowa i może zostać uznana za incydent.

Jeżeli Kaspersky Security Center został zainstalowany na koncie systemowym, grupy są tworzone tylko na urządzeniu Serwera administracyjnego. W takim przypadku zalecamy upewnienie się, że w grupie znajdują się tylko wpisy utworzone podczas instalacji Kaspersky Security Center. Nie zalecamy dodawania żadnych grup do grupy KLAdmins (lokalnej ani domeny), która jest tworzona automatycznie podczas instalacji Kaspersky Security Center. Należy także ograniczyć uprawnienia do zmiany tej grupy. Grupa KLAdmins może zawierać tylko pojedyncze nieuprzywilejowane konta.

Jeśli instalacja została przeprowadzona z poziomu konta użytkownika domeny, grupy KLAdmins i KLOperators są tworzone zarówno na Serwerze administracyjnym, jak i w domenie zawierającej Serwer administracyjny. Zalecane jest podobne podejście, takie jak instalacja konta lokalnego.

Ograniczanie członkostwa w roli Głównego administratora

Zalecamy ograniczenie członkostwa w roli Głównego administratora.

Domyślnie, po zainstalowaniu Serwera administracyjnego, rola głównego administratora jest przypisywana do lokalnej grupy administratorów i utworzonej grupy KLAdmins. Przydaje się do zarządzania, ale jest krytyczny z punktu widzenia bezpieczeństwa, ponieważ rola Głównego Administratora posiada szeroki zakres uprawnień, przydzielanie tej roli użytkownikom powinno być ściśle uregulowane.

Lokalni administratorzy mogą zostać wykluczeni z listy użytkowników z uprawnieniami administratora Kaspersky Security Center. Rola głównego administratora nie może zostać usunięta z grupy KLAdmins. Do grupy KLAdmins możesz dołączyć konta, które będą używane do zarządzania Serwerem administracyjnym.

Jeśli korzystasz z uwierzytelniania domeny, zalecamy ograniczenie uprawnień kont administratora domeny w Kaspersky Security Center. Domyślnie te konta mają rolę głównego administratora. Ponadto administrator domeny może dołączyć swoje konto do grupy KLAdmins, aby uzyskać rolę głównego administratora. Aby tego uniknąć, w ustawieniach bezpieczeństwa Kaspersky Security Center możesz dodać grupę Administratorzy domeny, a następnie zdefiniować dla niej reguły zakazujące. Zasady te muszą mieć pierwszeństwo przed dopuszczającymi.

Możesz także użyć predefiniowanych ról użytkowników z już skonfigurowanym zestawem uprawnień.

Konfigurowanie praw dostępu do funkcji aplikacji

Zalecamy korzystanie z elastycznej konfiguracji praw dostępu do funkcji Kaspersky Security Center dla każdego użytkownika lub grupy użytkowników.

Kontrola dostępu oparta na rolach umożliwia tworzenie standardowych ról użytkowników z predefiniowanym zestawem uprawnień i przypisywanie tych ról użytkownikom w zależności od ich zakresu obowiązków.

Główne zalety modelu kontroli dostępu opartego na rolach:

- Łatwość administracji
- Hierarchia ról

- Podejście w oparciu o najmniejsze uprawnienia
- Podział obowiązków

Możesz przypisywać wbudowane role do określonych pracowników na podstawie ich stanowisk lub tworzyć zupełnie nowe role.

Podczas konfigurowania ról zwróć uwagę na uprawnienia związane ze zmianą stanu ochrony urządzenia Serwera administracyjnego i zdalną instalacją oprogramowania firm trzecich:

- Zarządzanie grupami administracyjnymi.
- Operacje z Serwerem administracyjnym.
- Instalacja zdalna.
- Zmiana parametrów przechowywania zdarzeń i wysyłania powiadomień.

  To uprawnienie umożliwia ustawienie powiadomień uruchamiających skrypt lub moduł wykonywalny na urządzeniu Serwera administracyjnego po wystąpieniu zdarzenia.

Osobne konto do zdalnej instalacji aplikacji

Oprócz podstawowego zróżnicowania praw dostępu, zalecamy ograniczenie zdalnej instalacji aplikacji dla wszystkich kont (z wyjątkiem Głównego Administratora lub innego konta specjalistycznego).

Zalecamy korzystanie z osobnego konta do zdalnej instalacji aplikacji. Możesz przypisać rolę lub uprawnienia do osobnego konta.

Zabezpieczanie uprzywilejowanego dostępu do systemu Windows

Zalecamy uwzględnienie zaleceń firmy Microsoft dotyczących zapewnienia bezpieczeństwa dostępu uprzywilejowanego. Aby wyświetlić te zalecenia, przejdź do sekcji Zabezpieczanie uprzywilejowanego dostępu artykuł.

Jednym z kluczowych punktów rekomendacji jest wdrożenie Stacji Roboczych z Dostępem Uprzywilejowanym (PAW).

Używanie zarządzanego konta usługi (MSA) lub zarządzanych grupowo kont usługi (gMSA) do uruchamiania usługi Serwera administracyjnego

Usługa Active Directory ma specjalny typ kont do bezpiecznego uruchamiania usług, zwany grupowym kontem usługi zarządzanej (MSA/gMSA). Kaspersky Security Center obsługuje zarządzane konta usługi (MSA) i grupę zarządzanych kont usługi (gMSA). Jeśli w Twojej domenie używane są tego typu konta, możesz wybrać jedno z nich jako konto dla usługi Serwera administracyjnego.

Regularny audyt wszystkich użytkowników i działań użytkowników

Zalecamy przeprowadzanie regularnego audytu wszystkich użytkowników na urządzeniu Serwera administracyjnego. Pozwala to reagować na określone rodzaje zagrożeń bezpieczeństwa związanych z możliwym naruszeniem bezpieczeństwa urządzenia.

Można także śledzić działania użytkowników, takie jak łączenie się i rozłączanie z Serwerem administracyjnym, łączenie się z Serwerem administracyjnym z błędem, a także modyfikacje obiektów (w przypadku obiektów obsługujących zarządzanie wersjami).

Zarządzanie ochroną Serwera administracyjnego

Wybieranie oprogramowania zabezpieczającego Serwer administracyjny

W zależności od typu wdrożenia Serwera administracyjnego i ogólnej strategii ochrony wybierz aplikację, która ma chronić urządzenie Serwera administracyjnego.

Jeśli instalujesz Serwer administracyjny na dedykowanym urządzeniu, zalecamy wybranie aplikacji Kaspersky Endpoint Security w celu ochrony urządzenia Serwera administracyjnego. Pozwala to na zastosowanie wszystkich dostępnych technologii do ochrony urządzenia Serwera administracyjnego, w tym modułów analizy behawioralnej.

Jeżeli Serwer administracyjny jest zainstalowany na urządzeniu, które istnieje w infrastrukturze i było wcześniej używane do innych zadań, zalecamy rozważenie następującego oprogramowania zabezpieczającego:

- Kaspersky Industrial CyberSecurity for Nodes. Zalecamy zainstalowanie tej aplikacji na urządzeniach wchodzących w skład sieci przemysłowej. Kaspersky Industrial CyberSecurity for Nodes to aplikacja, która posiada certyfikaty kompatybilności z różnymi producentami oprogramowania przemysłowego.
- Zalecane rozwiązania zabezpieczające. Jeśli Serwer administracyjny jest zainstalowany na urządzeniu z innym oprogramowaniem, zalecamy uwzględnienie zaleceń tego dostawcy oprogramowania dotyczących kompatybilności produktów zabezpieczających (mogą już istnieć zalecenia dotyczące wyboru rozwiązania zabezpieczającego i konieczne może być skonfigurowanie strefy zaufanej).

Tworzenie osobnej zasady zabezpieczeń dla aplikacji zabezpieczającej

Zalecamy utworzenie oddzielnej zasady zabezpieczeń dla aplikacji chroniącej urządzenie Serwera administracyjnego. Ta zasada musi różnić się od zasady zabezpieczeń dla urządzeń klienckich. Pozwala to na określenie najbardziej odpowiednich ustawień bezpieczeństwa dla Serwera administracyjnego, bez wpływu na poziom ochrony innych urządzeń.

Zalecamy podzielenie urządzeń na grupy, a następnie umieszczenie urządzenia Serwera administracyjnego w osobnej grupie, dla której można utworzyć specjalną zasadę zabezpieczeń.

Moduły ochrony

Jeśli nie ma specjalnych zaleceń od dostawcy oprogramowania innej firmy zainstalowanego na tym samym urządzeniu co Serwer administracyjny, zalecamy aktywację i skonfigurowanie wszystkich dostępnych modułów ochrony (po sprawdzeniu działania tych modułów ochrony przez określony czas).

Konfigurowanie zapory sieciowej urządzenia Serwera administracyjnego

Na urządzeniu Serwera administracyjnego zalecamy skonfigurowanie zapory sieciowej w celu ograniczenia liczby urządzeń, z których administratorzy mogą łączyć się z Serwerem administracyjnym poprzez Konsolę administracyjną lub Kaspersky Security Center Web Console.

Domyślnie Serwer administracyjny używa portu 13291 do odbierania połączeń z Konsoli administracyjnej oraz portu 13299 do odbierania połączeń z Kaspersky Security Center Web Console. Zalecamy ograniczenie liczby urządzeń, z których Serwer administracyjny może być zarządzany przy użyciu tych portów.

Zarządzanie ochroną urządzeń klienckich

Ograniczenie dodawania kluczy licencyjnych do pakietów instalacyjnych

Pakiety instalacyjne są przechowywane w folderze współdzielonym Serwera administracyjnego, w podfolderze Pakiety. Jeśli dodasz klucz licencyjny do pakietu instalacyjnego, klucz licencyjny może zostać naruszony, ponieważ udostępnione prawa dostępu Odczyt są włączone do repozytorium pakietów instalacyjnych.

Aby uniknąć naruszenia klucza licencyjnego, nie zalecamy dodawania kluczy licencyjnych do pakietów instalacyjnych.

Zalecamy korzystanie z automatycznej dystrybucji kluczy licencyjnych do zarządzanych urządzeń, wdrażanie za pomocą zadania Dodaj klucz licencyjny dla zarządzanej aplikacji oraz ręczne dodawanie kodu aktywacyjnego lub pliku klucza do urządzeń.

Automatyczne reguły przenoszenia urządzeń pomiędzy grupami administracyjnymi

Zalecamy ograniczenie stosowania automatycznych reguł przenoszenia urządzeń między grupami administracyjnymi.

Jeśli używasz automatycznych reguł przenoszenia urządzeń, może to prowadzić do propagowania zasad, które zapewniają przenoszonemu urządzeniu większe uprawnienia niż urządzenie przed przeniesieniem.

Ponadto przeniesienie urządzenia klienckiego do innej grupy administracyjnej może spowodować propagację ustawień zasad. Te ustawienia zasad mogą być niepożądane w przypadku dystrybucji do urządzeń gościa i niezaufanych.

To zalecenie nie dotyczy jednorazowego wstępnego przydziału urządzeń do grup administracyjnych.

Wymagania bezpieczeństwa dla punktów dystrybucji i bram połączeń

Urządzenia z zainstalowanym Agentem sieciowym mogą działać jako punkt dystrybucji i wykonywać następujące funkcje:

- Rozsyłaj aktualizacje i pakiety instalacyjne otrzymane z Serwera administracyjnego na urządzenia klienckie w grupie.
- Wykonaj zdalną instalację oprogramowania innych firm i aplikacji Kaspersky na urządzeniach klienckich.
- Przeszukiwać sieć w celu odnalezienia nowych urządzeń i zaktualizowania informacji o tych istniejących. Punkt dystrybucji może wykorzystywać te same metody wykrywania urządzeń, co Serwer administracyjny.

Umieszczanie punktów dystrybucji w sieci organizacji służących do:

- Zmniejszanie obciążenia na Serwerze administracyjnym
- Optymalizacja ruchu
- Zapewnienie Serwerowi administracyjnemu dostępu do urządzeń w trudno dostępnych częściach sieci

Biorąc pod uwagę dostępne możliwości, zalecamy zabezpieczenie urządzeń pełniących rolę punktów dystrybucji przed wszelkiego rodzaju nieautoryzowanym dostępem (w tym fizycznym).

Ograniczenie automatycznego przydzielania punktów dystrybucji

Aby uprościć administrację i zachować funkcjonalność sieci, zalecamy automatyczne przydzielanie punktów dystrybucji. Jednak w przypadku sieci przemysłowych i małych sieci zalecamy unikanie automatycznego przypisywania punktów dystrybucji, ponieważ na przykład prywatne informacje o kontach używanych do przesyłania zadań instalacji zdalnej mogą być przesyłane do punktów dystrybucji za pomocą systemu operacyjnego.

W przypadku sieci przemysłowych i małych sieci można ręcznie przypisać urządzenia, które będą działać jako punkty dystrybucji.

Możesz także przeglądać Raport z działalności punktów dystrybucji.

Wymagania bezpieczeństwa dla urządzeń użytkowników Kaspersky Security Center

Urządzenia użytkowników Kaspersky Security Center muszą spełniać specjalne wymagania bezpieczeństwa. Zalecamy zabezpieczenie tych urządzeń przed wszelkiego rodzaju nieautoryzowanym dostępem (również fizycznym):

Urządzenia użytkowników Kaspersky Security Center obejmują:

- Urządzenia, z których użytkownicy łączą się z Kaspersky Security Center Web Console za pomocą przeglądarki.
- Urządzenia, z których użytkownicy łączą się z Kaspersky Security Center przy użyciu konsoli administracyjnej opartej na MMC.
- Urządzenia, z których aplikacje, które komunikują się z Serwerem administracyjnym za pośrednictwem OpenAPI, są połączone z Kaspersky Security Center.

Wymagania bezpieczeństwa dla urządzeń z zainstalowaną Kaspersky Security Center Web Console

Urządzenia z zainstalowaną Kaspersky Security Center Web Console służą do zarządzania systemem Kaspersky Security Center, dlatego też muszą spełniać specjalne wymagania dotyczące bezpieczeństwa tych urządzeń. Zalecamy zabezpieczenie tych urządzeń przed wszelkiego rodzaju nieautoryzowanym dostępem (również fizycznym).

Konfigurowanie ochrony dla zarządzanych aplikacji

Zasady aplikacji zarządzanych

Zalecamy utworzenie zasady dla każdego typu używanej aplikacji i każdego komponentu Kaspersky Security Center (Agent sieciowy, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Agent itp.). Ta zasada musi być zastosowana do wszystkich zarządzanych urządzeń (główna grupa administracyjna) lub do oddzielnej grupy, do której nowe zarządzane urządzenia są automatycznie przenoszone zgodnie ze skonfigurowanymi regułami przenoszenia.

Określenie hasła do wyłączenia ochrony i odinstalowania aplikacji

Aby uniemożliwić intruzom wyłączenie aplikacji zabezpieczających Kaspersky, zdecydowanie zalecamy włączenie ochrony hasłem przy wyłączaniu ochrony i dezinstalacji aplikacji zabezpieczających Kaspersky. Można ustawić hasło na przykład dla Kaspersky Endpoint Security for Windows, Kaspersky Security for Windows Servers, Agenta sieciowego i innych aplikacji Kaspersky. Po włączeniu ochrony hasłem zalecamy zablokowanie tych ustawień poprzez zamknięcie „kłódki".

Określanie hasła do ręcznego połączenia urządzenia klienckiego z Serwerem administracyjnym (narzędzie klmover)

Narzędzie klmover umożliwia ręczne podłączenie urządzenia klienckiego do Serwera administracyjnego. Podczas instalacji Agenta sieciowego na urządzeniach klienckich narzędzie jest automatycznie kopiowane do folderu instalacyjnego Agenta sieciowego.

Aby uniemożliwić intruzom przeniesienie urządzeń poza Serwer administracyjny kontrolujący, zdecydowanie zalecamy włączenie ochrony hasłem podczas uruchamiania narzędzia klmover. Aby włączyć ochronę hasłem, wybierz opcję **Użyj hasła dezinstalacyjnego** w ustawieniach zasady Agenta sieciowego.

Narzędzie klmover wymaga uprawnień administratora lokalnego. Zabezpieczenie hasłem do uruchomienia narzędzia klmover można pominąć w przypadku urządzeń obsługiwanych bez uprawnień administratora lokalnego.

Włączenie opcji **Użyj hasła dezinstalacyjnego** umożliwia również ochronę hasłem narzędzia Cleaner (cleaner.exe).

Używanie Kaspersky Security Network

We wszystkich zasadach zarządzanych aplikacji oraz we właściwościach Serwera administracyjnego zalecamy włączenie korzystania z Kaspersky Security Network (KSN) i zaakceptowanie Oświadczenia KSN. Podczas aktualizacji lub aktualizacji Serwera administracyjnego możesz zaakceptować zaktualizowane Oświadczenie KSN. W niektórych przypadkach, gdy korzystanie z usług w chmurze jest zabronione przez prawo lub inne przepisy, możesz wyłączyć KSN.

Regularne skanowanie zarządzanych urządzeń

W przypadku wszystkich grup urządzeń zalecamy utworzenie zadania, które okresowo przeprowadza pełne skanowanie urządzeń.

Odkrywanie nowych urządzeń

Zalecamy odpowiednie skonfigurowanie ustawień wykrywania urządzeń: skonfiguruj integrację z Active Directory, a także określ zakresy adresów IP do wykrywania nowych urządzeń.

Ze względów bezpieczeństwa możesz użyć domyślnej grupy administracyjnej, która obejmuje wszystkie nowe urządzenia oraz domyślne zasady mające wpływ na tę grupę.

Wybieranie folderu współdzielonego

W przypadku wdrażania Serwera administracyjnego na urządzeniu z systemem Windows z wyborem istniejącego folderu współdzielonego (który jest używany na przykład do umieszczania pakietów instalacyjnych i przechowywania zaktualizowanych baz danych), zalecamy upewnienie się, że uprawnienia do odczytu są przyznane grupie Wszyscy, a uprawnienia do zapisu są przyznane grupie KLAdmins.

Konserwacja Serwera administracyjnego

Tworzenie kopii zapasowych danych Serwera administracyjnego

Kopia zapasowa danych umożliwia przywrócenie danych Serwera administracyjnego bez utraty danych.

Domyślnie zadanie tworzenia kopii zapasowej danych jest tworzone automatycznie po instalacji Serwera administracyjnego i jest wykonywane okresowo, zapisując kopie zapasowe w odpowiednim katalogu. Ustawienia zadania tworzenia kopii zapasowej danych można zmienić w następujący sposób:

- Częstotliwość tworzenia kopii zapasowych wzrasta
- Określono specjalny katalog do zapisywania kopii
- Zmieniono hasła do kopii zapasowych

Jeśli przechowujesz kopie zapasowe w specjalnym katalogu, innym niż katalog domyślny, zalecamy ograniczenie listy kontroli dostępu (ACL) do tego katalogu. Konta Serwera administracyjnego oraz konta bazy danych Serwera administracyjnego muszą mieć uprawnienia do zapisu dla tego katalogu.

Konserwacja Serwera administracyjnego

Konserwacja Serwera administracyjnego pozwala na zmniejszenie rozmiaru bazy danych oraz zwiększenie wydajności i ulepszenie działania aplikacji. Zalecamy przeprowadzanie konserwacji Serwera administracyjnego przynajmniej raz w tygodniu.

Konserwacja Serwera administracyjnego jest wykonywana przy pomocy dedykowanego zadania. Podczas konserwacji Serwera administracyjnego aplikacja wykonuje następujące działania:

- Sprawdza, czy w bazie danych znajdują się jakiekolwiek błędy
- Reorganizuje indeksy w bazie danych
- Aktualizuje statystyki bazy danych
- Zmniejsza bazę danych (jeśli to konieczne)

Instalowanie aktualizacji systemu operacyjnego i aktualizacji oprogramowania innych firm

Zdecydowanie zalecamy regularne instalowanie aktualizacji oprogramowania dla systemu operacyjnego i oprogramowania innych firm na urządzeniu Serwera administracyjnego.

Urządzenia klienckie nie wymagają ciągłego połączenia z Serwerem administracyjnym, dlatego bezpieczne jest ponowne uruchomienie urządzenia Serwera administracyjnego po zainstalowaniu aktualizacji. Wszystkie zdarzenia zarejestrowane na urządzeniach klienckich podczas przestoju Serwera administracyjnego są do niego wysyłane po przywróceniu połączenia.

Transfer zdarzeń do systemów innych producentów

Monitorowanie i raportowanie

W celu szybkiego reagowania na problemy związane z bezpieczeństwem zalecamy skonfigurowanie funkcji monitorowania i raportowania.

Eksportowanie zdarzeń do systemów SIEM

W celu szybkiego wykrycia problemów związanych z bezpieczeństwem, zanim wystąpią poważne szkody, zalecamy wykorzystanie eksportu zdarzeń w systemie SIEM.

Powiadomienia e-mail o zdarzeniach audytu

Kaspersky Security Center umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. W celu szybkiego reagowania na sytuacje awaryjne zalecamy skonfigurowanie Serwera administracyjnego do wysyłania powiadomień o zdarzeniach audytu, zdarzeniach krytycznych, zdarzeniach błędu i ostrzeżeniach, które publikuje.

Ponieważ zdarzenia te są zdarzeniami wewnątrzsystemowymi, można spodziewać się ich niewielkiej liczby, co ma zastosowanie w przypadku wysyłki.

Statystyki funkcji Serwera administracyjnego

Aby zapewnić szybką reakcję na problemy z bezpieczeństwem, zalecamy skonfigurowanie wysyłania statystyk funkcji Serwera administracyjnego do aplikacji innych firm za pomocą protokołu SNMP (Simple Network Management Protocol).

Zalecenia dotyczące bezpieczeństwa systemów informatycznych innych firm

Zalecenia dotyczące bezpieczeństwa z CIS Benchmarks

W przypadku korzystania z wersji systemów operacyjnych, platform wirtualizacyjnych lub serwerów baz danych obsługiwanych przez Serwer administracyjny i Agenta sieciowego, zalecamy zastosowanie najlepszych praktyk bezpieczeństwa informacji z Centrum Bezpieczeństwa Internetowego (CIS), jeśli takie istnieją, w celu dostrojenia tych systemów informatycznych.

Centrum Bezpieczeństwa Internetu (CIS) jest organizacją non-profit zajmującą się poprawą bezpieczeństwa w dziedzinie technologii informatycznych. W szczególności CIS opracowuje i dystrybuuje standardy bezpieczeństwa, takie jak CIS Controls i CIS Benchmarks. Standardy te stanowią zbiór zaleceń i praktyk zapewniających bezpieczeństwo systemów informatycznych.

Portal CIS zawiera rekomendacje dla wersji następujących systemów informatycznych obsługiwanych przez Serwer administracyjny i Agenta sieciowego:

- Systemy operacyjne następujących rodzin:
  - Windows dla komputerów stacjonarnych
  - Windows dla serwerów
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- Platformy wirtualizacyjne VMware
- Serwery baz danych:
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Zalecenia dotyczące bezpieczeństwa dla systemu operacyjnego Astra Linux

Korzystając z systemu operacyjnego Astra Linux należy przestrzegać zaleceń dotyczących bezpieczeństwa opisanych w czerwonej księdze dla odpowiedniej wersji Astra Linux.

Zalecenia dotyczące bezpieczeństwa dla systemu operacyjnego RED OS

Korzystając z systemu operacyjnego RED OS, należy stosować się do zaleceń dotyczących bezpieczeństwa z podręcznika administratora opisanych w oficjalnej dokumentacji RED OS.

Zalecenia dotyczące korzystania z aplikacji zabezpieczających Kaspersky

Korzystanie z hasła KLAdmin w Kaspersky Endpoint Security for Windows

Z jednego urządzenia z zainstalowanym programem Kaspersky Endpoint Security for Windows może korzystać wielu użytkowników o różnym poziomie znajomości obsługi komputera. Jeśli użytkownicy mają nieograniczony dostęp do programu Kaspersky Endpoint Security for Windows i jego ustawień, ogólny poziom ochrony urządzenia może być obniżony. Ochrona hasłem umożliwia ograniczenie dostępu użytkowników do Kaspersky Endpoint Security for Windows na podstawie przyznanych im uprawnień (na przykład uprawnienia do zamykania aplikacji).

Jednym ze sposobów ograniczenia dostępu do Kaspersky Endpoint Security for Windows i jego parametrów jest użycie konta KLAdmin. Konto KLAdmin to konto administratora z nieograniczonym dostępem do programu Kaspersky Endpoint Security for Windows. Konto KLAdmin ma prawo do wykonywania wszelkich działań chronionych hasłem w programie Kaspersky Endpoint Security for Windows. Uprawnień konta KLAdmin nie można cofnąć. Możesz ustawić hasło do konta KLAdmin we właściwościach zasad Kaspersky Endpoint Security for Windows. Administrator Kaspersky Endpoint Security for Windows ponosi pełną odpowiedzialność za bezpieczne korzystanie z hasła do konta KLAdmin. Jeśli Twoja organizacja ma własną politykę dotyczącą haseł, postępuj zgodnie z instrukcjami zawartymi w tej polityce.

Nasze zalecenia dotyczące ochrony organizacji przed kradzieżą hasła KLAdmin są następujące:

- **Wymagania ogólne**

  Nie używaj nazwy konta ani części nazwy jako hasła.

- **Minimalne wymagania dotyczące długości hasła**

  Utwórz hasło składające się z co najmniej 10 znaków.

- **Wymagania dotyczące korzystania z wielu rodzajów znaków**

  Ustaw złożone hasło, które będzie zawierać znaki z różnych kategorii: małe i wielkie litery, cyfry oraz znaki specjalne.

- **Wymagania dotyczące wygaśnięcia hasła**

  Ustaw minimalny okres ważności hasła wynoszący 90 dni. Nowe hasło nie może być takie samo jak jakiekolwiek hasło z 24 ostatnio użytych haseł.

Przygotowanie do wdrożenia

Ta sekcja opisuje kroki, jakie należy podjąć przed zainstalowaniem Kaspersky Security Center.

Planowanie instalacji Kaspersky Security Center

Ta sekcja zawiera informacje o najbardziej odpowiednich opcjach instalacji komponentów Kaspersky Security Center w sieci organizacji w zależności od następujących kryteriów:

- Całkowitą liczbę urządzeń
- Jednostki (biura lokalne, oddziały), które są oddalone geograficznie lub pod względem organizacyjnym
- Oddalone od siebie sieci połączone wąskimi kanałami
- Potrzeba uzyskania dostępu do Serwera administracyjnego przez Internet

Typowe schematy wdrażania systemu ochrony

Ta sekcja opisuje standardowe schematy wdrażania systemu ochrony w sieci firmowej, korzystając z Kaspersky Security Center.

System musi być chroniony przed wszelkimi rodzajami nieautoryzowanego dostępu. Przed zainstalowaniem aplikacji na urządzeniu i fizyczną ochroną Serwerów administracyjnych i punktów dystrybucji zalecamy zainstalowanie wszystkich dostępnych aktualizacji zabezpieczeń dla systemu operacyjnego.

Możesz użyć Kaspersky Security Center do wdrożenia systemu ochrony w sieci korporacyjnej, wykorzystując następujące schematy:

- Wdrożenie systemu ochrony poprzez Kaspersky Security Center przy pomocy jednej z następujących metod:
  - Poprzez Konsolę administracyjną
  - Poprzez Kaspersky Security Center Web Console

  Aplikacje Kaspersky są instalowane automatycznie na urządzeniach klienckich, które łączą się automatycznie z Serwerem administracyjnym poprzez Kaspersky Security Center.

  Podstawowy schemat zdalnej instalacji to instalacja systemu ochrony poprzez Konsolę administracyjną. Korzystanie z Kaspersky Security Center Web Console umożliwia instalację aplikacji Kaspersky z poziomu przeglądarki internetowej.
- Ręczna instalacja systemu ochrony przy pomocy autonomicznych pakietów instalacyjnych wygenerowanych przez Kaspersky Security Center.

  Instalacja aplikacji Kaspersky na urządzeniach klienckich i stacji roboczej administratora jest wykonywana ręcznie; ustawienia połączenia urządzeń klienckich z Serwerem administracyjnym są określane podczas instalacji Agenta sieciowego.

Ta metoda wdrożenia jest zalecana w sytuacjach, gdy zdalna instalacja nie jest możliwa.

Kaspersky Security Center umożliwia także wdrożenie systemu ochrony przy użyciu zasad grupy Microsoft Active Directory®.

Informacje dotyczące planowania instalacji Kaspersky Security Center w sieci organizacji

Jeden Serwer administracyjny może obsługiwać maksymalnie 100 000 urządzeń. Jeśli całkowita liczba urządzeń w sieci organizacji przekroczy 100 000, wówczas w tej sieci należy zainstalować kilka Serwerów administracyjnych i połączyć je w hierarchię w celu uproszczenia scentralizowanego zarządzania.

Jeśli organizacja zawiera znaczną liczbę zdalnych biur lokalnych (oddziałów), z których każdy posiada swojego administratora, znacznym ułatwieniem będzie zainstalowanie Serwera administracyjnego w każdym z tych biur. W przeciwnym razie biura te należy postrzegać jako odizolowane sieci komunikujące się przez wąskie kanały; patrz sekcja „Standardowa konfiguracja: Duże oddziały posiadające swoich administratorów".

Podczas korzystania z oddalonych od siebie sieci połączonych wąskimi kanałami, ruch sieciowy można zmniejszyć, wskazując kilku Agentów sieciowych jako punkty dystrybucji (zapoznaj się z tabelą zawierającą wyliczenie liczby punktów dystrybucji). W tym przypadku wszystkie urządzenia w oddalonej sieci pobierają uaktualnienia z tych lokalnych centrów aktualizacji. Punkty dystrybucji mogą pobrać uaktualnienia zarówno z Serwera administracyjnego (domyślny scenariusz) oraz z serwerów Kaspersky dostępnych w Internecie (patrz sekcja „Standardowa konfiguracja: Małe zdalne biura").

Sekcja „Standardowa konfiguracja Kaspersky Security Center" zawiera szczegółowy opis standardowej konfiguracji Kaspersky Security Center. Podczas planowania instalacji wybierz najodpowiedniejszą konfigurację, mając na uwadze strukturę organizacji.

Na etapie planowania wdrożenia należy rozważyć przydzielenie do Serwera administracyjnego specjalnego certyfikatu X.509. Przydzielenie certyfikatu X.509 do Serwera administracyjnego może być przydatne między innymi do:

- Sprawdzania ruchu SSL poprzez kończenie żądań SSL na serwerze proxy lub do korzystania ze zwrotnego serwera proxy
- Integracji z infrastrukturą kluczy publicznych (PKI) organizacji
- Określenia wymaganych wartości w polach certyfikatu
- Zapewnienia wymaganej siły szyfrowania certyfikatu

Wybieranie struktury ochrony firmy

Wybór struktury ochrony organizacji jest definiowany przez następujące czynniki:

- Topologię sieci firmy.
- Strukturę organizacyjną.
- Liczbę pracowników zajmujących się ochroną sieci, a także zakres ich obowiązków.
- Zasoby sprzętu, które mogą zostać przydzielone dla komponentów do zarządzania ochroną.

- Przepustowość kanałów komunikacji, które mogą zostać przydzielone w celu utrzymania działania składników ochrony w sieci organizacji.

- Ograniczenia czasu wykonywania krytycznych działań administracyjnych w sieci firmowej. Na krytyczne działania administracyjne składają się, na przykład, dystrybucja uaktualnień antywirusowych baz danych i modyfikacja zasad dla urządzeń klienckich.

Podczas wybierania struktury ochrony zalecamy najpierw określić dostępną sieć i zasoby sprzętu, które będą wykorzystane do działania scentralizowanego systemu ochrony.

W celu przeprowadzenia analizy infrastruktury sprzętu i sieci zalecane jest wykonanie następujących czynności:

1. Określenie następujących ustawień sieci, w obrębie której zostanie zainstalowana ochrona:

   - Liczba segmentów sieci.

   - Prędkość komunikacji przez kanały komunikacyjne pomiędzy pojedynczymi segmentami sieci.

   - Liczba zarządzanych urządzeń w każdym segmencie sieci.

   - Przepustowość każdego kanału komunikacji, który może zostać przydzielony w celu utrzymania działania ochrony.

2. Określenie maksymalnego dozwolonego czasu na wykonanie kluczowych działań administracyjnych dla wszystkich zarządzanych urządzeń.

3. Przeanalizuj informacje z kroków 1 i 2, a także dane z testów obciążeniowych systemu administracyjnego. Opierając się na wynikach analizy, odpowiedz na następujące pytania:

   - Czy jest możliwa obsługa wszystkich klientów przy pomocy pojedynczego Serwera administracyjnego, czy też niezbędna jest hierarchia Serwerów administracyjnych?

   - Jaka konfiguracja sprzętowa Serwerów administracyjnych jest potrzebna do zajmowania się wszystkimi klientami w przedziale czasu określonym w punkcie 2?

   - Czy konieczne jest użycie punktów dystrybucji do zmniejszenia obciążenia kanałów komunikacji?

Po uzyskaniu odpowiedzi na powyższe pytania, możesz stworzyć zestaw dozwolonych struktur ochrony organizacji.

W sieci firmowej można użyć jednej z poniższych standardowych struktur ochrony:

- Jeden Serwer administracyjny. Wszystkie urządzenia klienckie są połączone z jednym Serwerem administracyjnym. Serwer administracyjny działa jako punkt dystrybucji.

- Jeden Serwer administracyjny z punktami dystrybucji. Wszystkie urządzenia klienckie są połączone z jednym Serwerem administracyjnym. Niektóre urządzenia klienckie w sieci działają jako punkty dystrybucji.

- Hierarchia Serwerów administracyjnych. Dla każdego segmentu sieci przydzielony jest pojedynczy Serwer administracyjny, który staje się częścią ogólnej hierarchii Serwerów administracyjnych. Główny Serwer administracyjny działa jako punkt dystrybucji.

- Hierarchia Serwerów administracyjnych z punktami dystrybucji. Dla każdego segmentu sieci przydzielony jest pojedynczy Serwer administracyjny, który staje się częścią ogólnej hierarchii Serwerów administracyjnych. Niektóre urządzenia klienckie w sieci działają jako punkty dystrybucji.

Standardowa konfiguracja Kaspersky Security Center

Ta sekcja opisuje standardowe konfiguracje używane podczas wdrażania komponentów Kaspersky Security Center w sieci organizacji:

- Jedno biuro
- Kilka dużych oddziałów, które są oddalone geograficznie od siebie i posiadają swoich własnych administratorów
- Wiele małych biur, które są oddalone geograficznie od siebie

Standardowa konfiguracja: Jedno biuro

W sieci organizacji można zainstalować jeden lub kilka Serwerów administracyjnych. Liczba Serwerów administracyjnych może zostać wybrana w oparciu o dostępny sprzęt lub całkowitą liczbę zarządzanych urządzeń.

Jeden Serwer administracyjny może obsługiwać maksymalnie 100 000 urządzeń. Należy rozważyć możliwość zwiększenia liczby zarządzanych urządzeń w najbliższej przyszłości: wygodniejsze może być podłączenie do jednego Serwera administracyjnego mniejszej liczby urządzeń.

Serwery administracyjne mogą być instalowane w sieci wewnętrznej lub w strefie DMZ, w zależności od tego, czy wymagany jest dostęp do Serwera administracyjnego przez Internet.

Jeśli jest używanych kilka Serwerów, zalecane jest połączenie ich w hierarchię. Korzystanie z hierarchii Serwerów administracyjnych pozwala uniknąć mieszania zasad i zadań oraz zarządzać całym zbiorem zarządzanych urządzeń tak, jakby były zarządzane przez jeden Serwer administracyjny (czyli wyszukiwać urządzenia, tworzyć wybory urządzeń oraz generować raporty).

Standardowa konfiguracja: Duże oddziały posiadające swoich administratorów

Jeśli organizacja posiada kilka dużych oddziałów, które są oddalone geograficznie od siebie, należy uwzględnić opcję wdrożenia Serwerów administracyjnych w każdym z biur. W jednym biurze można wdrożyć jeden lub kilka Serwerów administracyjnych, w zależności od liczby urządzeń klienckich i dostępnego sprzętu. W tym przypadku, dla każdego z biur można przeprowadzić „Standardową konfigurację: Jedno biuro". Aby ułatwić zarządzanie, zalecane jest połączenie wszystkich Serwerów administracyjnych w hierarchię (najlepiej wielopoziomową).

Jeśli niektórzy pracownicy przemieszczają się między biurami ze swoimi urządzeniami (laptopami), utwórz profile połączenia Agenta sieciowego w zasadzie Agenta sieciowego. Profile połączeń Agenta sieciowego są obsługiwane tylko dla urządzeń Windows i macOS.

Standardowa konfiguracja: Małe zdalne biura

Ta standardowa konfiguracja została utworzona z myślą o głównej siedzibie i wielu małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem Internetu. Każde z tych zdalnych biur może znajdować się poza NAT (Network Address Translation - translacja adresów sieciowych), czyli nie można nawiązać połączenia między dwoma zdalnymi biurami, gdyż są odizolowane.

W głównej siedzibie należy zainstalować Serwer administracyjny, natomiast we wszystkich pozostałych biurach należy przydzielić jeden lub kilka punktów dystrybucji. Jeśli biura są połączone przez internet, przydatne może być utworzenie zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla punktów dystrybucji, aby mogły one pobierać uaktualnienia bezpośrednio z serwerów Kaspersky, folderu lokalnego lub sieciowego, a nie z Serwera administracyjnego.

Jeśli niektóre urządzenia w zdalnym biurze nie mają bezpośredniego dostępu do Serwera administracyjnego (na przykład, dostęp do Serwera administracyjnego jest możliwy przez Internet, ale niektóre urządzenia nie mają dostępu do Internetu), punkty dystrybucji muszą zostać przełączone do trybu bramy połączenia. W tym przypadku Agenty sieciowe na urządzeniach w zdalnym biurze zostaną połączone, w celu dalszej synchronizacji, z Serwerem administracyjnym, ale poprzez bramę, a nie bezpośrednio.

Ponieważ Serwer administracyjny najprawdopodobniej nie będzie mógł przeszukać sieci zdalnego biura, zalecane jest przekazanie tej funkcji punktowi dystrybucji.

Serwer administracyjny nie będzie mógł wysyłać powiadomień poprzez port UDP o numerze 15000 na zarządzane urządzenia znajdujące się poza NAT w zdalnym biurze. Aby rozwiązać ten problem, we właściwościach urządzeń pełniących rolę punktów dystrybucji możesz włączyć tryb stałego połączenia z Serwerem administracyjnym (pole **Nie odłączaj od Serwera administracyjnego**). Ten tryb jest dostępny, jeśli całkowita liczba punktów dystrybucji nie przekracza 300. Aby zapewnić ciągłą łączność między zarządzanym urządzeniem a Serwerem administracyjnym, należy używać serwerów push. Szczegółowe informacje można znaleźć w następującym temacie: Używanie punktu dystrybucji jako serwera push.

Wybieranie systemu zarządzania bazą danych (DBMS) dla Serwera administracyjnego

Podczas wybierania systemu zarządzania bazą danych (DBMS), który zostanie użyty przez Serwer administracyjny, należy brać pod uwagę liczbę urządzeń podlegających Serwerowi administracyjnemu.

Poniższa tabela zawiera listę prawidłowych opcji DBMS, a także zalecenia i ograniczenia dotyczące ich używania.

Zalecenia i ograniczenia dotyczące DBMS

DBMS	Zalecenia i ograniczenia
SQL Server Express Edition 2016 lub nowszy	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 10 000 urządzeń. Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasady Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach. Można ograniczyć maksymalną liczbę zdarzeń w repozytorium zdarzeń, aby zapobiec przepełnieniu bazy danych. Szczegółowe informacje można znaleźć w następującym temacie: Obliczanie miejsca na bazę danych. Jednoczesne korzystanie z systemu DBMS serwera SQL Server Express Edition przez Serwer administracyjny i inną aplikację jest surowo zabronione. Baza danych Microsoft SQL Express nie jest obsługiwana dla zadania **Wykonaj synchronizację Windows Update**.
Lokalny serwer SQL Server inny niż Express, 2016 lub nowszy	Brak ograniczeń.
Zdalny serwer SQL Server inny niż Express, 2016 lub nowszy	Ważne tylko wtedy, gdy oba urządzenia są w tej samej domenie Windows®; jeśli domeny są inne, należy nawiązać między nimi obustronną relację zaufania.
Lokalny lub zdalny MySQL 5.5, 5.6 lub 5.7 (MySQL w wersjach 5.5.1, 5.5.2, 5.5.3, 5.5.4 i 5.5.5 nie jest już obsługiwany)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 10 000 urządzeń. Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasady Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach. Szczegółowe informacje można znaleźć w następującym temacie: Obliczanie miejsca na bazę danych.
Lokalny lub zdalny MySQL 8.0.20 lub nowszy	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 50 000 urządzeń. Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasady Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach. Szczegółowe informacje można znaleźć w następującym temacie: Obliczanie miejsca na bazę danych.

DBMS	Zalecenia i ograniczenia
Lokalny lub zdalny MariaDB (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 20 000 urządzeń. Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasady Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach. Szczegółowe informacje można znaleźć w następującym temacie: Obliczanie miejsca na bazę danych.
PostgreSQL, Postgres Pro (zobacz obsługiwane wersje)	Użyj jednego z tych DBMS, jeśli zamierzasz uruchomić jeden Serwer administracyjny dla mniej niż 50 000 urządzeń. Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasady Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach. Szczegółowe informacje można znaleźć w następującym temacie: Obliczanie miejsca na bazę danych.

Jeśli wybierzesz MSSQL 2019, musisz użyć zbiorczej poprawki CU12 lub nowszej. Pozwoli to uniknąć błędów i przeciążenia systemu, które mogą wystąpić.

Stosowanie zbiorczej poprawki CU12 podczas używania SQL Server 2019 jako systemu DBMS

Jeśli używasz SQL Server 2019 jako systemu DBMS i nie masz zbiorczej poprawki CU12 lub nowszej, aby uniknąć błędów, takich jak „Brak wystarczającej ilości pamięci systemowej w puli zasobów 'internal', aby uruchomić to zapytanie".

Po zainstalowaniu Kaspersky Security Center wykonaj następujące kroki:

1. Nawiąż połączenie z SQL Server przy użyciu SQL Management Studio.
2. Uruchom następujące polecenia (jeśli wybrałeś inną nazwę dla bazy danych, użyj nazwy zamiast KAV):

```
USE KAV
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. Uruchom ponownie usługę SQL Server 2019.

Konfigurowanie serwera MariaDB x64 do pracy z Kaspersky Security Center 15.1

Aby pomyślnie skonfigurować serwer MariaDB x64 do pracy z Kaspersky Security Center, należy użyć domyślnych parametrów serwera, z wyjątkiem parametrów serwera określonych w tym artykule.

Kaspersky Security Center 15.1 obsługuje MariaDB DBMS. Aby uzyskać więcej informacji na temat obsługiwanych wersji MariaDB, zobacz sekcję Wymagania sprzętowe i programowe.

Jeśli używasz MariaDB DBMS dla Kaspersky Security Center, włącz obsługę InnoDB i pamięci MEMORY oraz kodowania UTF-8 i UCS-2.

Zalecane ustawienia dla pliku my.ini

W celu skonfigurowania pliku my.ini:

1. Otwórz plik my.ini w dowolnym edytorze tekstu.

2. Dodaj następujące wiersze do sekcji `[mysqld]` pliku my.ini:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< rzeczywista wartość nie może być niższa niż 80%
oczekiwanego rozmiaru bazy danych KAV >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

   Wartość `innodb_buffer_pool_size` nie może być mniejsza niż 80 procent oczekiwanego rozmiaru bazy danych KAV. Należy pamiętać, że określona pamięć jest przydzielana podczas uruchamiania serwera. Jeśli rozmiar bazy danych jest mniejszy niż określony rozmiar bufora, przydzielana jest tylko wymagana pamięć. Jeśli używasz MariaDB w wersji 10.4.3 lub starszej, rzeczywisty rozmiar przydzielonej pamięci jest o około 10 procent większy niż określony rozmiar bufora.

   Zalecane jest użycie wartości parametru `innodb_flush_log_at_trx_commit=0`, ponieważ wartości „1” lub „2” negatywnie wpływają na prędkość działania MariaDB. Upewnij się, że parametr `innodb_file_per_table` jest ustawiony na `1`.

   W przypadku MariaDB 10.1 dodatkowo wprowadź następujące wiersze w sekcji [mysqld]:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

   W przypadku MariaDB 10.6 dodatkowo wprowadź następujące wiersze w sekcji [mysqld]:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

Domyślnie dodatki optymalizujące `join_cache_incremental`, `join_cache_hashed` i `join_cache_bka` są włączone. Jeśli te dodatki nie są włączone, musisz je włączyć.

W celu sprawdzenia, czy dodatki optymalizujące są włączone:

1. W konsoli klienta MariaDB wykonaj polecenie:

```
SELECT @@optimizer_switch;
```

2. Sprawdź, czy jego dane wyjściowe zawierają następujące wiersze:

```
join_cache_incremental=on
join_cache_hashed=on
join_cache_bka=on
```

Jeśli te wiersze są obecne i mają wartość `on`, to dodatki optymalizujące są włączone.

Jeśli tych wierszy brakuje lub mają one wartość `off`, wykonaj następujące czynności:

1. Otwórz plik my.ini w dowolnym edytorze tekstu.

2. Dodaj następujące wiersze do sekcji `[mysqld]` pliku my.ini:

```
optimizer_switch='join_cache_incremental=on'
optimizer_switch='join_cache_hashed=on'
optimizer_switch='join_cache_bka=on'
```

Dodatki `join_cache_incremental`, `join_cache_hash` i `join_cache_bka` są włączone.

Konfigurowanie serwera MySQL x64 do pracy z Kaspersky Security Center 15.1

Aby pomyślnie skonfigurować serwer MySQL x64 do pracy z Kaspersky Security Center, należy użyć domyślnych parametrów serwera, z wyjątkiem parametrów serwera określonych w tym artykule.

Jeśli używasz MySQL DBMS dla Kaspersky Security Center, włącz obsługę InnoDB i pamięci MEMORY oraz kodowania UTF-8 i UCS-2.

Zalecane ustawienia dla pliku my.ini

W celu skonfigurowania pliku my.ini:

1. Otwórz plik my.ini w dowolnym edytorze tekstu.

2. Dodaj następujące wiersze do sekcji `[mysqld]` pliku my.ini:

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=< rzeczywista wartość nie może być niższa niż 80%
oczekiwanego rozmiaru bazy danych KAV >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (w większości przypadków, serwer używa niewielkich
transakcji)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Należy pamiętać, że określona w wartości `innodb_buffer_pool_size` pamięć jest przydzielana podczas uruchamiania serwera. Jeśli rozmiar bazy danych jest mniejszy niż określony rozmiar bufora, przydzielana jest tylko wymagana pamięć. Rzeczywisty rozmiar przydzielonej pamięci jest o około 10 procent większy niż określony rozmiar bufora. Więcej informacji można znaleźć w dokumentacji MySQL.

Zalecane jest użycie wartości parametru `innodb_flush_log_at_trx_commit = 0`, ponieważ wartości „1” lub „2” negatywnie wpływają na prędkość działania MySQL. Upewnij się, że parametr `innodb_file_per_table` jest ustawiony na `1`.

Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center 15.1

Aby pomyślnie skonfigurować serwer PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center, należy użyć domyślnych parametrów serwera, z wyjątkiem parametrów serwera określonych w tym artykule.

Kaspersky Security Center 15.1 obsługuje DBMS PostgreSQL i Postgres Pro. Jeśli używasz jednego z tych systemów DBMS, rozważ skonfigurowanie parametrów serwera DBMS w celu optymalizacji pracy DBMS z Kaspersky Security Center.

Domyślna ścieżka do pliku konfiguracyjnego to: `C:\Program Files\PostgreSQL\<WERSJA>\data\postgresql.conf`

Zalecane parametry w przypadku PostgreSQL i Postgres Pro:

- `max_connections = 151`
- `shared_buffers = N`

  N = 25 procent wartości pamięci RAM urządzenia, na którym jest zainstalowany DBMS Jeśli pamięć RAM to mniej niż 1 GB, pozostaw wartość domyślną.
- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `maintenance_work_mem = 128MB`
- `max_stack_depth = 2MB`
- `max_parallel_workers_per_gather = 0`
- `standard_conforming_strings = on`

Jeśli używasz Postgres Pro 15.7 lub Postgres Pro 15.7.1, wyłącz parametr `enable_compound_index_stats`:

`enable_compound_index_stats = off`

Po zaktualizowaniu pliku konfiguracyjnego ponownie załaduj konfigurację lub uruchom ponownie serwer DBMS.

Aby uzyskać szczegółowe informacje na temat parametrów serwerów PostgreSQL i Postgres Pro oraz sposobu określania parametrów, zapoznaj się z odpowiednią dokumentacją DBMS.

Zapoznaj się z następującym tematem, aby uzyskać szczegółowe informacje na temat tworzenia i konfigurowania kont dla PostgreSQL i Postgres Pro: Konfigurowanie kont do pracy z PostgreSQL i Postgres Pro.

Obsługa klastra o wysokiej dostępności

Klastry PostgreSQL o wysokiej dostępności są obsługiwane przy następujących ustawieniach:

- Typ replikacji: synchroniczny
- Minimalna liczba węzłów: 3
- Maksymalna liczba węzłów: 15

Aby skorzystać z tej funkcji, uruchom następujące polecenie, aby włączyć flagę KLCS_FF_SUPPORT_POSTGRES_FAIILOVER:

```
sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv ".core/.independent" -s klcsff -n
KLCS_FF_SUPPORT_POSTGRES_FAIILOVER -t d -v 1
```

Rola Postgres używana przez Serwer do uzyskiwania dostępu do DBMS musi mieć uprawnienia do odczytu następujących widoków (domyślnie włączone):

- pg_stat_replication
- pg_stat_wal_receiver

Zarządzanie urządzeniami mobilnymi z zainstalowanym programem Kaspersky Endpoint Security for Android

Urządzenia mobilne z zainstalowanym programem Kaspersky Endpoint Security for Android™ (zwane dalej "urządzenia KES") są zarządzane przy użyciu Serwera administracyjnego. Kaspersky Security Center obsługuje następujące funkcje zarządzania urządzeniami KES:

- Zarządzanie urządzeniami mobilnymi jak urządzeniami klienckimi:
  - Członkostwo w grupach administracyjnych
  - Monitorowanie, takie jak przeglądanie stanów, zdarzeń i raportów
  - Modyfikowanie ustawień lokalnych i przydzielanie zasad dla Kaspersky Endpoint Security for Android
- Wysyłanie poleceń w sposób scentralizowany
- Zdalne instalowanie pakietów aplikacji mobilnych

Serwer administracyjny zarządza urządzeniami KES przez TLS, port TCP 13292.

Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet

Wykonanie następujących czynności wymaga dostępu do Serwera administracyjnego przez Internet:

- Regularne aktualizowanie baz danych, modułów oprogramowania i aplikacji Kaspersky
- Aktualizowanie oprogramowania firm trzecich

Domyślnie połączenie internetowe w przypadku Serwera administracyjnego nie jest wymagane w celu instalowania aktualizacji oprogramowania firmy Microsoft na zarządzanych urządzeniach. Na przykład zarządzane urządzenia mogą pobierać aktualizacje oprogramowania firmy Microsoft bezpośrednio z serwerów Microsoft Update lub z systemu Windows Server z programem Microsoft Windows Server Update Services (WSUS) wdrożonymi w sieci organizacji. Serwer administracyjny musi być połączony z Internetem w następujących przypadkach:

  - Używanie Serwera administracyjnego jako serwera WSUS
  - Instalowanie aktualizacji oprogramowania firm trzecich innego niż oprogramowanie firmy Microsoft

- Eliminowanie luk w oprogramowaniu innych firm

  Połączenie internetowe w przypadku Serwera administracyjnego jest wymagane, aby można było wykonywać następujące zadania:

  - Sporządzanie listy zalecanych poprawek dla luk w oprogramowaniu firmy Microsoft. Lista jest tworzona i regularnie aktualizowana przez specjalistów z Kaspersky.
  - Naprawianie luk w oprogramowaniu firm trzecich innym niż oprogramowanie firmy Microsoft.

- Zarządzanie urządzeniami (laptopami) użytkowników mobilnych
- Zarządzanie urządzeniami w zdalnych biurach
- Komunikowanie się z głównym lub podrzędnym Serwerem administracyjnym w zdalnych biurach
- Zarządzanie urządzeniami mobilnymi

Ta sekcja opisuje podstawowe sposoby zapewnienia dostępu do Serwera administracyjnego poprzez Internet. W każdym przypadku skupiającym się na zapewnieniu Serwerowi administracyjnemu dostępu do Internetu może być wymagany dedykowany certyfikat dla Serwera administracyjnego.

Dostęp do internetu: Serwer administracyjny w sieci lokalnej

Jeśli Serwer administracyjny znajduje się w wewnętrznej sieci organizacji, możesz udostępnić port TCP o numerze 13000 Serwera administracyjnego z zewnątrz za pomocą przekierowania portów. Jeśli wymagane jest zarządzanie urządzeniami mobilnymi, możesz udostępnić port 13292 TCP.

Dostęp do internetu: Serwer administracyjny w strefie DMZ

Jeśli Serwer administracyjny znajduje się w DMZ sieci organizacji, nie ma on dostępu do wewnętrznej sieci organizacji. Dlatego też występują następujące ograniczenia:

- Serwer administracyjny nie może wykryć nowych urządzeń.
- Serwer administracyjny nie może wykonać wstępnego wdrożenia Agenta sieciowego przy użyciu wymuszonej instalacji na urządzeniach w wewnętrznej sieci organizacji.

Dotyczy to tylko wstępnej instalacji Agenta sieciowego. Jednakże jakiekolwiek późniejsze uaktualnienia Agenta sieciowego lub instalacja aplikacji zabezpieczającej mogą zostać wykonane przez Serwer administracyjny. Jednocześnie, wstępna instalacja Agentów sieciowych może odbyć się, na przykład, poprzez zasady grupy Microsoft® Active Directory®.

- Serwer administracyjny nie może wysyłać powiadomień na zarządzane urządzenia poprzez port UDP o numerze 15000, co nie jest krytyczne dla działania Kaspersky Security Center.

- Serwer administracyjny nie może przeszukiwać Active Directory. Jednakże w większości scenariuszy wyniki przeszukiwania Active Directory nie są wymagane.

Jeśli powyższe ograniczenia są postrzegane jako krytyczne, można je znieść przy pomocy punktów dystrybucji znajdujących się w sieci organizacji:

- Aby przeprowadzić wstępne wdrożenie na urządzeniach bez Agenta sieciowego, w pierwszej kolejności zainstaluj Agenta sieciowego na jednym z urządzeń, a następnie przypisz mu stan punktu dystrybucji. W rezultacie, wstępna instalacja Agenta sieciowego na pozostałych urządzeniach zostanie przeprowadzona przez Serwer administracyjny poprzez ten punkt dystrybucji.

- Aby wykrywać nowe urządzenia w wewnętrznej sieci organizacji i przeszukiwać Active Directory, w jednym z punktów dystrybucji musisz włączyć odpowiednie metody wykrywania urządzeń.

Aby zapewnić pomyślne wysyłanie powiadomień przez port UDP o numerze 15000 na zarządzane urządzenia znajdujące się w wewnętrznej sieci organizacji, musisz wypełnić całą swoją sieć punktami dystrybucji. We właściwościach przypisanych punktów dystrybucji zaznacz pole **Nie odłączaj od Serwera administracyjnego**. Serwer administracyjny nawiąże stale połączenie z punktami dystrybucji, które będą mogły wysyłać powiadomienia poprzez port UDP o numerze 15000 na urządzenia, które znajdują się w wewnętrznej sieci organizacji (to może być.sieć IPv4 lub IPv6).

Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej

Serwer administracyjny może znajdować się w wewnętrznej sieci organizacji, w strefie zdemilitaryzowanej (DMZ), gdzie może być urządzenie z Agentem sieciowym działającym jako brama połączenia z odwróconym połączeniem (Serwer administracyjny nawiązuje połączenie z Agentem sieciowym). W tym przypadku, w celu zapewnienia dostępu do Internetu muszą zostać spełnione następujące warunki:

- Agent sieciowy musi być zainstalowany na urządzeniu, które znajduje się w DMZ. Jeśli instalujesz Agenta sieciowego, w oknie **Brama połączenia** kreatora instalacji wybierz **Użyj Agenta sieciowego jako bramy połączenia w DMZ**.

- Urządzenie z zainstalowaną bramą połączenia musi zostać dodane do punktu dystrybucji. Po dodaniu bramy połączeniu, w oknie **Dodaj punkt dystrybucji** wybierz opcję **Wybierz → Dodaj bramę połączenia w DMZ na podstawie adresu**.

- Aby używać połączenia internetowego do podłączania zewnętrznych urządzeń stacjonarnych z Serwerem administracyjnym, należy poprawić pakiet instalacyjny Agenta sieciowego. We właściwościach utworzonego pakietu instalacyjnego wybierz opcję **Zaawansowane → Połącz z Serwerem administracyjnym korzystając z bramy połączenia**, a następnie określ nowo utworzoną bramę połączenia.

Dla bramy połączenia w strefie DMZ Serwer administracyjny tworzy certyfikat podpisany przez certyfikat Serwera administracyjnego. Jeśli administrator zdecyduje przydzielić Serwerowi administracyjnemu certyfikat niestandardowy, musi to zrobić przed utworzeniem bramy połączenia w strefie DMZ.

Jeśli niektórzy pracownicy korzystają z laptopów, które mogą łączyć się z Serwerem administracyjnym z sieci lokalnej lub poprzez Internet, przydatne będzie utworzenie w zasadzie Agenta sieciowego reguły przełączania dla Agenta sieciowego.

Informacje o punktach dystrybucji

Urządzenie z zainstalowanym Agentem sieciowym może być używane jako punkt dystrybucji. W tym trybie Agent sieciowy może wykonywać następujące funkcje:

- Rozsyłać uaktualnienia (mogą być one pobierane z Serwera administracyjnego lub z serwerów Kaspersky). W drugim przypadku należy utworzyć zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji* dla urządzenia pełniącego rolę punktu dystrybucji:
    - Instalować oprogramowanie (włączając w to wstępną instalację Agentów sieciowych) na pozostałych urządzeniach.
    - Przeszukiwać sieć w celu odnalezienia nowych urządzeń i zaktualizowania informacji o tych istniejących. Punkt dystrybucji może stosować te same metody wykrywania urządzeń co Serwer administracyjny.

Wdrożenie punktów dystrybucji w sieci organizacji realizuje następujące cele:

- Zmniejszanie obciążenia na Serwerze administracyjnym.
- Optymalizowanie ruchu sieciowego.
- Zapewnienie Serwerowi administracyjnemu dostępu do urządzeń w ciężko dostępnych miejscach sieci organizacji. Dostępność punktu dystrybucji w sieci poza NAT (w powiązaniu z Serwerem administracyjnym) umożliwia Serwerowi administracyjnemu wykonywanie następujących działań:
    - Wysyłanie powiadomień do urządzeń przez UDP w sieci IPv4 lub IPv6
    - Przeszukiwanie sieci IPv4 lub IPv6
    - Przeprowadzanie wstępnego wdrożenia
    - Pełnienie funkcji serwera push

Punkt dystrybucji jest przydzielony do grupy administracyjnej. W tym przypadku zakres działania punktu dystrybucji obejmuje wszystkie urządzenia w grupie administracyjnej i jej podgrupach. Jednakże urządzenie pełniące funkcję punktu dystrybucji może nie znajdować się w grupie administracyjnej, do której zostało przydzielone.

Możesz sprawić, że punkt dystrybucji będzie działał jako brama połączenia. W tym przypadku urządzenia objęte zakresem działania punktu dystrybucji będą łączyły się z Serwerem administracyjnym poprzez bramę, a nie bezpośrednio. Ten tryb może być przydatny w scenariuszach, które nie zezwalają na nawiązywanie bezpośredniego połączenia między Serwerem administracyjnym a zarządzanymi urządzeniami.

Jeśli używasz urządzenia opartego na systemie Linux jako punktu dystrybucji, zdecydowanie zalecamy zwiększenie limitu deskryptorów plików dla usługi klnagent, ponieważ jeśli zakres punktu dystrybucji obejmuje wiele urządzeń, domyślna maksymalna liczba plików, które można otworzyć, może być niewystarczająca.

Zwiększenie limitu deskryptorów plików dla usługi klnagent

Jeśli zakres punktu dystrybucji opartego na systemie Linux obejmuje wiele urządzeń, domyślny limit plików, które można otworzyć (deskryptory plików) może nie być wystarczający. Aby tego uniknąć, możesz zwiększyć limit deskryptorów plików dla usługi klnagent.

Aby zwiększyć limit deskryptorów plików dla usługi klnagent:

1. Na urządzeniu opartym na systemie Linux, które działa jako punkt dystrybucji, wykonaj następujące polecenie:

   ```
   systemctl edit klnagent64.service
   ```

2. Określ miękkie i twarde limity deskryptorów plików w parametrze `LimitNOFILE` w sekcji `[Service]`:

   ```
   LimitNOFILE=<miękki limit zasobów>:<twardy limit zasobów>
   ```

   Na przykład, `LimitNOFILE=32768:131072`. Należy pamiętać, że miękki limit deskryptorów plików musi być mniejszy lub równy twardemu limitowi.

3. Uruchom następujące polecenie, aby upewnić się, że parametry zostały określone poprawnie:

   ```
   systemd-analyze verify klnagent64.service
   ```

   Jeśli parametry zostaną określone niepoprawnie, to polecenie może wyświetlić jeden z następujących błędów:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Jeśli wystąpi ten błąd, oznacza to, że symbole w wierszu `LimitNOFILE` zostały określone niepoprawnie. Należy sprawdzić i poprawić wprowadzony wiersz.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Jeśli wystąpi ten błąd, miękki limit wprowadzonych deskryptorów plików jest większy niż twardy limit. Musisz sprawdzić wprowadzony wiersz i upewnić się, że miękki limit deskryptorów plików jest mniejszy lub równy twardemu limitowi.

4. Uruchom następujące polecenie, aby ponownie załadować proces systemowy:

   ```
   systemctl daemon-reload
   ```

5. Uruchom następujące polecenie, aby ponownie uruchomić usługę Agenta sieciowego:

   ```
   systemctl restart klnagent
   ```

6. Uruchom następujące polecenie, aby upewnić się, że określone parametry zostały zastosowane poprawnie:

   ```
   less /proc/<ID procesu nagent>/limits
   ```

   gdzie parametr `<ID procesu nagent>` jest identyfikatorem procesu Agenta sieciowego. Aby uzyskać identyfikator, możesz uruchomić następujące polecenie:

   ```
   ps -ax | grep klnagent
   ```

W przypadku punktu dystrybucji opartego na systemie Linux zwiększa się limit plików, które można otworzyć.

Obliczanie liczby i konfigurowanie punktów dystrybucji

Im więcej urządzeń klienckich zawiera sieć, tym więcej punktów dystrybucji wymaga. Nie jest zalecane wyłączanie automatycznego przypisywania punktów dystrybucji. Jeśli automatyczne przypisywanie punktów dystrybucji jest włączone, Serwer administracyjny przypisuje punkty dystrybucji, gdy liczba urządzeń klienckich jest dosyć duża, oraz definiuje ich konfigurację.

Używanie specjalnie przypisanych punktów dystrybucji

Jeśli planujesz używać określonych urządzeń jako punktów dystrybucji (na przykład, specjalnie wybranych serwerów), możesz zrezygnować z automatycznego przypisywania punktów dystrybucji. W tym przypadku upewnij się, że na urządzeniach, które mają pełnić rolę punktów dystrybucji, jest wystarczająca ilość wolnego miejsca, nie są regularnie wyłączane, a tryb uśpienia jest na nich wyłączony.

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)
10–100	1
Więcej niż 100	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Korzystanie ze standardowych urządzeń klienckich (stacji roboczych) jako punktów dystrybucji

Jeśli planujesz używać standardowych urządzeń klienckich (czyli stacji roboczych) jako punktów dystrybucji, zalecane jest przypisanie punktów dystrybucji w sposób pokazany w tabelach poniżej, aby uniknąć nadmiernego obciążenia kanałów komunikacji i Serwera administracyjnego:

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)
10–30	1
31–300	2
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Jeśli punkt dystrybucji jest wyłączony (lub z jakiegoś powodu niedostępny), zarządzane urządzenia w tym obszarze mogą uzyskać dostęp do Serwera administracyjnego w celu pobrania uaktualnień.

Hierarchia Serwerów administracyjnych

W MSP może działać kilka Serwerów administracyjnych. Niewygodne może być zarządzanie kilkoma oddzielnymi Serwerami administracyjnymi, dlatego dobrym wyjściem jest utworzenie hierarchii. Zastosowanie konfiguracji „główny/podrzędny" dla dwóch Serwerów administracyjnych oferuje następujące możliwości:

- Podrzędny Serwer administracyjny dziedziczy zasady i zadania od głównego Serwera administracyjnego, zapobiegając dzięki temu powielaniu ustawień.
- Wybory urządzeń na głównym Serwerze administracyjnym mogą zawierać urządzenia z podrzędnych Serwerów administracyjnych.
- Raporty na głównym Serwerze administracyjnym mogą zawierać dane (w tym szczegółowe informacje) z podrzędnych Serwerów administracyjnych.

W zakresie wyżej wymienionych opcji główny Serwer administracyjny odbiera dane tylko z niewirtualnych podrzędnych Serwerów administracyjnych. To ograniczenie nie dotyczy wirtualnych Serwerów administracyjnych, które współdzielą bazę danych ze swoim głównym Serwerem administracyjnym.

Wirtualne Serwery administracyjne

W oparciu o fizyczny Serwer administracyjny można utworzyć kilka wirtualnych Serwerów administracyjnych, które będą podobne do podrzędnych Serwerów administracyjnych. W przeciwieństwie do trybu poufnego dostępu, który jest oparty na listach kontroli dostępu (ACL), tryb wirtualnego Serwera administracyjnego jest bardziej funkcjonalny i zapewnia większy stopień izolacji. Jako dodatek do dedykowanej struktury grup administracyjnych dla przypisanych urządzeń z zasadami i zadaniami, każdy wirtualny Serwer administracyjny zawiera swoją grupę nieprzypisanych urządzeń, własne zestawy raportów, wybranych urządzeń i zdarzeń, pakietów instalacyjnych, reguł przenoszenia itd. Zasięg działania wirtualnego Serwera administracyjnego może być wykorzystany przez dostawców usług (xSP) do zwiększenia izolacji klientów, a także przez organizacje działające na szeroką skalę z zaawansowanym przepływem pracy i dużą liczbą administratorów.

Wirtualne Serwery administracyjne są bardzo podobne do podrzędnych Serwerów administracyjnych, jednakże posiadają pewne różnice:

- Wirtualny Serwer administracyjny nie posiada większości ustawień globalnych i swoich własnych portów TCP.
- Wirtualny Serwer administracyjny nie posiada podrzędnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny nie posiada innych wirtualnych Serwerów administracyjnych.
- Fizyczny Serwer administracyjny wyświetla urządzenia, grupy, zdarzenia i obiekty na zarządzanych urządzeniach (elementy w Kwarantannie, rejestrze aplikacji itd.) ze wszystkich swoich wirtualnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny może skanować sieć wyłącznie przy podłączonych punktach dystrybucji.

Informacje o ograniczeniach Kaspersky Security Center

Poniższa tabela wyświetla ograniczenia bieżącej wersji Kaspersky Security Center.

Rodzaj ograniczenia	Wartość
Maksymalna liczba zarządzanych urządzeń na Serwer administracyjny	100 000
Maksymalna liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego**	300
Maksymalna liczba grup administracyjnych	10 000
Maksymalna liczba przechowywanych zdarzeń	45 000 000
Maksymalna liczba zasad	2000
Maksymalna liczba zadań	2000
Maksymalna całkowita liczba obiektów Active Directory (jednostek organizacyjnych i kont użytkowników, urządzeń oraz grup bezpieczeństwa)	1 000 000
Maksymalna liczba profili w zasadzie	100
Maksymalna liczba podrzędnych Serwerów administracyjnych w jednym głownym Serwerze administracyjnym	500
Maksymalna liczba wirtualnych Serwerów administracyjnych	500
Maksymalna liczba urządzeń, jaką obejmuje pojedynczy punkt dystrybucji (punkty dystrybucji mogą obejmować tylko urządzenia niemobilne)	10 000
Maksymalna liczba urządzeń, które mogą używać pojedynczej bramy połączenia	10 000, w tym urządzenia mobilne
Maksymalna liczba urządzeń mobilnych na Serwer administracyjny	100 000 minus liczba stacjonarnych zarządzanych urządzeń

Obciążenie sieci

Ta sekcja zawiera informacje o ilości ruchu sieciowego wymienianego między urządzeniami klienckimi a Serwerem administracyjnym podczas wykonywania kluczowych działań administracyjnych.

Największe obciążenie sieci jest wywoływane przez realizację następujących scenariuszy administracyjnych:

- Wstępna zdalna instalacja ochrony antywirusowej
- Wstępna aktualizacja baz danych programu antywirusowego
- Synchronizacja urządzenia klienckiego z Serwerem administracyjnym
- Regularna aktualizacja antywirusowych baz danych
- Przetwarzanie zdarzeń występujących na urządzeniach klienckich przez Serwer administracyjny

Wstępna zdalna instalacja ochrony antywirusowej

Ta sekcja zawiera informacje o rozmiarze ruchu sieciowego po zainstalowaniu na urządzeniu klienckim Agenta sieciowego i programu Kaspersky Endpoint Security for Windows (zobacz poniższą tabelę).

Agent sieciowy jest instalowany przy użyciu instalacji wymuszonej, podczas której pliki potrzebne do przeprowadzenia instalacji są kopiowane z Serwera administracyjnego do folderu współdzielonego na urządzeniu klienckim. Po instalacji, Agent sieciowy pobiera pakiet dystrybucyjny Kaspersky Endpoint Security for Windows, korzystając z połączenia z Serwerem administracyjnym.

Scenariusz	Instalacja Agenta sieciowego na pojedynczym urządzeniu klienckim	Instalowanie Kaspersky Endpoint Security for Windows na jednym urządzeniu klienckim (z aktualizacją baz danych)	Równoległa instalacja Agenta sieciowego i Kaspersky Endpoint Security for Windows
Ruch sieciowy z urządzenia klienckiego do Serwera administracyjnego, KB	1638,4	7843,84	9707,52
Ruch sieciowy z Serwera administracyjnego do urządzenia klienckiego, KB	69 990,4	259 317,76	329 318,4
Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego), KB	71 628,8	267 161,6	339 025,92

Po zainstalowaniu Agentów sieciowych na urządzeniach klienckich, jedno z urządzeń należących do grupy administracyjnej może być wyznaczone do pełnienia roli punktu dystrybucji. Będzie ono używane do rozsyłania pakietów instalacyjnych. W tej sytuacji rozmiar ruchu sieciowego przesyłanego podczas wstępnej zdalnej instalacji ochrony antywirusowej będzie się znacznie różnił w zależności od tego, czy używana jest multiemisja IP.

Jeśli multiemisja IP jest używana, pakiety instalacyjne tylko raz zostają wysłane do wszystkich uruchomionych urządzeń należących do grupy administracyjnej. Z tego powodu całkowity ruch sieciowy będzie N razy mniejszy, gdzie N oznacza całkowitą liczbę uruchomionych urządzeń należących do grupy administracyjnej. W przypadku, gdy funkcja multiemisji IP nie jest używana, całkowity ruch sieciowy jest podobny do ruchu sieciowego podczas pobierania pakietów dystrybucyjnych z Serwera administracyjnego. Jednakże źródłem pakietu będzie punkt dystrybucji, a nie Serwer administracyjny.

Wstępna aktualizacja baz danych programu antywirusowego

Ilość ruchu sieciowego podczas początkowej aktualizacji antywirusowych baz danych (podczas pierwszego uruchomienia zadania aktualizacji baz danych na urządzeniu klienckim) jest następująca:

- Ruch sieciowy z urządzenia klienckiego do Serwera administracyjnego: 1,8 MB.
- Ruch sieciowy z Serwera administracyjnego do urządzenia klienckiego: 113 MB.
- Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego): 114 MB.

Dane mogą się nieznacznie różnić w zależności od bieżącej wersji antywirusowych baz danych.

Synchronizowanie klienta z Serwerem administracyjnym

Scenariusz ten opisuje stan systemu administracyjnego w sytuacji, gdy zachodzi intensywna synchronizacja danych pomiędzy urządzeniem klienckim a Serwerem administracyjnym. Urządzenia klienckie nawiązują połączenie z Serwerem administracyjnym w przedziale czasowym określonym przez administratora. Serwer administracyjny porównuje stan danych na urządzeniu klienckim ze stanem danych na Serwerze, zapisuje w bazie danych informacje o ostatnim połączeniu urządzenia klienckiego i przeprowadza synchronizację danych.

Ta sekcja zawiera informacje o rozmiarach ruchu dla podstawowych scenariuszy administracyjnych przy łączeniu klienta z Serwerem administracyjnym (zobacz poniższą tabelę). Dane znajdujące się w tabeli mogą się nieznacznie różnić w zależności od bieżącej wersji antywirusowych baz danych.

Ruch sieciowy

Scenariusz	Ruch sieciowy z urządzeń klienckich do Serwera administracyjnego, KB	Ruch sieciowy z Serwera administracyjnego do urządzeń klienckich, KB	Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego), KB
Wstępna synchronizacja przed aktualizacją baz danych na urządzeniu klienckim	699,44	568,42	1267,86

Wstępna synchronizacja po aktualizacji baz danych na urządzeniu klienckim	735,8	4474,88	5210,68
Synchronizacja bez zmian na urządzeniu klienckim i Serwerze administracyjnym	11,99	6,73	18,72
Synchronizacja po zmianie wartości ustawień w zasadzie grupy	9,79	11,39	21,18
Synchronizacja po zmianie wartości ustawień w zadaniu grupowym	11,27	11,72	22,99
Wymuszona synchronizacja bez zmian na urządzeniu klienckim	77,59	99,45	177,04

Całkowita ilość ruchu sieciowego może znacznie się wahać, w zależności od tego, czy w grupach administracyjnych wykorzystywana jest opcja multiemisji IP. Jeśli opcja ta jest używana, całkowity rozmiar ruchu sieciowego będzie o około N razy mniejszy dla grupy, gdzie N oznacza całkowitą liczbę urządzeń należących do grupy administracyjnej.

Ilość ruchu sieciowego przy wstępnej synchronizacji przed i po aktualizacji baz danych jest określona dla następujących przypadków:

- Instalowanie Agenta sieciowego i aplikacji zabezpieczającej na urządzeniu klienckim
- Przenoszenie urządzenia klienckiego do grupy administracyjnej
- Stosowanie do urządzenia klienckiego zasady i zadań domyślnie utworzonych dla grupy

Tabela określa szybkość ruchu sieciowego w przypadku zmian wprowadzonych w jednym z ustawień ochrony, które znajdują się w ustawieniach zasady Kaspersky Endpoint Security. Dane dla innych ustawień zasady mogą się różnić od danych wyświetlonych w tabeli.

Dodatkowa aktualizacja baz danych programu antywirusowego

Rozmiar ruchu sieciowego w przypadku inkrementacyjnych aktualizacji antywirusowych baz danych po 20 godzinach od poprzedniej aktualizacji wygląda następująco:

- Ruch sieciowy z urządzenia klienckiego do Serwera administracyjnego: 169 KB.
- Ruch sieciowy z Serwera administracyjnego do urządzenia klienckiego: 16 MB.
- Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego): 16.3 MB.

Dane znajdujące się w tabeli mogą się nieznacznie różnić w zależności od bieżącej wersji antywirusowych baz danych.

Ilość ruchu sieciowego może znacznie się wahać, w zależności od tego, czy w grupach administracyjnych wykorzystywana jest opcja multiemisji IP. Jeśli opcja ta jest używana, całkowity rozmiar ruchu sieciowego będzie o około N razy mniejszy dla grupy, gdzie N oznacza całkowitą liczbę urządzeń należących do grupy administracyjnej.

Przetwarzanie zdarzeń występujących na klientach przez Serwer administracyjny

Ta sekcja zawiera informacje o ilości ruchu sieciowego, gdy na urządzeniu klienckim wystąpi zdarzenie „Wykryto wirusa", które jest wysyłane do Serwera administracyjnego i jest rejestrowane w jego bazie danych (patrz tabela poniżej).

Scenariusz	Przesyłanie danych do Serwera administracyjnego po wystąpieniu zdarzenia „Wykryto wirusa”	Przesyłanie danych do Serwera administracyjnego po wystąpieniu dziewięciu zdarzeń „Wykryto wirusa”
Ruch sieciowy z urządzenia klienckiego do Serwera administracyjnego, KB	49,66	64,05
Ruch sieciowy z Serwera administracyjnego do urządzenia klienckiego, KB	28,64	31,97
Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego), KB	78,3	96,02

Dane znajdujące się w tabeli mogą się nieznacznie różnić w zależności od aktualnej wersji aplikacji antywirusowej oraz zdarzeń, które są zdefiniowane w jej zasadzie do rejestracji w bazie danych Serwera administracyjnego.

Ruch na 24 godziny

Ta sekcja zawiera informacje o rozmiarach ruchu dla 24 godzin aktywności systemu administracyjnego w warunkach „spokoju”, kiedy nie występuje modyfikacja danych na urządzeniach klienckich i na Serwerze administracyjnym (patrz tabela poniżej).

Dane wymienione w tabeli opisują stan sieci po standardowej instalacji Kaspersky Security Center i po zamknięciu kreatora wstępnej konfiguracji. Częstotliwość synchronizacji urządzenia klienckiego z Serwerem administracyjnym wynosiła 20 minut; uaktualnienia były pobierane do repozytorium Serwera administracyjnego co godzinę.

Ilość ruchu sieciowego na 24 godziny w stanie bezczynności

Przepływ ruchu	Wartość
Ruch sieciowy z urządzenia klienckiego do Serwera administracyjnego, KB	3235,84
Ruch sieciowy z Serwera administracyjnego do urządzenia klienckiego, KB	64 378,88
Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego), KB	67 614,72

Przygotowywanie do zarządzania urządzeniami mobilnymi

Ta sekcja zawiera następujące informacje:

- Informacje o serwerze iOS MDM, przeznaczonym do zarządzania urządzeniami iOS poprzez zainstalowanie na nich dedykowanych profili iOS MDM
- Informacje o zarządzaniu urządzeniami mobilnymi, na których jest zainstalowany Kaspersky Endpoint Security for Android

Serwer iOS MDM

Serwer iOS MDM umożliwia zarządzanie urządzeniami iOS poprzez zainstalowane na nich profile iOS MDM. Obsługiwane są następujące funkcje:

- Blokowanie urządzenia
- Resetowanie hasła
- Usuwanie danych

- Instalowanie i dezinstalowanie aplikacji
- Użycie profilu iOS MDM z ustawieniami zaawansowanymi (np. ustawienia VPN, ustawienia e-mail, ustawienia Wi-Fi, ustawienia aparatu, certyfikaty itd.)

Serwer iOS MDM jest usługą sieciową odbierającą połączenia przychodzące z urządzeń mobilnych poprzez swój protokół TLS (domyślne jest to port 443), która jest zarządzana poprzez Kaspersky Security Center przy użyciu Agenta sieciowego. Agent sieciowy jest instalowany lokalnie, na urządzeniu z zainstalowanym serwerem iOS MDM.

Podczas instalacji serwera iOS MDM administrator musi wykonać następujące czynności:

- Zapewnić Agentowi sieciowemu dostęp do Serwera administracyjnego
- Zapewnić urządzeniom mobilnym dostęp do portu TCP serwera iOS MDM

Ta sekcja przedstawia dwie standardowe konfiguracje serwera iOS MDM.

Standardowa konfiguracja: Kaspersky Device Management for iOS w strefie DMZ

Serwer iOS MDM znajduje się w strefie zdemilitaryzowanej (DMZ) sieci lokalnej organizacji z dostępem do Internetu. Specjalną funkcją tej konfiguracji jest brak jakichkolwiek problemów podczas uzyskiwania dostępu do usługi sieciowej iOS MDM z poziomu urządzeń przez Internet.

Ponieważ zarządzanie serwerem iOS MDM wymaga zainstalowania Agenta sieciowego lokalnie, należy zapewnić interakcję Agenta sieciowego z Serwerem administracyjnym. Można to zrobić przy użyciu jednej z następujących metod:

- Przenosząc Serwer administracyjny do strefy DMZ.
- Korzystając z bramy połączenia:

  a. Na urządzeniu z zainstalowanym serwerem iOS MDM połącz Agenta sieciowego z Serwerem administracyjnym poprzez bramę połączenia.

  b. Na urządzeniu z zainstalowanym serwerem iOS MDM wskaż Agenta sieciowego jako bramę połączenia.

Standardowa konfiguracja: Serwer iOS MDM w sieci lokalnej organizacji

Serwer iOS MDM znajduje się w wewnętrznej sieci organizacji. Port 443 (port domyślny) musi być włączony w celu umożliwienia dostępu zewnętrznego, na przykład poprzez opublikowanie usługi sieciowej iOS MDM na odwrotnym serwerze proxy, który obsługuje delegowanie protokołu Kerberos.

Każda standardowa konfiguracja wymaga dla serwera iOS MDM dostępu do usług sieciowych Apple (zakres 17.0.0.0/8) poprzez port TCP 2197. Ten port jest używany do informowania urządzeń o nowych poleceniach przy użyciu dedykowanej usługi o nazwie APNs.

Zarządzanie urządzeniami mobilnymi z zainstalowanym programem Kaspersky Endpoint Security for Android

Urządzenia mobilne z zainstalowanym programem Kaspersky Endpoint Security for Android™ (zwane dalej "urządzenia KES") są zarządzane przy użyciu Serwera administracyjnego. Kaspersky Security Center obsługuje następujące funkcje zarządzania urządzeniami KES:

- Zarządzanie urządzeniami mobilnymi jak urządzeniami klienckimi:
  - Członkostwo w grupach administracyjnych
  - Monitorowanie, takie jak przeglądanie stanów, zdarzeń i raportów
  - Modyfikowanie ustawień lokalnych i przydzielanie zasad dla Kaspersky Endpoint Security for Android
- Wysyłanie poleceń w sposób scentralizowany
- Zdalne instalowanie pakietów aplikacji mobilnych

Serwer administracyjny zarządza urządzeniami KES przez TLS, port TCP 13292.

Informacje o wydajności Serwera administracyjnego

Ta sekcja wyświetla wyniki testów wydajnościowych Serwera administracyjnego dla różnych konfiguracji sprzętowych, a także ograniczenia dotyczące połączenia zarządzanych urządzeń z Serwerem administracyjnym.

Ograniczenia połączenia z Serwerem administracyjnym

Serwer administracyjny obsługuje zarządzanie do 100 000 urządzeń bez straty na wydajności.

Ograniczenia połączeń z Serwerem administracyjnym bez straty na wydajności:

- Jeden Serwer administracyjny może obsługiwać maksymalnie 500 wirtualnych Serwerów administracyjnych.
- Główny Serwer administracyjny obsługuje nie więcej niż 1000 sesji jednocześnie.
- Wirtualne Serwery administracyjne obsługują nie więcej niż 1000 sesji jednocześnie.

Rezultaty testów wydajnościowych Serwera administracyjnego

Rezultaty testów wydajnościowych Serwera administracyjnego pozwoliły określić maksymalną liczbę urządzeń klienckich, z którymi Serwer administracyjny może się zsynchronizować w określonych przedziałach czasu. Informacje te mogą być wykorzystane do stworzenia optymalnego schematu wdrożenia ochrony antywirusowej w sieciach komputerowych.

Podczas testów użyte zostały następujące konfiguracje sprzętowe Serwera administracyjnego (patrz tabele poniżej):

Konfiguracja sprzętowa Serwera administracyjnego

Parametr	Wartość
Procesor	Intel Xeon CPU E5630, częstotliwość taktowania 2.53 GHz, 2 gniazda, 8 rdzeni, 16 procesorów logicznych
Pamięć RAM	26 GB
Dysk twardy	IBM ServeRAID M5014 SCSI Disk Device, 487 GB
System operacyjny	Microsoft Windows Server 2019 Standard, wersja 10.0.17763, kompilacja 17763
Sieć	QLogic BCM5709C Gigabit Ethernet (klient NDIS VBD)

Konfiguracja sprzętowa urządzenia z serwerem SQL

Parametr	Wartość
Procesor	Intel Xeon CPU X5570, częstotliwość taktowania 2.93 GHz, 2 gniazda, 8 rdzeni, 16 procesorów logicznych
Pamięć RAM	32 GB
Dysk twardy	Urządzenie dyskowe Adaptec Array SCSI, 2047 GB
System operacyjny	Microsoft Windows Server 2019 Standard, wersja 10.0.17763, kompilacja 17763
Sieć	Intel 82576 Gigabit

Serwer administracyjny obsługiwał tworzenie 500 wirtualnych Serwerów administracyjnych.

Okres synchronizacji wynosił 15 minut dla każdych 10 000 zarządzanych urządzeń (patrz tabela poniżej).

Ogólne rezultaty testów obciążeniowych Serwera administracyjnego

Okres synchronizacji (min)	Liczba zarządzanych urządzeń
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
90	60 000
105	70 000
120	80 000
135	90 000
150	100 000

Jeśli łączysz Serwer administracyjny z serwerem bazodanowym MySQL lub SQL Express, nie zaleca się zarządzać przy pomocy aplikacji liczbą urządzeń większą niż 10 000. W przypadku systemu zarządzania bazą danych MariaDB maksymalna zalecana liczba zarządzanych urządzeń to 20 000.

Wyniki sprawdzania działania serwera KSN proxy

Jeśli Twoja sieć firmowa zawiera dużą liczbę urządzeń klienckich i używają one Serwera administracyjnego jako serwera proxy KSN, sprzęt Serwera administracyjnego musi spełniać określone wymagania, aby możliwe było przetwarzanie żądań z urządzeń klienckich. Możesz wykorzystać wyniki testowania do oceny obciążenia Serwera administracyjnego w swojej sieci i rozplanować zasoby sprzętowe, aby zapewnić normalne funkcjonowanie usługi KSN proxy.

Tabele poniżej pokazują konfigurację sprzętową Serwera administracyjnego i serwera SQL. Ta konfiguracja została użyta do testowania.

Konfiguracja sprzętowa Serwera administracyjnego

Parametr	Wartość
Procesor	Intel Xeon CPU E5450, częstotliwość taktowania 3.00 GHz, 2 gniazda, 8 rdzeni, 16 procesorów logicznych
Pamięć RAM	32 GB
System operacyjny	Microsoft Windows Server 2016 Standard

Konfiguracja sprzętowa serwera SQL

Parametr	Wartość
Procesor	Intel Xeon CPU E5450, częstotliwość taktowania 3.00 GHz, 2 gniazda, 8 rdzeni, 16 procesorów logicznych
Pamięć RAM	32 GB
System operacyjny	Microsoft Windows Server 2019 Standard

Poniższa tabela wyświetla wyniki testu.

Wyniki podsumowujące testowanie działania serwera proxy KSN

Parametr	Wartość
Maksymalna liczba żądań przetworzonych na sekundę	4914
Maksymalne zużycie procesora	36%

Ustawienia sieciowe dotyczące interakcji z usługami zewnętrznymi

Kaspersky Security Center używa następujących ustawień sieciowych do interakcji z usługami zewnętrznymi.

Ustawienia sieci	Adres	Opis
Port: 443 Protokół: HTTPS	activation-v2.kaspersky.com	Aktywacja aplikacji.
Port: 443 Protokół: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Aktualizowanie baz danych, modułów i aplikacji Kaspersky.
Port: 443 Protokół: HTTPS	https://downloads.upd.kaspersky.com	• Aktualizowanie baz danych, modułów i aplikacji Kaspersky. • Sprawdzanie, czy serwery Kaspersky są dostępne. Przed pobraniem baz danych i modułów oprogramowania Kaspersky oprogramowanie Kaspersky Security Center sprawdza, czy serwery Kaspersky są dostępne. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS.

Ustawienia sieci	Adres	Opis
Port: 80 Protokół: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Aktualizowanie baz danych, modułów i aplikacji Kaspersky.
Port: 443 Protokół: HTTPS	ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com	Używanie Kaspersky Security Network.
Port: 443, 1443 Protokół: HTTPS	ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Używanie Kaspersky Security Network.
Port: 443 Protokół: HTTPS	click.kaspersky.com redirect.kaspersky.com	Klikanie odnośników z poziomu interfejsu.

Ustawienia sieci	Adres	Opis
Port: 80 Protokół: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Serwery te stanowią część infrastruktury klucza publicznego (PKI) i są niezbędne do weryfikacji statusu ważności certyfikatów podpisu cyfrowego Kaspersky. Lista CRL to lista unieważnionych certyfikatów. OCSP umożliwia sprawdzenie statusu konkretnego certyfikatu w czasie rzeczywistym. Serwery te pomagają zapewnić bezpieczeństwo interakcji z certyfikatami cyfrowymi i chronią przed możliwymi atakami.
Port: 443 Protokół: HTTPS	https://ipm-klca.kaspersky.com	Ogłoszenia marketingowe.

Aby zapewnić prawidłową współpracę Kaspersky Security Center z usługami zewnętrznymi, należy uwzględnić następujące zalecenia:
- Na urządzeniach sieciowych i serwerze proxy organizacji należy zezwolić na nieszyfrowany ruch sieciowy na portach 443 i 1443.
- Podczas interakcji Serwera administracyjnego z serwerami aktualizacji Kaspersky i serwerami Kaspersky Security Network należy zapobiegać przechwytywaniu ruchu sieciowego z podmianą certyfikatu (ataki MITM).

Aby pobrać aktualizacje poprzez protokół HTTP lub HTTPS za pomocą narzędzia klscflag:

1. Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Jeśli chcesz pobrać aktualizacje przez protokół HTTP, uruchom jedno z następujących poleceń:

   - Na urządzeniu z zainstalowanym Serwerem administracyjnym:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - W punkcie dystrybucji:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Jeśli chcesz pobrać aktualizacje za pośrednictwem protokołu HTTPS, uruchom jedno z następujących poleceń:

   - Na urządzeniu z zainstalowanym Serwerem administracyjnym:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - W punkcie dystrybucji:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Instalowanie Agenta sieciowego i aplikacji zabezpieczającej

Aby zarządzać urządzeniami w organizacji, na każdym z nich należy zainstalować Agenta sieciowego. Zdalna instalacja aplikacji Kaspersky Security Center na urządzeniach w firmie zazwyczaj rozpoczyna się od zainstalowania na nich Agenta sieciowego.

W systemie Microsoft Windows XP Agent sieciowy może nie wykonać poprawnie następujących działań: pobranie uaktualnień bezpośrednio z serwerów Kaspersky (jako punkt dystrybucji); działanie jako serwer proxy KSN (jako punkt dystrybucji); oraz wykrywanie luk firm trzecich (jeśli używane jest Zarządzanie lukami i poprawkami).

Wstępne wdrożenie

Aby zarządzać urządzeniami w organizacji, na każdym z nich należy zainstalować Agenta sieciowego.

Instalację Agenta sieciowego na zarządzanym urządzeniu z systemem Windows można przeprowadzić następującymi sposobami:

- Używając narzędzi firm trzecich do zdalnej instalacji aplikacji.
- Klonując obraz dysku twardego administratora z systemem operacyjnym i Agentem sieciowym, przy pomocy narzędzi do zarządzania obrazami dysku, dostępnych w Kaspersky Security Center, lub przy użyciu narzędzi firm trzecich.
- Korzystając z zasad grupy w systemie Windows, używając standardowych narzędzi do zarządzania systemu Windows dla zasad grupy lub w trybie automatycznym, poprzez odpowiednią, dedykowaną opcję w zadaniu zdalnej instalacji programu Kaspersky Security Center.
- W trybie wymuszonym, poprzez wykorzystanie zasobów systemu operacyjnego za pośrednictwem zadania zdalnej instalacji Kaspersky Security Center.
- Wysyłając do użytkowników urządzeń odnośniki do pakietów autonomicznych, wygenerowanych przez Kaspersky Security Center. Pakiety autonomiczne to moduły wykonywalne, które zawierają pakiety dystrybucyjne wybranych aplikacji wraz ze zdefiniowanymi ustawieniami.
- Ręcznie, poprzez uruchomienie instalatorów aplikacji na urządzeniach.

Pierwszą instalację Agenta sieciowego na zarządzanym urządzeniu z systemem Linux można przeprowadzić następującymi sposobami:

- Łącząc się z zarządzanym urządzeniem poprzez SSH i uruchamiając zadanie instalacji zdalnej.
- Uruchamiając instalację pakietu na zarządzanym urządzeniu.

Pierwszą instalację Agenta sieciowego na zarządzanym urządzeniu z systemem macOS można przeprowadzić następującymi sposobami:

- Uruchamiając zadanie instalacji zdalnej za pośrednictwem punktu dystrybucji systemu macOS.
- Wysyłając do użytkowników urządzeń odnośniki do pakietów autonomicznych, wygenerowanych przez Kaspersky Security Center. Pakiety autonomiczne to moduły wykonywalne, które zawierają pakiety dystrybucyjne wybranych aplikacji wraz z predefiniowanymi ustawieniami.

Po zainstalowaniu Agenta sieciowego na urządzeniu można wykonać zdalną instalację aplikacji Kaspersky na tym urządzeniu za pośrednictwem tego Agenta sieciowego. Pakiet dystrybucyjny aplikacji, która ma zostać zainstalowana, jest przesyłany za pośrednictwem kanałów komunikacji pomiędzy Agentami sieciowymi i Serwerem administracyjnym wraz z ustawieniami instalacji, zdefiniowanymi przez administratora. Aby przesłać pakiet dystrybucyjny, możesz użyć węzłów pośredniczących, na przykład, punktów dystrybucji, dostarczania multiemisyjnego itd.

Podczas wybierania metody i strategii wdrożenia aplikacji w zarządzanej sieci należy mieć na uwadze kilka czynników (częściowa lista):

- Konfigurację sieci organizacji.
- Całkowitą liczbę urządzeń.
- Obecność w sieci organizacji urządzeń, które nie należą do żadnej domeny Active Directory; oraz obecność jednakowych kont z uprawnieniami administratora na tych urządzeniach.
- Pojemność kanału pomiędzy Serwerem administracyjnym a urządzeniami.
- Rodzaj komunikacji pomiędzy Serwerem administracyjnym a zdalnymi podsieciami oraz pojemność kanałów sieciowych w tych podsieciach.
- Ustawienia zabezpieczeń zostaną zastosowane na urządzeniach zdalnych na początku wdrożenia. Parametry te umożliwiają nawiązanie zdalnego połączenia z zarządzanym urządzeniem i rozpoczęcie instalacji.

Konfigurowanie instalatorów

Przed uruchomieniem wdrożenia aplikacji Kaspersky w sieci, należy określić ustawienia instalacji (ustawienia definiowane podczas instalacji aplikacji). Podczas instalacji Agenta sieciowego należy określić przynajmniej adres połączenia z Serwerem administracyjnym; niektóre ustawienia zaawansowane też mogą być wymagane. W zależności od wybranej metody instalacji, ustawienia można zdefiniować w różny sposób. W najprostszym przypadku (ręczna instalacja interaktywna na wybranym urządzeniu) wszystkie odpowiednie ustawienia można skonfigurować z poziomu interfejsu instalatora.

Ta metoda definiowania ustawień jest nieodpowiednia w nieinteraktywnej („cichej") instalacji aplikacji w grupach urządzeń. Na ogół administrator musi określić wartości dla ustawień w sposób scentralizowany; te wartości mogą być następnie wykorzystane w instalacji cichej na wybranych urządzeniach w sieci.

Pakiety instalacyjne

Pierwsza i główna metoda definiowania ustawień instalacji aplikacji jest uniwersalna i tym samym jest odpowiednia dla wszystkich metod instalacji: przy użyciu narzędzi Kaspersky Security Center oraz większości narzędzi firm trzecich. Ta metoda obejmuje utworzenie pakietów instalacyjnych aplikacji w Kaspersky Security Center.

Pakiety instalacyjne są generowane przy użyciu następujących metod:

- Automatycznie, z określonych pakietów dystrybucyjnych, na podstawie załączonych *deskryptorów* (pliki z rozszerzeniem .kud, które zawierają reguły dla instalacji, wyniki analizy oraz inne informacje)
- Z plików wykonywalnych instalatorów lub z instalatorów w formacie natywnym (.msi, .deb, .rpm), dla aplikacji standardowych lub obsługiwanych

Wygenerowane pakiety instalacyjne są zorganizowane hierarchicznie jako foldery z podfolderami i plikami. Oprócz oryginalnego pakietu dystrybucyjnego, pakiet instalacyjny zawiera ustawienia dostępne do modyfikacji (w tym ustawienia instalatora oraz reguły przetwarzania dla takich sytuacji, jak konieczność ponownego uruchomienia systemu operacyjnego w celu zakończenia instalacji), a także drobne moduły pomocnicze.

Wartości ustawień instalacji, które są charakterystyczne dla pojedynczej obsługiwanej aplikacji, można zdefiniować w interfejsie Konsoli administracyjnej podczas tworzenia pakietu instalacyjnego. Podczas zdalnej instalacji aplikacji przy użyciu narzędzi Kaspersky Security Center pakiety instalacyjne są dostarczane na urządzenia, dzięki czemu uruchomienie instalatora aplikacji udostępni dla tej aplikacji wszystkie ustawienia zdefiniowane przez administratora. Jeśli do zainstalowania aplikacji firmy Kaspersky używasz narzędzi firm trzecich, musisz zapewnić dostępność całego pakietu instalacyjnego, czyli pakietu dystrybucyjnego i jego ustawień. Pakiety instalacyjne są tworzone i przechowywane przez Kaspersky Security Center w dedykowanym podfolderze folderu udostępnionego.

W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.

Instrukcje dotyczące korzystania z tej metody konfiguracji dla aplikacji Kaspersky przed ich zainstalowaniem przy użyciu narzędzi firm trzecich można znaleźć w sekcji „Zdalna instalacja przy użyciu zasad grupy Microsoft Windows".

Natychmiast po zainstalowaniu programu Kaspersky Security Center, automatycznie zostaje wygenerowanych kilka pakietów instalacyjnych. Pakiety te są gotowe do zainstalowania i zawierają pakiety Agenta sieciowego oraz pakiety aplikacji zabezpieczających dla Microsoft Windows.

Klucz licencyjny dla aplikacji można ustawić we właściwościach pakietu instalacyjnego, jednakże zalecane jest unikanie tej metody dystrybucji licencji, gdyż w łatwy sposób można uzyskać dostęp do pakietów instalacyjnych. Dla kluczy licencyjnych należy używać zadań automatycznego rozsyłania kluczy licencyjnych lub instalacji.

Właściwości MSI i pliki transformacji

Innym sposobem skonfigurowania instalacji na platformie Windows jest zdefiniowanie właściwości MSI i plików transformacji. Ta metoda może być stosowana w następujących przypadkach:

- Podczas instalacji poprzez zasady grupy systemu Windows, korzystając ze standardowych narzędzi Microsoft lub innych narzędzi firm trzecich do zarządzania zasadami grupy systemu Windows.
- Podczas instalacji aplikacji przy użyciu narzędzi firm trzecich przeznaczonych do zarządzania instalatorami w formacie instalatora Microsoft.

Zdalna instalacja przy użyciu narzędzi firm trzecich

Jeśli w organizacji dostępne są jakiekolwiek narzędzia do zdalnej instalacji aplikacji (na przykład, Microsoft System Center), wygodnym rozwiązaniem będzie przeprowadzenie wstępnej zdalnej instalacji przy użyciu tych narzędzi.

Należy wykonać następujące czynności:

- Wybierz metodę konfiguracji instalacji, która najbardziej odpowiada używanemu narzędziu do zdalnej instalacji.
- Zdefiniuj mechanizm synchronizacji pomiędzy modyfikacją ustawień pakietów instalacyjnych (poprzez interfejs Konsoli administracyjnej) a działaniem wybranych narzędzi firm trzecich, używanych do zdalnej instalacji aplikacji z pakietu instalacyjnego.
- Podczas instalacji z folderu współdzielonego upewnij się, że ten zasób plików posiada wystarczającą pojemność.

Informacje o zadaniach zdalnej instalacji w Kaspersky Security Center

Kaspersky Security Center oferuje różne mechanizmy zdalnej instalacji aplikacji, które są zaimplementowane pod postacią zadań zdalnej instalacji (instalacja wymuszona, instalacja poprzez skopiowanie obrazu dysku twardego, instalacja poprzez zasady grupy systemu Microsoft Windows). Możesz utworzyć zadanie zdalnej instalacji dla określonej grupy administracyjnej oraz dla wskazanych urządzeń lub wyboru urządzeń (takie zadania są wyświetlane w Konsoli administracyjnej, w folderze **Zadania**). Podczas tworzenia zadania możesz wybrać pakiety instalacyjne (Agenta sieciowego i / lub innej aplikacji), które zostaną zainstalowane w obrębie tego zadania, a także określić pewne ustawienia, które definiują metodę zdalnej instalacji. Dodatkowo można użyć kreatora zdalnej instalacji, którego działanie polega na utworzeniu zadania zdalnej instalacji i monitorowaniu wyników.

Zadania dla grup administracyjnych dotyczą urządzeń znajdujących się w określonej grupie oraz wszystkich urządzeń we wszystkich podgrupach tej grupy administracyjnej. Zadanie obejmuje urządzenia podrzędnych Serwerów administracyjnych znajdujących się w grupie lub jej dowolnych podgrupach, jeśli odpowiednie ustawienie zostało włączone w zadaniu.

Zadania dla określonych urządzeń aktualizują listę urządzeń klienckich przy każdym uruchomieniu zgodnie z zawartością wyborów w momencie uruchomienia zadania. Jeśli wybór zawiera urządzenia, które zostały połączone z podrzędnymi Serwerami administracyjnymi, zadanie zostanie uruchomione także na tych urządzeniach. Szczegółowe informacje dotyczące tych ustawień i metod instalacji znajdują się poniżej.

Aby zapewnić pomyślne działanie zadania zdalnej instalacji na urządzeniach połączonych z podrzędnymi Serwerami administracyjnymi, należy użyć zadania przekazywania do przekazania pakietów instalacyjnych używanych przez zadanie użytkownika do odpowiednich podrzędnych Serwerów administracyjnych.

Wdrażanie poprzez przechwycenie i skopiowanie obrazu urządzenia

Jeśli konieczne jest zainstalowanie Agenta sieciowego na urządzeniach, na których musi zostać (ponownie) zainstalowany system operacyjny i inne oprogramowanie, możesz wykorzystać mechanizm przechwytywania i kopiowania obrazu tego urządzenia.

W celu przeprowadzenia wdrożenia poprzez przechwycenie i skopiowanie dysku twardego:

1. Utwórz urządzenie referencyjne z zainstalowanym systemem operacyjnym i niezbędnym oprogramowaniem, włączając w to Agenta sieciowego i aplikację zabezpieczającą.

2. Przechwyć obraz urządzenia referencyjnego i roześlij ten obraz na nowe urządzenia przy użyciu dedykowanego zadania z Kaspersky Security Center.

   Aby przechwytywać i instalować obrazy dysków, możesz skorzystać z narzędzi firm trzecich dostępnych w organizacji lub z funkcji (na mocy licencji Zarządzania lukami i poprawkami) oferowanej przez Kaspersky Security Center.

Jeśli do zarządzania obrazami dysków używasz narzędzi firm trzecich, podczas zdalnej instalacji na urządzeniu z obrazu referencyjnego musisz usunąć informacje, których Kaspersky Security Center używa do identyfikowania zarządzanego urządzenia. W przeciwnym razie Serwer administracyjny nie będzie mógł poprawnie odróżnić urządzeń, które zostały utworzone poprzez skopiowanie tego samego obrazu.

Podczas przechwytywania obrazu dysku przy użyciu narzędzi Kaspersky Security Center ten problem jest rozwiązywany automatycznie.

Kopiowanie dysku przy użyciu narzędzi firm trzecich

Jeśli podczas przechwytywania obrazu urządzenia z zainstalowanym Agentem sieciowym stosujesz narzędzia firm trzecich, użyj jednej z następujących metod:

- Zalecana metoda. Podczas instalacji Agenta sieciowego na urządzeniu referencyjnym, przed pierwszym uruchomieniem usługi Agenta sieciowego przechwyć obraz urządzenia (ponieważ unikatowa informacja identyfikująca urządzenie jest tworzona przy pierwszym połączeniu Agenta sieciowego z Serwerem administracyjnym). Zalecane jest unikanie uruchamiania usługi Agenta sieciowego, aż do zakończenia operacji przechwytywania obrazu.

- Na urządzeniu referencyjnym zatrzymaj usługę Agenta sieciowego i uruchom narzędzie klmover z kluczem -dupfix. Narzędzie klmover znajduje się w pakiecie instalacyjnym Agenta sieciowego. Unikaj kolejnych uruchomień usługi Agenta sieciowego, dopóki operacja przechwytywania obrazu nie zostanie zakończona.

- Obowiązkowo narzędzie klmover zostanie uruchomione z kluczem -dupfix przed pierwszym uruchomieniem usługi Agenta sieciowego na urządzeniach docelowych, przy pierwszym uruchomieniu systemu operacyjnego po zainstalowaniu obrazu. Narzędzie klmover znajduje się w pakiecie instalacyjnym Agenta sieciowego.

- Użyj trybu klonowania dysku Agenta sieciowego.

Jeśli obraz dysku twardego został niepoprawnie skopiowany, możesz rozwiązać ten problem.

Możesz także przechwycić obraz urządzenia bez zainstalowanego Agenta sieciowego. W tym celu wykonaj wdrożenie obrazu na urządzeniach docelowych, a następnie zainstaluj Agenta sieciowego. W przypadku korzystania z tej metody zapewnij dostęp do folderu sieciowego za pomocą autonomicznych pakietów instalacyjnych z urządzenia.

Niepoprawne kopiowanie obrazu dysku twardego

Jeśli obraz dysku z zainstalowanym Agentem sieciowym został skopiowany bez przestrzegania zasad zdalnej instalacji, niektóre urządzenia mogą być wyświetlane razem w Konsoli administracyjnej pod postacią pojedynczej ikony z ciągle zmieniającą się nazwą.

Ten problem można rozwiązać przy użyciu jednej z następujących metod:

- Usuwając Agenta sieciowego

  Ta metoda jest najbardziej niezawodna. Na urządzeniach, które zostały niepoprawnie skopiowane z obrazu, należy usunąć Agenta sieciowego przy użyciu narzędzi innych firm, a następnie zainstalować go ponownie. Agent sieciowy nie może zostać usunięty przy użyciu narzędzi Kaspersky Security Center, ponieważ Serwer administracyjny nie potrafi odróżnić wadliwych urządzeń (w Konsoli administracyjnej mają tę samą ikonę).

- Uruchamiając narzędzie klmover z przełącznikiem "-dupfix"

  Użyj narzędzi firm trzecich, aby raz uruchomić narzędzie klmover, znajdujące się w folderze instalacyjnym Agenta sieciowego, z przełącznikiem "-dupfix" (klmover -dupfix) na wadliwych urządzeniach (tych, które zostały niepoprawnie skopiowane z obrazu). Narzędzie nie może zostać uruchomione przy użyciu narzędzi Kaspersky Security Center, ponieważ Serwer administracyjny nie potrafi odróżnić wadliwych urządzeń (w Konsoli administracyjnej mają tę samą ikonę).

  Następnie, przed uruchomienie narzędzia, usuń ikonę, pod którą wadliwe urządzenia były wyświetlane.

- Wzmacniając regułę wykrywania niepoprawnie skopiowanych urządzeń.

  > Ta metoda jest stosowana tylko wtedy, gdy zainstalowany jest Serwer administracyjny oraz Agent sieciowy w wersji 10 Service Pack 1 lub nowszej.

  Reguła wykrywania niepoprawnie skopiowanych Agentów sieciowych musi zostać wzmocniona w taki sposób, że zmiana nazwy NetBIOS urządzenia spowoduje automatyczną "naprawę" tych Agentów sieciowych (przy założeniu, że wszystkie skopiowane urządzenia posiadają unikatowe nazwy NetBIOS).

  Na urządzeniu z zainstalowanym Serwerem administracyjnym należy zaimportować plik reg (wyświetlony poniżej) do Rejestru, a następnie uruchomić ponownie usługę Serwera administracyjnego.

  - Jeśli na urządzeniu z Serwerem administracyjnym zainstalowany jest 32-bitowy system operacyjny:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

  - Jeśli na urządzeniu z Serwerem administracyjnym zainstalowany jest 64-bitowy system operacyjny:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

Zdalna instalacja przy użyciu zasad grupy Microsoft Windows

Przeprowadzenie wstępnej instalacji Agentów sieciowych poprzez zasady grupy Microsoft Windows jest zalecane wtedy, gdy spełnione są następujące warunki:

- Urządzenie należy do domeny Active Directory.
- Schemat zdalnej instalacji umożliwia zaczekanie na kolejne rutynowe ponowne uruchomienie urządzeń docelowych przed rozpoczęciem zdalnej instalacji Agentów sieciowych na tych urządzeniach (lub można wymusić zastosowanie na tych urządzeniach zasady grupy systemu Windows).

Ten schemat instalacji charakteryzuje się następującymi cechami:

- Pakiet dystrybucyjny aplikacji w formacie Microsoft Installer (pakiet MSI) znajduje się w folderze współdzielonym (folder, w którym konta SystemLokalny urządzeń docelowych mają uprawnienia do odczytu).
- W zasadzie grupy Active Directory, dla pakietu dystrybucyjnego tworzony jest obiekt instalacji.
- Obszar instalacji jest ustawiany poprzez określenie jednostki organizacyjnej (OU) i/lub grupy zabezpieczeń, która zawiera urządzenia docelowe.
- Następnym razem, gdy urządzenie docelowe zaloguje się do domeny (przed zalogowaniem się użytkowników do systemu), wszystkie zainstalowane aplikacje są sprawdzane pod kątem żądanej aplikacji. Jeśli żądana aplikacja nie zostanie odnaleziona, pakiet dystrybucyjny zostanie pobrany z zasobu określonego w zasadzie, a następnie zostanie zainstalowany.

Ten schemat zdalnej instalacji niesie za sobą korzyść, jaką jest instalowanie przypisanych aplikacji na urządzeniach docelowych podczas ładowania systemu operacyjnego, czyli nawet przed zalogowaniem się użytkownika do systemu. Nawet jeśli użytkownik, który nie ma wystarczających uprawnień, usunie aplikację, zostanie ona ponownie zainstalowana przy kolejnym uruchomieniu systemu operacyjnego. Wadą tego schematu wdrożenia jest fakt, że zmiany w zasadzie grupowej, które zostały wprowadzone przez administratora, nie zostaną zastosowane, aż do ponownego uruchomienia urządzenia (jeśli nie są używane narzędzia dodatkowe).

Zasady grupy można użyć do zainstalowania Agenta sieciowego oraz innych aplikacji, jeśli ich instalatory są w formacie Windows Installer.

Jeśli wybierzesz ten schemat zdalnej instalacji, musisz mieć na uwadze obciążenie zasobu plików, z którego pliki zostaną skopiowane na urządzenia po zastosowaniu zasad grupy systemu Windows.

Zarządzanie zasadami Microsoft Windows przy użyciu zadania zdalnej instalacji z programu Kaspersky Security Center

Najprostszym sposobem zainstalowania aplikacji poprzez zasady grupy systemu Microsoft Windows jest zaznaczenie opcji **Przypisz pakiet instalacyjny do zasad grupy Active Directory** we właściwościach zadania zdalnej instalacji z programu Kaspersky Security Center. W tym przypadku, podczas uruchamiania zadania Serwer administracyjny automatycznie wykonuje następujące działania:

- Tworzy wymagane obiekty w zasadach grupy systemu Microsoft Windows.
- Tworzy dedykowane grupy zabezpieczeń, umieszcza w nich urządzenia docelowe i przypisuje do nich instalację wybranych aplikacji. Zbiór grup zabezpieczeń zostanie zaktualizowany przy każdym uruchomieniu zadania, zgodnie z pulą urządzeń w momencie uruchomienia.

Aby ta funkcja działała, we właściwościach zadania określ konto, które posiada uprawnienia do zapisu w zasadach grupy Active Directory.

Jeśli chcesz zainstalować Agenta sieciowego i inną aplikację przy użyciu tego samego zadania, zaznaczenie opcji **Przypisz pakiet instalacyjny do zasad grupy Active Directory** spowoduje utworzenie obiektu instalacji w zasadzie Active Directory tylko dla Agenta sieciowego. Druga aplikacja wybrana w zadaniu zostanie zainstalowana przy użyciu narzędzi Agenta sieciowego od razu po jego zainstalowaniu na urządzeniu. Jeśli poprzez zasady grupy systemu Windows chcesz zainstalować aplikację inną niż Agent sieciowy, musisz utworzyć zadanie instalacji tylko dla tego pakietu instalacyjnego (bez pakietu Agenta sieciowego). Nie każda aplikacja może zostać zainstalowana przy użyciu zasad grupy Microsoft Windows. Więcej szczegółów na temat tej możliwości można znaleźć w informacjach opisujących możliwe metody instalowania aplikacji.

Jeśli żądane obiekty są tworzone w zasadzie grupy przy użyciu narzędzi Kaspersky Security Center, folder współdzielony Kaspersky Security Center zostanie użyty jako źródło pakietu instalacyjnego. Podczas planowania zdalnej instalacji należy zestawić prędkość odczytu tego folderu z liczbą urządzeń i rozmiarem pakietu dystrybucyjnego przeznaczonego do zainstalowania. Przydatne może być umieszczenie folderu współdzielonego Kaspersky Security Center w dedykowanym repozytorium plików charakteryzującym się wysoką wydajnością.

Oprócz łatwości użycia, automatyczne tworzenie zasad grupy systemu Windows poprzez Kaspersky Security Center posiada następujące korzyści: podczas planowania instalacji Agenta sieciowego można w łatwy sposób określić grupę administracyjną Kaspersky Security Center, do której urządzenia będą automatycznie przenoszone po zakończeniu instalacji. Tę grupę można określić przy użyciu kreatora tworzenia nowego zadania lub w oknie ustawień zadania zdalnej instalacji.

Podczas zarządzania zasadami grupy systemu Windows poprzez Kaspersky Security Center możesz wskazać urządzenia dla obiektu zasad grupy, tworząc grupę zabezpieczeń. Kaspersky Security Center synchronizuje zawartość grupy zabezpieczeń z bieżącym zbiorem urządzeń uwzględnionych w zadaniu. Jeśli do zarządzania zasadami grupy używasz innych narzędzi, możesz skojarzyć obiekty zasad grupy bezpośrednio z wybranymi jednostkami organizacyjnymi Active Directory.

Samodzielna instalacja aplikacji przy użyciu zasad Microsoft Windows

Administrator może tworzyć obiekty wymagane do zainstalowania w zasadach grupy systemu Windows w swoim imieniu. W tym przypadku administrator może udostępnić odnośniki do pakietów przechowywanych w folderze współdzielonym Kaspersky Security Center lub wysłać te pakiety na dedykowany serwer plików i udostępnić odnośniki do ich pobrania.

Dostępne są następujące scenariusze instalacji:

- Administrator tworzy pakiet instalacyjny i konfiguruje jego ustawienia w Konsoli administracyjnej. Obiekt zasad grupy zawiera odnośnik do pliku MSI tego pakietu, który jest przechowywany w folderze współdzielonym Kaspersky Security Center.

- Administrator tworzy pakiet instalacyjny i konfiguruje jego ustawienia w Konsoli administracyjnej. Następnie administrator kopiuje cały podfolder EXEC tego pakietu z folderu współdzielonego Kaspersky Security Center do folderu w dedykowanym zasobie plików w organizacji. Obiekt zasad grupy zawiera odnośnik do pliku MSI tego pakietu, który jest przechowywany w podfolderze w dedykowanym zasobie plików w organizacji.

- Administrator pobiera pakiet dystrybucyjny aplikacji (w tym pakiet Agenta sieciowego) z Internetu i wysyła go do dedykowanego zasobu plików w organizacji. Obiekt zasad grupy zawiera odnośnik do pliku MSI tego pakietu, który jest przechowywany w podfolderze w dedykowanym zasobie plików w organizacji. Ustawienia instalacji są definiowane poprzez konfigurowanie właściwości MSI lub poprzez konfigurowanie plików transformacji MST.

Wymuszona zdalna instalacja przy użyciu zadania zdalnej instalacji z Kaspersky Security Center

Aby wykonać wstępne wdrożenie Agenta sieciowego lub innych aplikacji, możesz wymusić instalację wybranych pakietów instalacyjnych, korzystając z zadania zdalnej instalacji programu Kaspersky Security Center — pod warunkiem, że każde urządzenie ma konto(-a) użytkownika z uprawnieniami administratora lokalnego.

Instalacja wymuszona może być zastosowana także wtedy, gdy urządzenia nie są dostępne bezpośrednio dla Serwera administracyjnego, na przykład: urządzenia znajdują się w odizolowanych sieciach lub urządzenia są w sieci lokalnej, a Serwer administracyjny znajduje się w strefie DMZ.

W przypadku wdrożenia początkowego Agent sieciowy nie jest instalowany. Dlatego w ustawieniach zadania zdalnej instalacji nie można wybrać opcji dystrybucji plików wymaganych do instalacji aplikacji za pomocą Agenta sieciowego. Dystrybucję plików można przeprowadzić wyłącznie za pośrednictwem zasobów systemu operacyjnego, za pośrednictwem Serwera administracyjnego lub punktów dystrybucji.

Usługa Serwera administracyjnego musi być uruchomiona na koncie posiadającym uprawnienia administracyjne na urządzeniach docelowych. Alternatywnie możesz określić konto, które ma dostęp do części admin$ w ustawieniach ogólnych zadania zdalnej instalacji.

Domyślnie zadanie zdalnej instalacji jest stosowane na urządzeniach poprzez użycie danych logowania konta, na którym uruchomiony jest Serwer administracyjny. Należy wyjaśnić, że chodzi o konto używane do uzyskiwania dostępu do części admin$, a nie o konto, na którym uruchamiane jest zadanie zdalnej instalacji. Instalacja zostanie przeprowadzona z poziomu konta SystemLokalny.

Możesz bezpośrednio wskazać urządzenia docelowe, wybrać grupę administracyjną Kaspersky Security Center, do której należą; lub utworzyć wybór urządzeń w oparciu o określone kryterium. Instalacja rozpoczyna się zgodnie z terminarzem zadania. Jeśli we właściwościach zadania włączone jest ustawienie **Uruchom pominięte zadania**, zadanie może zostać uruchomione albo natychmiast po włączeniu urządzeń docelowych, albo po ich przeniesieniu do docelowej grupy administracyjnej.

Instalacja wymuszona obejmuje dostarczenie pakietów instalacyjnych do urządzeń docelowych, skopiowanie plików do zasobu admin$ na każdym urządzeniu docelowym, a także zdalną rejestrację usług pomocniczych na tych urządzeniach. Dostarczenie pakietów instalacyjnych do punktów dystrybucji odbywa się poprzez funkcję Kaspersky Security Center zapewniającą interakcję z siecią. W tym przypadku muszą być spełnione następujące warunki:

- Dostęp do urządzeń docelowych jest możliwy od strony Serwera administracyjnego lub od strony punktu dystrybucji.
- Rozwiązywanie nazw urządzeń docelowych działa poprawnie w sieci.
- Zasób administracyjny (admin$) pozostanie włączony na urządzeniach docelowych.
- Na urządzeniach docelowych uruchomione są następujące usługi systemowe:
  - Serwer (LanmanServer)

    Domyślnie ta usługa jest uruchomiona.
  - Program uruchamiający procesy serwera DCOM (DcomLaunch)

- Mapowanie punktów końcowych RPC (RpcEptMapper)
- Zdalne wywoływanie procedur (RpcSs)

- Port TCP 445 jest otwarty na urządzeniach docelowych, aby umożliwić zdalny dostęp za pomocą Windows Management Instrumentation.

  Sprawdzany jest również port TCP 445 w celu ustalenia typu systemu operacyjnego urządzenia docelowego przed wykonaniem instalacji zdalnej (jeśli port UDP 137 jest niedostępny).

  > Protokoły TCP 139, UDP 137 i UDP 138 są używane przez starsze protokoły i nie są już potrzebne w obecnych aplikacjach.

  W zaporze sieciowej muszą być dozwolone dynamiczne porty dostępu wychodzącego w celu nawiązywania połączeń z Serwera administracyjnego i punktów dystrybucji do urządzeń docelowych.

- Ustawienia zabezpieczeń zasad domeny usługi Active Directory umożliwiają działanie protokołu NTLM podczas wdrażania Agenta Sieciowego.

- Na urządzeniach docelowych z systemem Microsoft Windows XP tryb Proste udostępnianie plików jest wyłączony.

- Na urządzeniach docelowych model współdzielenia dostępu i zabezpieczeń jest ustawiony jako *Klasyczny – lokalni użytkownicy uwierzytelniają się jako oni sami*. W żadnym wypadku nie może to być *tylko Gość – lokalni użytkownicy uwierzytelniają się jako Gość*.

- Urządzenia docelowe są członkami domeny lub wcześniej są tworzone na urządzeniach docelowych jednakowe konta z uprawnieniami administratora.

> Aby pomyślnie zainstalować Agenta sieciowego lub inne aplikacje na urządzeniu, które nie jest przyłączone do domeny Active Directory systemu Windows Server 2003 lub nowszego, należy wyłączyć zdalną kontrolę konta użytkownika (UAC) na tym urządzeniu. Zdalna kontrola konta użytkownika (UAC) jest jednym z powodów uniemożliwiających lokalnym kontom administracyjnym dostęp do admin$, który jest konieczny do wymuszonej instalacji Agenta sieciowego lub innych aplikacji. Wyłączenie zdalnej kontroli konta użytkownika (UAC) nie ma wpływu na lokalną UAC.

Podczas instalacji na nowych urządzeniach, które jeszcze nie zostały przydzielone do żadnej grupy administracyjnej Kaspersky Security Center, możesz otworzyć właściwości zadania zdalnej instalacji i określić grupę administracyjną, do której urządzenia zostaną przeniesione po zakończeniu instalacji Agenta sieciowego.

> Podczas tworzenia zadania grupowego należy pamiętać, że każde zadanie grupowe ma wpływ na wszystkie urządzenia we wszystkich grupach zagnieżdżonych w wybranej grupie. Dlatego też należy unikać powielania zadań instalacji w podgrupach.

Prostszym sposobem tworzenia zadań wymuszonej instalacji aplikacji jest instalacja automatyczna. We właściwościach grupy administracyjnej należy otworzyć listę pakietów instalacyjnych a następnie wybrać te, które muszą zostać zainstalowane na urządzeniach w tej grupie. W rezultacie, wybrane pakiety instalacyjne zostaną automatycznie zainstalowane na wszystkich urządzeniach w tej grupie i wszystkich jej podgrupach. Przedział czasu, w trakcie którego pakiety zostaną zainstalowane, zależy od przepustowości sieci i całkowitej liczby urządzeń w sieci.

Aby zmniejszyć obciążenie Serwera administracyjnego podczas dostarczania pakietów instalacyjnych do urządzeń docelowych, w zadaniu instalacji można wybrać instalację za pośrednictwem punktów dystrybucji. Należy zauważyć, że ta metoda instalacji powoduje duże obciążenie urządzeń pełniących role punktów dystrybucji. W związku z tym zaleca się wybór urządzeń spełniających wymagania stawiane punktom dystrybucji. Jeśli korzystasz z punktów dystrybucji, upewnij się, że znajdują się one w każdej z odizolowanych podsieci, w których znajdują się urządzenia docelowe.

Korzystanie z punktów dystrybucji jako lokalnych centrów instalacji jest dobrym rozwiązaniem, gdy instalacja na urządzeniach w podsieciach komunikujących się z Serwerem administracyjnym odbywa się poprzez kanały o małej przepustowości, a pomiędzy urządzeniami w tej samej podsieci dostępny jest szeroki kanał.

Co więcej, wolna przestrzeń na dysku w partycji, na której znajduje się folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit, musi wielokrotnie przekraczać całkowity rozmiar pakietów dystrybucyjnych instalowanych aplikacji.

Uruchamianie pakietów autonomicznych utworzonych przez Kaspersky Security Center

Powyżej opisane metody wstępnej zdalnej instalacji Agenta sieciowego i innych aplikacji nie zawsze będą mogły zostać zaimplementowane, gdyż nie jest możliwe spełnienie wszystkich wymaganych warunków. W takich przypadkach można utworzyć standardowy plik wykonywalny zwany *autonomicznym pakietem instalacyjnym* poprzez Kaspersky Security Center, korzystając z pakietów instalacyjnych z odpowiednimi ustawieniami instalacji, które zostały przygotowane przez administratora. Autonomiczny pakiet instalacyjny jest przechowywany w folderze współdzielonym Kaspersky Security Center.

Korzystając z Kaspersky Security Center, możesz wysłać do wybranych użytkowników wiadomość e-mail zawierającą odnośnik do tego pliku w folderze współdzielonym oraz prośbę o jego uruchomienie (w trybie interaktywnym lub z przełącznikiem "-s" dla cichej instalacji). Do wiadomości e-mail możesz załączyć autonomiczny pakiet instalacyjny, a następnie wysłać ją do użytkowników urządzeń, którzy nie mają dostępu do folderu współdzielonego Kaspersky Security Center. Administrator może skopiować pakiet autonomiczny na dysk wymienny, dostarczyć go na odpowiednie urządzenie, a następnie uruchomić go.

Pakiet autonomiczny można utworzyć z pakietu Agenta sieciowego, pakietu innej aplikacji (na przykład, zabezpieczającej) lub z obu pakietów. Jeśli pakiet autonomiczny został utworzony z pakietu Agenta sieciowego i innej aplikacji, instalacja rozpocznie się z Agenta sieciowego.

Podczas tworzenia pakietu autonomicznego z pakietu Agenta sieciowego możesz określić grupę administracyjną, do której nowe urządzenia (te, które nie zostały przydzielone do żadnej grup administracyjnych) zostaną automatycznie przeniesione po zakończeniu instalacji Agenta sieciowego na tych urządzeniach.

Pakiety autonomiczne mogą być uruchomione w trybie interaktywnym (opcja domyślna), wyświetlając wynik instalacji aplikacji, które zawierają, lub mogą być uruchomione w trybie cichym (z kluczem "-s"). Tryb cichy może zostać użyty dla instalacji ze skryptów, na przykład, ze skryptów skonfigurowanych do uruchamiania po wdrożeniu obrazu systemu operacyjnego. Wynik instalacji w trybie cichym jest determinowany przez kod zwrotny procesu.

Autonomiczny Agent sieciowy dla systemu Linux ma opcjonalną zależność od narzędzia nmap. Jeśli narzędzie nmap jest niedostępne lub ma wersję starszą niż 6.0, funkcja Broadcast DHCP Discover nie jest obsługiwana.

Opcje ręcznej instalacji aplikacji

Administratorzy lub doświadczeni użytkownicy mogą zainstalować aplikacje ręcznie w trybie interaktywnym. Mogą oni użyć oryginalnych pakietów dystrybucyjnych lub wygenerowanych z nich pakietów instalacyjnych, które są przechowywane w folderze współdzielonym Kaspersky Security Center. Domyślnie instalatory są uruchamiane w trybie interaktywnym i wyświetlają użytkownikom komunikaty z pytaniami o podanie wszystkich wymaganych wartości. Jednakże podczas uruchamiania procesu setup.exe z katalogu głównego pakietu instalacyjnego z przełącznikiem "-s", instalator zostanie uruchomiony w trybie cichym i z ustawieniami, które zostały określone podczas konfiguracji pakietu instalacyjnego.

Podczas uruchamiania procesu setup.exe z katalogu głównego pakietu instalacyjnego, przechowywanego w folderze współdzielonym Kaspersky Security Center, pakiet zostanie najpierw skopiowany do tymczasowego folderu lokalnego, a następnie instalator aplikacji zostanie uruchomiony z folderu lokalnego.

Tworzenie pliku MST

Aby przekształcić zawartość pakietu MSI i zastosować niestandardowe ustawienia do istniejącego pliku MSI, należy utworzyć plik transformacji w formacie MST. Aby to zrobić, użyj edytora Orca.exe, który jest zawarty w Windows SDK.

Aby utworzyć plik MST:

1. Uruchom edytor Orca.exe.
2. Przejdź do zakładki **Plik** i w menu kliknij opcję **Otwórz**.
3. Wybierz plik Kaspersky Network Agent.msi.
4. Przejdź do zakładki **Transformacja** i w menu wybierz **Nowa transformacja**.
5. W kolumnie **Tabele** wybierz **Właściwość** i wpisz następujące wartości:
   - *EULA=1*
   - *SERVERADDRESS=<Adres Serwera administracyjnego>*

   Kliknij przycisk **Zapisz**.
6. Przejdź do zakładki **Transformacja** i w menu wybierz opcję **Generuj transformację**.
7. W oknie, które zostanie otwarte, podaj nazwę tworzonego pliku transformacji, a następnie kliknij przycisk **Zapisz**.

Plik MST zostaje zapisany.

Zdalna instalacja aplikacji na urządzeniach z zainstalowanym Agentem sieciowym

Jeśli na urządzeniu jest zainstalowany działający Agent sieciowy, połączony z głównym Serwerem administracyjnym (lub jednym z jego Serwerów podrzędnych), możesz zaktualizować Agenta sieciowego na tym urządzeniu, a także zainstalować, zaktualizować lub usunąć dowolne obsługiwane aplikacje poprzez Agenta sieciowego.

Możesz włączyć opcję **Przy użyciu Agenta sieciowego** we właściwościach zadania zdalnej instalacji.

Jeśli ta opcja jest zaznaczona, pakiety instalacyjne z ustawieniami instalacji, zdefiniowanymi przez administratora, zostaną przesłane na urządzenia docelowe poprzez kanały komunikacyjne między Agentem sieciowym a Serwerem administracyjnym.

Aby zoptymalizować obciążenie na Serwerze administracyjnym oraz zminimalizować ruch pomiędzy Serwerem administracyjnym a urządzeniami, należy wskazać punkty dystrybucji w każdej sieci zdalnej lub domenie rozgłoszeniowej (sekcja „Informacje o punktach dystrybucji" oraz sekcja „Tworzenie struktury grup administracyjnych i przydzielanie punktów dystrybucji"). W tym przypadku pakiety instalacyjne oraz ustawienia instalatora są rozsyłane z Serwera administracyjnego na urządzenia docelowe poprzez punkty dystrybucji.

Co więcej, możliwe jest użycie punktów dystrybucji do transmisyjnego (multiemisja) dostarczania pakietów instalacyjnych, co pozwala znacząco zmniejszyć ruch sieciowy podczas zdalnej instalacji aplikacji.

Podczas wysyłania pakietów instalacyjnych na urządzenia docelowe poprzez kanały komunikacyjne między Agentami sieciowymi a Serwerem administracyjnym, wszystkie pakiety instalacyjne, które zostały przygotowane do wysłania, zostaną także zbuforowane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Jeśli używanych jest kilka dużych pakietów instalacyjnych różnych typów oraz wykorzystywana jest duża liczba punktów dystrybucji, rozmiar tego folderu może drastycznie się powiększyć.

Nie można ręcznie usunąć plików z folderu FTServer. Jeśli oryginalne pakiety instalacyjne zostaną usunięte, odpowiednie dane zostaną automatycznie usunięte z folderu FTServer.

Dane pobierane przez punkty dystrybucji są zapisywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Nie można ręcznie usunąć plików z folderu $FTCITmp. Po zakończeniu działania zadań korzystających z danych z tego folderu, jego zawartość zostanie automatycznie usunięta.

Ponieważ pakiety instalacyjne są rozsyłane poprzez kanały komunikacyjne między Serwerem administracyjnym a Agentami sieciowymi z repozytorium pośredniczącego w formacie zoptymalizowanym dla transferów sieciowych, nie można wprowadzać żadnych zmian w pakietach instalacyjnych, przechowywanych w oryginalnym folderze każdego pakietu instalacyjnego. Takie zmiany nie zostałyby automatycznie zarejestrowane przez Serwer administracyjny. Jeśli chcesz ręcznie zmodyfikować pliki pakietów instalacyjnych (chociaż zalecane jest unikanie takiego rozwiązania), należy zmodyfikować dowolne ustawienia pakietu instalacyjnego w Konsoli administracyjnej. Zmodyfikowanie ustawień pakietu instalacyjnego w Konsoli administracyjnej spowoduje, że Serwer administracyjny zaktualizuje obraz pakietu w pamięci podręcznej, który został przygotowany do przesłania na urządzenia docelowe.

Zarządzanie ponownym uruchamianiem urządzeń w zadaniu zdalnej instalacji

Aby zakończyć zdalną instalację aplikacji, często wymagane jest ponowne uruchomienie urządzeń (szczególnie w systemie Windows).

Jeśli korzystasz z zadania zdalnej instalacji z Kaspersky Security Center, w Kreatorze tworzenia nowego zadania lub w oknie właściwości zadania, które zostało utworzone (sekcja **Ponowne uruchomienie systemu operacyjnego**), możesz wybrać akcję, która zostanie wykonana, gdy urządzenie z systemem Windows wymaga ponownego uruchomienia:

- **Nie uruchamiaj ponownie urządzenia**. W tym przypadku komputer nie zostanie automatycznie uruchomiony ponownie. Aby zakończyć instalację, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań instalacji na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**. W tym przypadku urządzenie jest zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia instalacji. Opcja jest przydatna, gdy zadania instalacji są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**. W tym przypadku, na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Opcja **Pytaj użytkownika o akcję** jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia komputera.

Aktualizowanie baz danych w pakiecie instalacyjnym aplikacji zabezpieczającej

Przed rozpoczęciem wdrażania ochrony należy pamiętać o możliwości aktualizacji antywirusowych baz danych (w tym modułów i łat), dostarczanych wraz z pakietem dystrybucyjnym aplikacji zabezpieczającej. Dobrym rozwiązaniem jest zaktualizowanie baz danych w pakiecie instalacyjnym aplikacji przed rozpoczęciem wdrożenia (na przykład przy użyciu odpowiedniego polecenia z menu kontekstowego wybranego pakietu instalacyjnego). Zmniejszy to liczbę ponownych uruchomień wymaganych do zakończenia wdrożenia ochrony na urządzeniach docelowych.

Korzystanie z narzędzi do zdalnej instalacji aplikacji z Kaspersky Security Center do uruchamiania odpowiednich plików wykonywalnych na zarządzanych urządzeniach

Korzystając z Kreatora tworzenia nowego pakietu, możesz wybrać dowolny plik wykonywalny i zdefiniować dla niego ustawienia wiersza poleceń. W tym celu należy dodać do pakietu instalacyjnego sam wybrany plik lub cały folder, w którym ten plik się znajduje. Następnie konieczne jest utworzenie zadania zdalnej instalacji i wybranie utworzonego pakietu instalacyjnego.

Podczas wykonywania zadania, na urządzeniach docelowych zostanie uruchomiony określony plik wykonywalny ze zdefiniowanymi ustawieniami wiersza poleceń.

Jeśli używasz instalatorów w formacie Microsoft Windows Installer (MSI), Kaspersky Security Center przeanalizuje wyniki instalacji przy użyciu standardowych narzędzi.

Jeśli dostępna jest licencja Zarządzania lukami i poprawkami, Kaspersky Security Center (podczas tworzenia pakietu instalacyjnego dla dowolnej obsługiwanej aplikacji w środowisku korporacyjnym) użyje także reguł do zainstalowania i przeanalizowania wyników instalacji, które znajdują się w jego aktualizowanej bazie danych.

W innym przypadku domyślne zadanie dla plików wykonywalnych poczeka na zakończenie uruchomionych procesów i wszystkich jego procesów podrzędnych. Po zakończeniu wszystkich uruchomionych procesów, zadanie zostanie zakończone pomyślnie niezależnie od kodu zwrotnego procesu instalacji. Aby zmienić takie zachowanie tego zadania, przed utworzeniem zadania należy ręcznie zmodyfikować pliki .kpd, które zostały wygenerowane przez Kaspersky Security Center w folderze nowo utworzonego pakietu instalacyjnego i jego podfolderach.

Pliki .kpd używają kodowania ASCII. Pliki .kud używają kodowania Unicode.

Aby zadanie nie czekało na zakończenie uruchomionych procesów, w sekcji [SetupProcessResult] ustaw wartość ustawienia Wait na 0:

```
[SetupProcessResult]
Wait=0
```

Aby zadanie czekało tylko na zakończenie uruchomionych procesów w systemie Windows, a nie na zakończenie procesów podrzędnych, w sekcji [SetupProcessResult] ustaw wartość ustawienia WaitJob na 0, na przykład:

```
[SetupProcessResult]
WaitJob=0
```

Aby zadanie zostało pomyślnie ukończone lub zwróciło błąd, w zależności od kodu zwrotnego uruchomionego procesu, utwórz plik wykonywalny .bat, który zapisze kod błędu do pliku, na przykład:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Następnie zmodyfikuj pliki .kud wygenerowane przez Kaspersky Security Center w folderze nowo utworzonego pakietu instalacyjnego:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

W tym przypadku każdy kod inny niż te znajdujące się na liście będzie zwracany jako błąd.

W celu wyświetlenia wiersza z komentarzem na temat pomyślnego zakończenia zadania lub błędu w wynikach zadania, w sekcji [SetupProcessResult_SuccessCodes] i [SetupProcessResult_ErrorCodes] wpisz krótki opis błędów odpowiadających kodom zwrotnym procesu, na przykład:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A restart is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation canceled by the user
1603=Fatal error during installation
```

W celu użycia narzędzi Kaspersky Security Center do zarządzania ponownym uruchomieniem urządzenia (jeśli ponowne uruchomienie jest wymagane do zakończenia działania), w sekcji [SetupProcessResult_NeedReboot] umieść listę kodów zwrotnych procesu, które wskazują na konieczność ponownego uruchomienia komputera:

```
[SetupProcessResult_NeedReboot]
3010=
```

Monitorowanie wdrożenia

W celu monitorowania instalacji Kaspersky Security Center oraz upewnienia się, że aplikacja zabezpieczająca i Agent sieciowy są zainstalowane na zarządzanych urządzeniach należy sprawdzić wskaźnik w sekcji **Wdrażanie**. Wskaźnik ten zlokalizowany jest w obszarze roboczym węzła Serwera administracyjnego w oknie głównym Konsoli administracyjnej. Kolory wskaźnika odzwierciedlają bieżący stan zdalnej instalacji. Obok wskaźnika wyświetlana jest liczba urządzeń, na których jest zainstalowany Agent sieciowy i aplikacje zabezpieczające. Jeśli uruchomione są jakiekolwiek zadania instalacji, postęp ich wykonania możesz monitorować w tym miejscu. Jeśli wystąpią jakiekolwiek błędy instalacyjne, liczba błędów zostanie wyświetlona w tym miejscu. Szczegóły dotyczące błędów można wyświetlić, klikając odnośnik.

Możesz także wykorzystać schemat zdalnej instalacji z obszaru roboczego folderu **Zarządzane urządzenia** na zakładce **Grupy**. Wykres odzwierciedla proces zdalnej instalacji i wyświetla liczbę urządzeń bez Agenta sieciowego, z Agentem sieciowym lub z Agentem sieciowym i aplikacją zabezpieczającą.

Więcej informacji o postępie wykonania zdalnej instalacji (lub działaniu określonego zadania instalacji) można uzyskać, otwierając okno wyników odpowiedniego zadania zdalnej instalacji: Kliknij zadanie prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wyniki**. Okno będzie wyświetlało dwie listy: górna lista zawiera stany zadania na urządzeniach, natomiast dolna lista zawiera zdarzenia zadania na urządzeniu, które jest aktualnie wybrane na górnej liście.

Informacje o błędach zdalnej instalacji zostaną dodane do dziennika zdarzeń aplikacji Kaspersky na Serwerze administracyjnym. Informacje o błędach są także dostępne w odpowiednim wyborze zdarzeń, w węźle Serwer administracyjny, na zakładce **Zdarzenia**.

Konfigurowanie instalatorów

Ta sekcja zawiera informacje na temat plików instalatorów Kaspersky Security Center i ustawień instalacji, a także zalecenia dotyczące instalacji Serwera administracyjnego i Agenta sieciowego w trybie cichym.

Informacje ogólne

Instalatory komponentów Kaspersky Security Center 15.1 (Serwer administracyjny, Agent sieciowy i Konsola administracyjna) bazują na technologii Instalatora Windows. Pakiet MSI jest podstawą instalatora. Ten format pakietów umożliwia wykorzystanie wszystkich korzyści oferowanych przez Instalator Windows: skalowalność, dostępność systemu poprawek, system transformacji, scentralizowana instalacja za pośrednictwem rozwiązań firm trzecich oraz niewidoczna rejestracja w systemie operacyjnym.

Instalacja w trybie cichym (z plikiem odpowiedzi)

Instalatory Serwera administracyjnego i Agenta sieciowego mogą pracować z plikiem odpowiedzi (ss_install.xml), w którym zintegrowane są parametry instalacji w trybie cichym bez udziału użytkownika. Plik ss_install.xml znajduje się w tym samym folderze co pakiet MSI. Jest on używany automatycznie podczas instalacji w trybie cichym. Możesz włączyć tryb cichej instalacji z użyciem klucza „/s" wiersza polecenia.

Na przykład:

```
setup.exe /s
```

Przed uruchomieniem instalatora w trybie cichym przeczytaj Umowę licencyjną użytkownika końcowego (EULA). Jeśli pakiet dystrybucyjny Kaspersky Security Center nie zawiera pliku TXT z treścią Umowy licencyjnej użytkownika końcowego, możesz pobrać ten plik ze strony internetowej Kaspersky.

Plik ss_install.xml jest wewnętrznym formatem parametrów instalatora Kaspersky Security Center. Pakiety dystrybucyjne zawierają plik ss_install.xml z domyślnymi parametrami.

Nie należy ręcznie modyfikować pliku ss_install.xml. Ten plik może być modyfikowany tylko przy użyciu narzędzi Kaspersky Security Center podczas edytowania parametrów pakietów instalacyjnych w Konsoli administracyjnej.

W celu zmodyfikowania pliku odpowiedzi dla instalacji Serwera administracyjnego:

1. Otwórz pakiet dystrybucyjny Kaspersky Security Center. Jeśli używasz pełnego pakietu pliku EXE, rozpakuj go.
2. Utwórz folder Serwer, otwórz wiersz polecenia, a następnie uruchom następujące polecenie:
   ```
   setup.exe /r ss_install.xml
   ```
   Plik instalacyjny Kaspersky Security Center uruchomi się.
3. Postępuj zgodnie z instrukcjami kreatora, aby skonfigurować instalację Kaspersky Security Center.

   Po zakończeniu działania kreatora plik odpowiedzi jest automatycznie modyfikowany zgodnie z nowymi ustawieniami określonymi przez użytkownika.

Instalacja Agenta sieciowego w trybie cichym (bez pliku odpowiedzi)

Agenta sieciowego można zainstalować przy użyciu jednego pakietu .msi, określając wartości właściwości MSI w standardowy sposób. Ten scenariusz umożliwia zainstalowanie Agenta sieciowego przy użyciu zasad grupy.

Nie zmieniaj nazwy pakietu instalacyjnego Kaspersky Network Agent.msi. Zmiana nazwy tego pakietu może spowodować błędy instalacji podczas przyszłych aktualizacji Agenta sieciowego.

Aby uniknąć konfliktów pomiędzy parametrami zdefiniowanymi poprzez właściwości MSI a parametrami zdefiniowanymi w pliku odpowiedzi, możesz wyłączyć plik odpowiedzi, ustawiając właściwość `DONT_USE_ANSWER_FILE=1`. Plik MSI znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center, w folderze Packages\NetAgent\exec. Poniżej znajduje się przykład uruchomienia instalatora Agenta sieciowego z pakietem .msi.

Instalacja Agenta sieciowego w trybie cichym wymaga akceptacji warunków Umowy Licencyjnej Użytkownika Końcowego. Użyj parametru `EULA=1` tylko wtedy, gdy w pełni przeczytałeś, zrozumiałeś i zaakceptowałeś warunki Umowy licencyjnej użytkownika końcowego.

Na przykład:
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Możliwe jest także zdefiniowanie parametrów instalacji dla pakietu .msi poprzez wcześniejsze przygotowanie pliku odpowiedzi (z rozszerzeniem .mst). To polecenie wygląda następująco:

Na przykład:
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

W jednym poleceniu można określić kilka plików odpowiedzi.

Jeśli chcesz uaktualnić Agenta sieciowego za pomocą Instalatora Windows, uruchom następujące polecenie:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Częściowa konfiguracja instalacji poprzez setup.exe

Podczas uruchamiania instalacji aplikacji z pliku setup.exe, do pakietu MSI możesz dodać wartości dowolnych właściwości MSI.

To polecenie wygląda następująco:

Na przykład:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Parametry instalacji Serwera administracyjnego

Poniższa tabela opisuje właściwości MSI, które można skonfigurować podczas instalacji Serwera administracyjnego. Wszystkie parametry są opcjonalne, za wyjątkiem EULA i PRIVACYPOLICY.

Właściwość MSI	Opis	Dostępne wartości
Umowa licencyjna użytkownika końcowego	Akceptacja postanowień i warunków Umowy licencyjnej (wymagana)	• 1—W pełni przeczytałem, rozumiem i akceptuję warunki Umowy licencyjnej. • Inna wartość lub brak wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
PRIVACYPOLICY	Akceptacja postanowień i warunków Polityki prywatności (wymagana)	• 1—Jestem świadomy i wyrażam zgodę na przetwarzanie oraz przesyłanie moich danych (również do innych krajów) zgodnie z Polityką prywatności. Potwierdzam, że w pełni przeczytałem(am) i rozumiem Politykę prywatności. • Inna wartość lub bez wartości — Nie akceptuję postanowień i warunków Polityki prywatności (instalacja nie zostanie wykonana).
INSTALLATIONMODETYPE	Typ instalacji Serwera administracyjnego	• Standardowa. • Niestandardowa.
INSTALLDIR	Folder instalacyjny aplikacji	Wartość wiersza.
ADDLOCAL	Lista komponentów przeznaczonych do zainstalowania (oddzielone przecinkami)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Minimalna lista komponentów wystarczających do poprawnego zainstalowania Serwera administracyjnego: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Rozmiar sieci	• NRT_1_100 — od 1 do 100 urządzeń. • NRT_100_1000 — od 101 do 1000 urządzeń. • NRT_GREATER_1000 — więcej niż 1000 urządzeń.
SRV_ACCOUNT_TYPE	Sposób określania użytkownika dla działania usługi Serwera administracyjnego	• SrvAccountDefault—konto użytkownika zostanie utworzone automatycznie • SrvAccountUser—konto użytkownika jest określane ręcznie
SERVERACCOUNTNAME	Nazwa użytkownika dla usługi	Wartość wiersza.
SERVERACCOUNTPWD	Hasło użytkownika dla usługi	Wartość wiersza.
DBTYPE	Typ bazy danych	• MySQL—używana będzie baza danych MySQL lub MariaDB. • MSSQL—używana będzie baza danych Microsoft SQL Server (SQL Express).
MYSQLSERVERNAME	Pełna nazwa serwera MySQL lub MariaDB	Wartość wiersza.
MYSQLSERVERPORT	Numer portu używanego do nawiązania połączenia z serwerem MySQL lub MariaDB	Wartość numeryczna.
MYSQLDBNAME	Nazwa bazy danych serwera MySQL lub MariaDB	Wartość wiersza.
MYSQLACCOUNTNAME	Nazwa użytkownika nawiązującego połączenie z bazą danych serwera MySQL lub MariaDB	Wartość wiersza.
MYSQLACCOUNTPWD	Hasło użytkownika nawiązującego połączenie z bazą danych serwera MySQL lub MariaDB	Wartość wiersza.
MSSQLCONNECTIONTYPE	Sposób użycia bazy danych MSSQL	• InstallMSSEE—instalacja z pakietu • ChooseExisting—użycie zainstalowanego serwera
MSSQLSERVERNAME	Pełna nazwa instancji serwera SQL	Wartość wiersza.
MSSQLDBNAME	Nazwa bazy danych serwera SQL	Wartość wiersza.
MSSQLAUTHTYPE	Metoda autoryzacji podczas nawiązywania połączenia z serwerem SQL	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Nazwa użytkownika nawiązującego połączenie z serwerem SQL w trybie SQLServer	Wartość wiersza.

Właściwość MSI	Opis	Dostępne wartości
MSSQLACCOUNTPWD	Hasło użytkownika nawiązującego połączenie z serwerem SQL w trybie SQLServer	Wartość wiersza.
CREATE_SHARE_TYPE	Metoda określania folderu współdzielonego	• Create—tworzy nowy folder współdzielony. W takim przypadku należy zdefiniować następujące właściwości: • SHARELOCALPATH—ścieżka dostępu do folderu lokalnego. • SHAREFOLDERNAME—nazwa sieciowa folderu. • Null—należy określić właściwość EXISTSHAREFOLDERNAME.
EXISTSHAREFOLDERNAME	Pełna ścieżka dostępu do istniejącego folderu współdzielonego	Wartość wiersza.
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	Wartość numeryczna.
SERVERSSLPORT	Numer portu używanego do nawiązania bezpiecznego połączenia SSL z Serwerem administracyjnym	Wartość numeryczna.
SERVERADDRESS	Adres Serwera administracyjnego	Wartość wiersza.
SERVERCERT2048BITS	Długość klucza certyfikatu Serwera administracyjnego (bity)	• 1—długość klucza certyfikatu Serwera administracyjnego wynosi 2048 bity. • 0 — długość klucza certyfikatu Serwera administracyjnego wynosi 1024 bity. • Jeśli nie określono wartości, długość klucza certyfikatu Serwera administracyjnego wynosi 2048 bity.
MOBILESERVERADDRESS	Adres Serwera administracyjnego do nawiązywania połączenia z urządzeniami mobilnymi; ignorowane, jeśli nie wybrano komponentu MobileSupport	Wartość wiersza.

Parametry instalacji Agenta sieciowego

Poniższa tabela opisuje właściwości MSI, które można skonfigurować podczas instalacji Agenta sieciowego. Wszystkie parametry są opcjonalne, za wyjątkiem EULA i SERVERADDRESS.

Parametry instalacji Agenta sieciowego w trybie cichym

Właściwość MSI	Opis	Dostępne wartości
EULA	Akceptacja postanowień i warunków Umowy licencyjnej	• 1—Potwierdzam, że w pełni przeczytałem(-am), rozumiem i akceptuję warunki niniejszej Umowy licencyjnej użytkownika końcowego. • 0—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana). • Bez wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
DONT_USE_ANSWER_FILE	Odczyt ustawień instalacji z pliku odpowiedzi	• 1—Nie używaj. • Inna wartość lub brak wartości—Odczyt.
INSTALLDIR	Ścieżka do folderu instalacyjnego Agenta sieciowego	Wartość wiersza.
SERVERADDRESS	Adres Serwera administracyjnego (wymagane)	Wartość wiersza.
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	Wartość numeryczna.

Właściwość MSI	Opis	Dostępne wartości
SERVERSSLPORT	Numer portu dla szyfrowanego połączenia z Serwerem administracyjnym przy użyciu protokołu SSL	Wartość numeryczna.
USESSL	Czy użyć połączenia SSL	• 1—użyj. • Inna wartość lub brak wartości—nie używaj.
OPENUDPPORT	Czy otworzyć port UDP	• 1—otwórz. • Inna wartość lub brak wartości—nie otwieraj.
UDPPORT	Numer portu UDP	Wartość numeryczna.
USEPROXY	Czy użyć serwera proxy. Ze względu na kompatybilność nie zaleca się określania ustawień połączenia proxy w ustawieniach pakietu instalacyjnego Agenta sieciowego.	• 1—użyj. • Inna wartość lub brak wartości—nie używaj.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Adres proxy i numer portu używanego do nawiązania połączenia z serwerem proxy	Wartość wiersza.
PROXYLOGIN	Konto używane do nawiązywania połączenia z serwerem proxy	Wartość wiersza.
PROXYPASSWORD	Hasło do konta dla połączenia z serwerem proxy (W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.)	Wartość wiersza.
GATEWAYMODE	Tryb użycia bramy połączenia	• 0—nie używaj bramy połączenia. • 1—użyj tego Agenta sieciowego jako bramy połączenia. • 2—połącz z Serwerem administracyjnym przy użyciu bramy połączenia.
GATEWAYADDRESS	Adres bramy połączenia	Wartość wiersza.
CERTSELECTION	Metoda pobierania certyfikatu	• GetOnFirstConnection—uzyskaj certyfikat z Serwera administracyjnego. • GetExistent—wybierz istniejący certyfikat. Jeśli ta opcja zostanie wybrana, należy określić właściwość CERTFILE.
CERTFILE	Ścieżka do pliku certyfikatu	Wartość wiersza.
VMVDI	Włącz tryb dynamiczny dla wirtualnej infrastruktury pulpitu Virtual Desktop Infrastructure (VDI).	• 1—włącz. • 0—nie włączaj. • Brak wartości—nie włączaj.
VMOPTIMIZE	Czy ustawienia Agenta sieciowego są optymalne dla hiperwizora	• 1—włącz. • 0—nie włączaj. • Brak wartości—nie włączaj.
LAUNCHPROGRAM	Czy uruchomić usługę Agenta sieciowego po instalacji. Parametr jest ignorowany, jeśli VMVDI=1	• 1—uruchom. • Inna wartość lub brak wartości—nie uruchamiaj.
NAGENTTAGS	Znacznik dla Agenta sieciowego (ma priorytet nad znacznikiem podanym w pliku odpowiedzi)	Wartość wiersza.

Infrastruktura wirtualna

Kaspersky Security Center obsługuje użycie maszyn wirtualnych. Możesz zainstalować Agenta sieciowego i aplikację zabezpieczającą na każdej maszynie wirtualnej, a także wdrożyć ochronę maszyn wirtualnych na poziomie hipernadzorcy. W pierwszym przypadku, do ochrony maszyn wirtualnych możesz użyć standardowej aplikacji zabezpieczającej lub Kaspersky Security for Virtualization Light Agent. W drugim przypadku możesz użyć Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center obsługuje przywracanie maszyn wirtualnych do ich poprzedniego stanu.

Wskazówki dotyczące zmniejszenia obciążenia na maszynach wirtualnych

Podczas instalacji Agenta sieciowego na maszynie wirtualnej zalecane jest rozważenie wyłączenia funkcji Kaspersky Security Center, które nie będą zbyt przydatne dla maszyn wirtualnych.

Podczas instalacji Agenta sieciowego na maszynie wirtualnej lub na szablonie przeznaczonym do wygenerowania maszyn wirtualnych, zalecane jest wykonanie następujących czynności:

- Jeśli uruchamiasz zdalną instalację, w oknie właściwości pakietu instalacyjnego Agenta sieciowego, w sekcji **Zaawansowane** zaznacz opcję **Optymalizuj ustawienia dla VDI**.
- Jeśli uruchamiasz instalację w trybie interaktywnym z udziałem kreatora, w oknie kreatora zaznacz opcję **Optymalizuj ustawienia Agenta sieciowego dla infrastruktury wirtualnej**.

Zaznaczenie tych opcji spowoduje zmianę ustawień Agenta sieciowego w taki sposób, że poniższe funkcje pozostaną domyślnie wyłączone (przed zastosowaniem zasady):

- Zbieranie informacji o zainstalowanym oprogramowaniu
- Zbieranie informacji o sprzęcie
- Zbieranie informacji o wykrytych lukach
- Zbieranie informacji o wymaganych aktualizacjach

Zazwyczaj te funkcje nie są potrzebne na maszynach wirtualnych, gdyż wykorzystują stałe oprogramowanie i sprzęt wirtualny.

Wyłączenie tych funkcji jest odwracalne. Jeśli jakakolwiek z wyłączonych funkcji jest potrzebna, możesz ją włączyć poprzez zasadę Agenta sieciowego lub poprzez ustawienia lokalne Agenta sieciowego. Ustawienia lokalne Agenta sieciowego są dostępne poprzez menu kontekstowe odpowiedniego urządzenia w Konsoli administracyjnej.

Obsługa dynamicznych maszyn wirtualnych

Kaspersky Security Center obsługuje dynamiczne maszyny wirtualne. Jeśli w sieci organizacji została wdrożona infrastruktura wirtualna, w pewnych przypadkach możliwe będzie korzystanie z dynamicznych (tymczasowych) maszyn wirtualnych. Dynamiczne maszyny wirtualne są tworzone pod unikatowymi nazwami w oparciu o szablony, które zostały przygotowane przez administratora. Użytkownik pracuje na maszynie wirtualnej przez jakiś czas, a następnie, po wyłączeniu maszyny zostanie ona usunięta z infrastruktury wirtualnej. Jeśli w sieci organizacji jest zainstalowany program Kaspersky Security Center, maszyna wirtualna z zainstalowanym Agentem sieciowym zostanie dodana do bazy danych Serwera administracyjnego. Po wyłączeniu maszyny wirtualnej, odpowiedni wpis musi także zostać usunięty z bazy danych Serwera administracyjnego.

Aby funkcja automatycznego usuwania wpisów na temat maszyn wirtualnych mogła działać, podczas instalacji Agenta sieciowego na szablonie dla dynamicznych maszyn wirtualnych wybierz opcję **Włącz tryb dynamiczny VDI**:

- Dla zdalnej instalacji—w oknie właściwości pakietu instalacyjnego Agenta sieciowego (sekcja **Zaawansowane**)
- Dla instalacji w trybie interaktywnym—w Kreatorze instalacji Agenta sieciowego

Staraj się unikać zaznaczania opcji **Włącz tryb dynamiczny VDI** podczas instalacji Agenta sieciowego na urządzeniach fizycznych.

Jeśli chcesz, żeby zdarzenia z dynamicznych maszyn wirtualnych były przechowywane na Serwerze administracyjnym przez jakiś czas po usunięciu tych maszyn wirtualnych, w oknie właściwości Serwera administracyjnego, w sekcji **Repozytorium zdarzeń** wybierz opcję **Przechowuj zdarzenia po usunięciu urządzeń** i określ maksymalny czas przechowywania zdarzeń (w dniach).

Nie zalecamy włączania szyfrowania dysku na dynamicznych maszynach wirtualnych.

Obsługa kopiowania maszyn wirtualnych

Kopiowanie maszyn wirtualnych z zainstalowanym Agentem sieciowym lub tworzenie maszyny wirtualnej z szablonu z zainstalowanym Agentem sieciowym odbywa się w ten sam sposób co zdalna instalacja Agenta sieciowego poprzez przechwycenie i skopiowanie obrazu dysku twardego. Oznacza to, że podczas kopiowania maszyn wirtualnych należy wykonać te same czynności, co podczas instalacji Agenta sieciowego poprzez skopiowanie obrazu dysku.

Jednakże dwa poniższe przypadki przedstawiają sytuacje, gdy Agent sieciowy automatycznie wykrywa kopiowanie. Dzięki temu nie ma potrzeby wykonywania wszystkich skomplikowanych działań wymienionych w sekcji "Wdrożenie poprzez przechwycenie i skopiowanie obrazu dysku twardego urządzenia":

- Opcja **Włącz tryb dynamiczny VDI** została wybrana po zainstalowaniu Agenta sieciowego - po każdym ponownym uruchomieniu systemu operacyjnego ta maszyna wirtualna będzie rozpoznawana jako nowe urządzenie, niezależnie od tego, czy została skopiowana.
- Używany jest jeden z następujących hipernadzorców: VMware™, HyperV® lub Xen®: Agent sieciowy wykrywa kopiowanie maszyny wirtualnej po zmienionych numerach ID sprzętu wirtualnego.

Analiza zmian w sprzęcie wirtualnym nie jest całkowicie wiarygodna. Przed szerszym zastosowaniem tej metody należy ją sprawdzić na małej puli maszyn wirtualnych dla wersji hipernadzorcy, który jest aktualnie używany w organizacji.

Obsługa przywracania systemu plików dla urządzeń z zainstalowanym Agentem sieciowym

Kaspersky Security Center jest aplikacją oferującą wiele funkcji. Przywrócenie poprzedniego stanu systemu plików na urządzeniu z zainstalowanym Agentem sieciowym doprowadzi do desynchronizacji danych i niepoprawnego działania Kaspersky Security Center.

Wycofanie systemu plików (lub jego części) może zostać wykonane w następujących przypadkach:

- Podczas kopiowania obrazu dysku twardego.
- Podczas przywracania stanu maszyny wirtualnej przy użyciu infrastruktury wirtualnej.
- Podczas przywracania danych z kopii zapasowej lub punktu odzyskiwania.

Scenariusze, w których oprogramowanie firm trzecich na urządzeniach z zainstalowanym Agentem sieciowym wpływa na zawartość folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\, są dla Kaspersky Security Center tylko krytycznymi scenariuszami. Dlatego też, jeśli to tylko możliwe, powinieneś zawsze wykluczać ten folder z procedury odzyskiwania.

Ponieważ zasady działania niektórych organizacji dopuszczają możliwość wycofania systemu plików urządzeń, obsługa wycofania systemu plików na urządzeniach z zainstalowanym Agentem sieciowym jest dostępna w Kaspersky Security Center od wersji 10 Maintenance Release 1 (Serwer administracyjny i Agenty sieciowe muszą być w wersjach 10 Maintenance Release 1 lub nowszych). Po wykryciu takich urządzeń są one automatycznie ponownie łączone z Serwerem administracyjnym z całkowitym wyczyszczeniem danych i pełną synchronizacją.

Domyślnie obsługa wykrywania wycofania systemu plików jest włączona w Kaspersky Security Center 15.1.

Jeśli jest to tylko możliwe, unikaj przywracania poprzedniego stanu folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ na urządzeniach z zainstalowanym Agentem sieciowym, gdyż całkowita ponowna synchronizacja danych zużywa dużą ilość zasobów.

Wycofanie stanu systemu jest całkowicie zabronione na urządzeniu z zainstalowanym Serwerem administracyjnym. Podobnie jest w przypadku wycofania baz danych używanych przez Serwer administracyjny.

Możesz przywrócić stan Serwera administracyjnego z kopii zapasowej tylko przy użyciu standardowego narzędzia klbackup.

Lokalna instalacja aplikacji

Sekcja ta opisuje procedurę instalacji aplikacji, które można zainstalować tylko na urządzeniach lokalnych.

Aby przeprowadzić lokalną instalację aplikacji na określonym urządzeniu klienckim, musisz mieć uprawnienia administratora na tym urządzeniu.

W celu zainstalowania aplikacji lokalnie na określonym urządzeniu klienckim:

1. Zainstaluj Agenta sieciowego na urządzeniu klienckim i skonfiguruj połączenie pomiędzy urządzeniem klienckim a Serwerem administracyjnym.

2. Zainstaluj wymagane aplikacje na urządzeniu zgodnie z opisem w dokumentacji tych aplikacji.

3. Na stacji roboczej administratora zainstaluj wtyczkę zarządzającą dla każdej z zainstalowanych aplikacji.

Kaspersky Security Center obsługuje również opcję lokalnej instalacji aplikacji przy pomocy autonomicznych pakietów instalacyjnych. Kaspersky Security Center nie obsługuje instalacji wszystkich aplikacji Kaspersky.

Lokalna instalacja Agenta sieciowego

W celu zainstalowania Agenta sieciowego lokalnie:

1. Na urządzeniu uruchom plik setup.exe z pakietu dystrybucyjnego pobranego z Internetu. Aby uzyskać szczegółowe informacje, zapoznaj się z następującym tematem: Pobieranie pakietu instalacyjnego Agenta sieciowego z zestawu dystrybucyjnego Kaspersky Security Center.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania.

2. W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj tylko Agenta sieciowego Kaspersky Security Center**, aby uruchomić kreatora instalacji Agenta sieciowego. Postępuj zgodnie z instrukcjami kreatora.

a. **Serwer administracyjny**

Port

Określa port inny niż SSL używany przez Serwer administracyjny do odbierania połączeń od Agentów sieciowych.

Domyślnie ta opcja jest ustawiona na 14 000.

Port SSL

Określa port SSL używany przez Serwer administracyjny do otrzymywania połączeń od Agentów sieciowych.

Domyślnie ta opcja jest ustawiona na 13 000.

Użyj SSL przy połączeniu z Serwerem administracyjnym

Jeśli ta opcja jest włączona, połączenie z Serwerem administracyjnym jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

Domyślnie opcja ta jest włączona.

Zezwól Agentowi sieciowemu na otwarcie portu UDP

Jeśli ta opcja jest włączona, instalator automatycznie otwiera port używany przez Serwer administracyjny do zarządzania urządzeniem klienckim i otrzymywania informacji o nim.

Domyślnie opcja ta jest włączona.

Port UDP

Umożliwia skonfigurowanie portu używanego przez Serwer administracyjny do zarządzania urządzeniem klienckim i otrzymywania informacji o nim.

Domyślnie ta opcja jest ustawiona na 15 000.

b. **Konfiguracja serwera proxy**

Użyj serwera proxy

Jeśli ta opcja jest włączona, możesz określić poświadczenia do uwierzytelniania serwera proxy.

Zalecamy określenie poświadczeń konta, które ma minimalne uprawnienia wymagane tylko do uwierzytelnienia serwera proxy.

Domyślnie opcja ta jest wyłączona.

Adres

Port

Konto

Nazwa użytkownika konta z poziomu którego nawiązywane jest połączenie z serwerem proxy.

Zalecamy określenie poświadczeń konta, które ma minimalne uprawnienia wymagane tylko do uwierzytelnienia serwera proxy.

Hasło

Hasło do konta, z poziomu którego nawiązywane jest połączenie z serwerem proxy.

Zalecamy określenie poświadczeń konta, które ma minimalne uprawnienia wymagane tylko do uwierzytelnienia serwera proxy.

c. **Brama połączenia**

Nie używaj bramy połączenia

Użyj Agenta sieciowego jako bramy połączenia w DMZ

Wybierz tę opcję, aby użyć Agenta sieciowego jako bramy połączenia w strefie zdemilitaryzowanej (DMZ), aby połączyć się z Serwerem administracyjnym, komunikować się z nim i bezpiecznie przechowywać dane w Agencie sieciowym podczas transmisji danych.

Połącz z Serwerem administracyjnym korzystając z bramy połączenia

Wybierz tę opcję, a następnie określ urządzenie, które będzie pełnić rolę bramy połączenia.

d. **Certyfikat Serwera administracyjnego**

e. **Znaczniki Agenta**

f. **Ustawienia zaawansowane**

Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany

Zalecamy pozostawienie tej opcji włączonej. Możesz wyczyścić tę opcję, aby wyłączyć automatyczne aktualizowanie i instalowanie poprawek dla komponentów Kaspersky Security Center. Administrator może włączyć funkcję automatycznego aktualizowania i instalowania poprawek w późniejszym czasie, korzystając z zasady.

Domyślnie opcja ta jest wyłączona.

Włącz ochronę usługi Agenta sieciowego

Gdy ta opcja pozostaje aktywna, po zainstalowaniu Agenta sieciowego na zarządzanym urządzeniu, składnik nie może zostać usunięty ani ponownie skonfigurowany bez wymaganych uprawnień. Usługa Agenta sieciowego nie może zostać zatrzymana. Ta opcja nie ma wpływu na kontrolery domeny.

Włącz tę opcję, aby chronić Agenta sieciowego na stacjach roboczych obsługiwanych z uprawnieniami lokalnego administratora.

Domyślnie opcja ta jest wyłączona.

Włącz tryb dynamiczny VDI

Jeżeli ta opcja jest włączona, tryb dynamiczny Virtual Desktop Infrastructure (VDI) będzie włączony dla Agenta sieciowego, zainstalowanego na maszynie wirtualnej.

Domyślnie opcja ta jest wyłączona.

Zoptymalizuj ustawienia Agenta sieciowego Kaspersky Security Center dla VDI. Wyłącz wykrywanie luk oraz inwentaryzację aplikacji i sprzętu. Możesz edytować bieżące ustawienia poprzez zasady Agenta sieciowego.

Jeśli ta opcja jest włączona, w ustawieniach Agenta sieciowego będą wyłączone następujące funkcje:

- Zbieranie informacji o zainstalowanym oprogramowaniu
- Zbieranie informacji o sprzęcie
- Zbieranie informacji o wykrytych lukach
- Zbieranie informacji o wymaganych aktualizacjach

Domyślnie opcja ta jest wyłączona.

g. **Uruchom aplikację**

Po zakończeniu działania kreatora instalacji, na urządzeniu zostanie zainstalowany Agent sieciowy.

Możesz wyświetlić właściwości usługi Agenta sieciowego Kaspersky Security Center; możesz także uruchamiać, zatrzymywać i monitorować aktywność Agenta sieciowego, korzystając ze standardowych narzędzi Microsoft Windows: Zarządzanie komputerem\Usługi.

Instalowanie Agenta sieciowego w trybie cichym

Agent sieciowy może zostać zainstalowany w trybie cichym, czyli bez interaktywnego wprowadzania parametrów instalacji. W trybie cichej instalacji używany jest instalator Windows (MSI) dla Agenta sieciowego. Plik MSI znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center, w folderze Packages\NetAgent\exec.

Nie zmieniaj nazwy pakietu instalacyjnego Kaspersky Network Agent.msi. Zmiana nazwy tego pakietu może spowodować błędy instalacji podczas przyszłych aktualizacji Agenta sieciowego.

Instalacja Agenta sieciowego z pakietu MSI możliwa jest tylko w trybie cichym, instalacja interaktywna z pakietu MSI nie jest obsługiwana.

W celu zainstalowania Agenta sieciowego na urządzeniu lokalnym w trybie cichym:

1. Przeczytaj Umowę licencyjną użytkownika końcowego. Użyj poniższego polecenia tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

2. Uruchom polecenie

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```

   gdzie `setup_parameters` to lista parametrów i ich odpowiednich wartości oddzielonych spacjami (`PROP1=PROP1VAL PROP2=PROP2VAL`).

Na liście parametrów będziesz musiał uwzględnić `EULA=1`. W przeciwnym razie Agent sieciowy nie zostanie zainstalowany.

Jeśli używasz standardowych ustawień połączenia dla Kaspersky Security Center oraz Agenta sieciowego na zdalnych urządzeniach, uruchom polecenie:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` to klucz do zapisywania raportów. Dziennik jest tworzony podczas instalacji Agenta sieciowego i zapisywany w C:\windows\temp\nag_inst.log.

Oprócz nag_inst.log aplikacja tworzy plik $klssinstlib.log, który zawiera dziennik instalacji. Ten plik jest przechowywany w folderze %windir%\temp lub %temp%. Do celów rozwiązywania problemów użytkownik lub specjalista z pomocy technicznej Kaspersky może potrzebować obu plików dziennika - nag_inst.log i $klssinstlib.log.

Jeśli chcesz dodatkowo określić port połączenia z Serwerem administracyjnym, uruchom polecenie:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

Parametr `SERVERPORT` odpowiada numerowi portu połączenia z Serwerem administracyjnym.

Nazwy i możliwe wartości parametrów, które mogą zostać użyte podczas instalacji Agenta sieciowego w trybie cichym znajdują się w sekcji Parametry instalacji Agenta sieciowego.

Jeśli chcesz uaktualnić Agenta sieciowego za pomocą Instalatora Windows, uruchom następujące polecenie:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Instalowanie Agenta sieciowego dla systemu Linux w trybie cichym (z plikiem odpowiedzi)

Możesz zainstalować Agenta sieciowego na urządzeniach Linux przy użyciu pliku odpowiedzi—pliku tekstowego, który zawiera niestandardowy zestaw parametrów instalacji: zmienne i ich odpowiednie wartości. Korzystanie z tego pliku odpowiedzi umożliwia uruchomienie instalacji w trybie cichym, czyli bez udziału użytkownika.

W celu przeprowadzenia instalacji Agenta sieciowego dla systemu Linux w trybie cichym:

1. Przygotuj odpowiednie urządzenie Linux do zdalnej instalacji. Pobierz i utwórz pakiet zdalnej instalacji, używając pakietu .deb lub .rpm Agenta sieciowego, korzystając z dowolnego odpowiedniego systemu do zarządzania pakietami.

2. Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym SUSE Linux Enterprise Server 15, w pierwszej kolejności zainstaluj pakiet insserv-compat, aby skonfigurować Agenta sieciowego.

   Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym RED OS 7.3.4 lub nowszym albo MSVSPHERE 9.2 lub nowszym, zainstaluj pakiet libxcrypt-compat, aby Agent sieciowy działał prawidłowo.

3. Przeczytaj Umowę licencyjną użytkownika końcowego. Wykonaj poniższe kroki tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

4. Utwórz plik odpowiedzi (w formacie TXT). Do plików z odpowiedziami dodaj listę zmiennych w formacie VARIABLE_NAME=variable_value, każda zmienna musi być w oddzielnym wierszu.

W celu poprawnego korzystania z pliku odpowiedzi, musisz umieścić go w minimalnym zestawie trzech wymaganych zmiennych:

- KLNAGENT_SERVER
- KLNAGENT_AUTOINSTALL
- EULA_ACCEPTED

Możesz także dodać dowolne opcjonalne zmienne, aby korzystać z bardziej określonych parametrów zdalnej instalacji. Poniższa tabela wyświetla listy zmiennych, które mogą znajdować się w pliku odpowiedzi:

Zmienne pliku odpowiedzi użyte jako parametry instalacji Agenta sieciowego dla systemu Linux w trybie cichym

Zmienne pliku odpowiedzi użyte jako parametry instalacji Agenta sieciowego dla systemu Linux w trybie cichym

Nazwa zmiennej	Wymagane	Opis	Możliwe wartości
KLNAGENT_SERVER	Tak	Zawiera nazwę Serwera administracyjnego przedstawioną jako w pełni kwalifikowaną nazwę domeny (FQDN) lub adres IP.	Nazwa DNS lub adres IP.
KLNAGENT_AUTOINSTALL	Tak	Definiuje, czy tryb cichej instalacji jest włączony.	1—Tryb cichy jest włączony; użytkownik nie zostanie zapytany o żadne działania podczas instalacji. Inna—Tryb cichy jest wyłączony; użytkownik może zostać zapytany o działania podczas instalacji.
EULA_ACCEPTED	Tak	Definiuje, czy użytkownik akceptuje Umowę licencyjną użytkownika końcowego Agenta sieciowego; jeśli brakuje wartości, może być interpretowane jako brak zgody na Umowę licencyjną użytkownika końcowego.	1—Potwierdzam, że w pełni przeczytałem(-am), rozumiem i akceptuję warunki niniejszej Umowy licencyjnej użytkownika końcowego. Inna wartość lub bez wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
KLNAGENT_PROXY_USE	Nie	Definiuje, czy połączenie z Serwerem administracyjnym będzie używało ustawień serwera proxy. Domyślna wartość to 0.	1—Ustawienia proxy są używane. Inna—Ustawienia proxy nie są używane.
KLNAGENT_PROXY_ADDR	Nie	Definiuje adres serwera proxy używany do nawiązania połączenia z Serwerem administracyjnym.	Nazwa DNS lub adres IP.
KLNAGENT_PROXY_LOGIN	Nie	Definiuje nazwę użytkownika użytą do zalogowania się do serwera proxy.	Dowolna istniejąca nazwa użytkownika.
KLNAGENT_PROXY_PASSWORD	Nie	Definiuje hasło użytkownika użyte do zalogowania się do serwera proxy.	Dowolny zestaw znaków alfanumerycznych dozwolonych przez format hasła w systemie operacyjnym.
KLNAGENT_VM_VDI	Nie	Definiuje, czy Agent sieciowy jest zainstalowany na obrazie do utworzenia dynamicznych maszyn wirtualnych.	1—Agent sieciowy jest zainstalowany na obrazie, który jest używany jednocześnie do utworzenia dynamicznych maszyn wirtualnych. Inna—Podczas instalacji nie jest używany żaden obraz.

KLNAGENT_VM_OPTIMIZE	Nie	Definiuje, czy ustawienia Agenta sieciowego są optymalne dla hipernadzorcy.	1—Domyślne ustawienia lokalne Agenta sieciowego są modyfikowane w taki sposób, że zezwalają na zoptymalizowane użycie na hipernadzorcy.
KLNAGENT_TAGS	Nie	Wyświetla znaczniki przypisane do instancji Agenta sieciowego.	Jedna lub kilka nazw znaczników oddzielonych średnikami.
KLNAGENT_UDP_PORT	Nie	Definiuje port UDP użyty przez Agenta sieciowego. Domyślna wartość to 15000.	Dowolny istniejący numer portu.
KLNAGENT_PORT	Nie	Definiuje port nie będący TLS, użyty przez Agenta sieciowego. Domyślna wartość to 14000.	Dowolny istniejący numer portu.
KLNAGENT_SSLPORT	Nie	Definiuje port TLS, użyty przez Agenta sieciowego. Domyślna wartość to 13000.	Dowolny istniejący numer portu.
KLNAGENT_USESSL	Nie	Definiuje, czy port Transport Layer Security (TLS) jest używany do nawiązywania połączenia.	1 (domyślna)—TLS jest używany. Inna—TLS nie jest używany.
KLNAGENT_GW_MODE	Nie	Definiuje, czy brama połączenia jest używana.	1 (domyślna)—Bieżące ustawienia nie są modyfikowane (przy pierwszym połączeniu określona jest brama połączenia). 2—Nie jest używana brama połączenia. 3—Brama połączenia jest używana. Wymagany jest KLNAGENT_GW_ADDRESS. 4—Instancja Agenta sieciowego jest używana jako brama połączenia w strefie zdemilitaryzowanej (DMZ). Wymagany jest certyfikat serwera.
KLNAGENT_GW_ADDRESS	Nie	Definiuje adres bramy połączenia. Wartość jest stosowana tylko wtedy, gdy KLNAGENT_GW_MODE=3.	Nazwa DNS lub adres IP.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Nie	Umożliwia uruchomienie rejestracji użytkownika jako narzędzia właściciela urządzenia po instalacji Agenta sieciowego. Jeśli opcja jest wyłączona, rejestracja jako właściciela urządzenia nie jest dostępna dla użytkownika.	1 — Narzędzie rejestracji użytkownika jako właściciela urządzenia zostanie uruchomione po zainstalowaniu Agenta sieciowego. Inne — wyłączone.

5. Uruchom instalację Agenta sieciowego. Zmienna środowiskowa KLAUTOANSWERS, która określa ścieżkę do pliku odpowiedzi, jest przekazywana do polecenia instalacji. Uruchom jedno z następujących poleceń:

   - Aby zainstalować Agenta sieciowego z pakietu RPM w 32-bitowym systemie operacyjnym, wykonaj następujące polecenie:
     `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> yum install ./klnagent-<numer kompilacji>.i386.rpm`

   - Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym, wykonaj następujące polecenie:
     `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> yum install ./klnagent64-<numer kompilacji>.x86_64.rpm`

- Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym dla architektury Arm, wykonaj następujące polecenie:
  `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> yum install ./klnagent64-<numer kompilacji>.aarch64.rpm`

- Aby zainstalować Agenta sieciowego z pakietu DEB w 32-bitowym systemie operacyjnym, wykonaj następujące polecenie:
  `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> apt install ./klnagent_<numer kompilacji>_i386.deb`

- Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym, wykonaj następujące polecenie:
  `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> apt install ./klnagent64_<build number>_amd64.deb`

- Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym dla architektury Arm, wykonaj następujące polecenie:
  `sudo KLAUTOANSWERS=<ścieżka do pliku odpowiedzi> apt install ./klnagent64_<numer kompilacji>_arm64.deb`

W zależności od konfiguracji systemu operacyjnego, możesz również użyć menedżerów pakietów rpm, dpkg lub dnf, aby zainstalować Agenta sieciowego.

Instalacja Agenta sieciowego dla systemu Linux zostanie uruchomiona w trybie cichym; użytkownik nie zostanie zapytany o żadne działania podczas procesu.

Przygotowanie urządzenia z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania do instalacji Agenta sieciowego

Przed instalacją Agenta sieciowego na urządzeniu z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania należy wykonać dwie procedury przygotowawcze — tę opisaną w instrukcjach poniżej i ogólne kroki przygotowania dla dowolnego urządzenia z systemem Linux.

> W wierszu poleceń uruchom polecenia podane w tej instrukcji na koncie z uprawnieniami administratora.

Przygotowanie urządzenia z systemem Astra Linux w trybie zamkniętego środowiska oprogramowania do instalacji Agenta sieciowego:

1. Otwórz plik `/etc/digsig/digsig_initramfs.conf` a następnie określ następujące ustawienie:
   `DIGSIG_ELF_MODE=1`

2. W wierszu polecenia uruchom następujące polecenie, aby zainstalować pakiet zgodności:
   `apt install astra-digsig-oldkeys`

3. Utwórz katalog dla klucza aplikacji:
   `mkdir -p /etc/digsig/keys/legacy/kaspersky/`

4. Umieść klucz aplikacji /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg w katalogu utworzonym w poprzednim kroku:
   `cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/`

Jeśli pakiet dystrybucyjny Kaspersky Security Center nie zawiera klucza aplikacji kaspersky_astra_pub_key.gpg, możesz go pobrać, klikając łącze: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Zaktualizuj dyski RAM:

   ```
   update-initramfs -u -k all
   ```

   Uruchom ponownie system.

Urządzenie z systemem Linux jest gotowe do instalacji Agenta sieciowego. Możesz zainstalować Agenta sieciowego zdalnie, w trybie interaktywnym lub w trybie cichym.

Instalowanie Agenta sieciowego dla systemu Linux w trybie interaktywnym

W tym artykule opisano, jak zainstalować Agenta sieciowego na urządzeniach z systemem Linux w trybie interaktywnym, określając krok po kroku parametry instalacji. Alternatywnie możesz użyć pliku odpowiedzi — pliku tekstowego, który zawiera niestandardowy zestaw parametrów instalacji: zmienne i ich odpowiednie wartości. Korzystanie z tego pliku odpowiedzi umożliwia uruchomienie instalacji w trybie cichym, czyli bez udziału użytkownika.

Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym RED OS 7.3.4 lub nowszym albo MSVSPHERE 9.2 lub nowszym, zainstaluj pakiet libxcrypt-compat, aby Agent sieciowy działał prawidłowo.

Instalowanie Agenta sieciowego w trybie interaktywnym:

1. Uruchom instalację Agenta sieciowego. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

   - Aby zainstalować Agenta sieciowego z pakietu RPM w 32-bitowym systemie operacyjnym:

     ```
     # yum -i klnagent-<numer kompilacji>.i386.rpm
     ```

   - Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym:

     ```
     # yum -i klnagent64-<numer kompilacji>.x86_64.rpm
     ```

   - Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym dla architektury Arm:

     ```
     # yum -i klnagent64-<numer kompilacji>.aarch64.rpm
     ```

   - Aby zainstalować Agenta sieciowego z pakietu DEB w 32-bitowym systemie operacyjnym:

     ```
     # apt install ./klnagent_<numer kompilacji>_i386.deb
     ```

   - Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym:

     ```
     # apt install ./klnagent64_<numer kompilacji>_amd64.deb
     ```

   - Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym dla architektury Arm:

     ```
     # apt install ./klnagent64_<numer kompilacji>_arm64.deb
     ```

2. Uruchom konfigurację Agenta sieciowego:

   ```
   # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Przeczytaj Umowę licencyjną użytkownika końcowego (EULA). Tekst jest wyświetlany w oknie wiersza poleceń. Naciśnij spację, aby wyświetlić następny segment tekstu. Następnie po wyświetleniu monitu wprowadź jedną z następujących wartości:

   - Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.
   - Wpisz `n`, jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego. Aby korzystać z Agenta sieciowego, musisz zaakceptować warunki Umowy licencyjnej użytkownika końcowego.
   - Wpisz `r`, aby ponownie wyświetlić Umowę licencyjną użytkownika końcowego.

4. Wprowadź nazwę DNS Serwera administracyjnego lub adres IP.
5. Wprowadź numer portu Serwera administracyjnego. Domyślnie wykorzystywany jest port 14000.
6. Wprowadź numer portu SSL Serwera administracyjnego. Domyślnie wykorzystywany jest port 13000.
7. Wpisz `y`, jeśli chcesz używać szyfrowania SSL dla ruchu pomiędzy Agentem sieciowym a Serwerem administracyjnym. W przeciwnym razie wpisz `n`.
8. W celu skonfigurowania Agenta sieciowego wybierz jedną z następujących opcji:

   - `[1]` —nie konfiguruj bramy połączenia.

     Twoje urządzenie nie będzie działać jako brama połączenia i nie będzie łączyć się z Serwerem administracyjnym poprzez bramę połączenia.

   - `[2]` —nie używaj bramy połączenia.

     Twoje urządzenie nie połączy się z Serwerem administracyjnym poprzez bramę połączenia.

   - `[3]` —Nawiąż połączenie z serwerem przy użyciu bramy połączenia.

     Twoje urządzenie połączy się z Serwerem administracyjnym poprzez bramę połączenia.

   - `[4]` —Użyj jako bramy połączenia.

     Twoje urządzenie będzie działać jako brama połączenia.

Agent sieciowy jest zainstalowany na urządzeniu z systemem Linux.

Lokalna instalacja wtyczki zarządzającej aplikacją

W celu zainstalowania wtyczki zarządzającej aplikacją:

Na urządzeniu z zainstalowaną Konsolą administracyjną uruchom plik wykonywalny klcfginst.exe, wchodzący w skład pakietu dystrybucyjnego aplikacji.

Plik klcfginst.exe wchodzi w skład wszystkich aplikacji, którymi można zarządzać poprzez Kaspersky Security Center. Instalacja jest wykonywana przez kreator i nie wymaga ręcznej konfiguracji ustawień.

Instalowanie aplikacji w trybie cichym

W celu zainstalowania aplikacji w trybie cichym:

1. Otwórz okno główne Kaspersky Security Center.
2. W folderze **Zdalna instalacja** drzewa konsoli, w podfolderze **Pakiety instalacyjne** wybierz pakiet instalacyjny odpowiedniej aplikacji lub utwórz nowy pakiet instalacyjny dla tej aplikacji.

   Pakiet instalacyjny będzie przechowywany na Serwerze administracyjnym w folderze Pakiety, który znajduje się w folderze współdzielonym. Każdemu pakietowi instalacyjnemu odpowiada oddzielny podfolder.

3. Otwórz folder, w którym przechowywany jest żądany pakiet instalacyjny, w jeden z następujących sposobów:

   - Skopiuj folder żądanego pakietu instalacyjnego z Serwera administracyjnego na urządzenie klienckie. Następnie otwórz skopiowany folder na urządzeniu klienckim.
   - Z poziomu urządzenia klienckiego otwórz folder współdzielony na Serwerze administracyjnym, który odpowiada wymaganemu pakietowi instalacyjnemu.

   Jeśli folder współdzielony znajduje się na urządzeniu z systemem operacyjnym Microsoft Windows Vista, należy wybrać wartość **Wyłączony** dla ustawienia **Kontrola konta użytkownika: Uruchom wszystkich administratorów w trybie Zatwierdzenie administratora** (**Start** → **Panel sterowania** → **Administracja** → **Zasady zabezpieczeń lokalnych** → **Ustawienia zabezpieczeń**).

4. Następnie, w zależności od wybranej aplikacji:

   - Dla programów Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers oraz Kaspersky Security Center przejdź do podfolderu exec i przy pomocy klucza /s uruchom plik wykonywalny (plik z rozszerzeniem .exe).
   - Dla pozostałych aplikacji firmy Kaspersky, z otwartego folderu, przy pomocy klucza /s uruchom plik wykonywalny (plik z rozszerzeniem .exe).

   Uruchomienie pliku wykonywalnego z kluczami `EULA=1` i `PRIVACYPOLICY=1` oznacza, że w pełni przeczytałeś, zrozumiałeś i akceptujesz warunki, odpowiednio Umowy licencyjnej użytkownika końcowego i Polityki prywatności. Jesteś także świadomy, że Twoje dane będą zarządzane i przesyłane (w tym do innych krajów) w sposób opisany w Polityce prywatności. Treść Umowy licencyjnej i Polityki prywatności znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center. Akceptacja warunków Umowy licencyjnej i Polityki prywatności jest niezbędna do zainstalowania aplikacji lub jej aktualizacji z poprzedniej wersji aplikacji.

Instalowanie aplikacji przy pomocy pakietów autonomicznych

Kaspersky Security Center umożliwia utworzenie autonomicznych pakietów instalacyjnych dla aplikacji. Autonomiczny pakiet instalacyjny jest plikiem wykonywalnym, który można umieścić na serwerze sieciowym, przesłać w wiadomości e-mail lub przenieść na urządzenie klienckie w inny sposób. Możesz uruchomić odebrany plik lokalnie na urządzeniu klienckim i zainstalować aplikację bez udziału Kaspersky Security Center.

Autonomiczny Agent sieciowy dla systemu Linux ma opcjonalną zależność od narzędzia nmap. Jeśli narzędzie nmap jest niedostępne lub ma wersję starszą niż 6.0, funkcja Broadcast DHCP Discover nie jest obsługiwana.

W celu zainstalowania aplikacji przy użyciu autonomicznego pakietu instalacyjnego:

1. Nawiąż połączenie z żądanym Serwerem administracyjnym.
2. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
3. W obszarze roboczym wybierz pakiet instalacyjny wymaganej aplikacji.
4. Uruchom proces tworzenia autonomicznego pakietu instalacyjnego, korzystając z jednej z następujących metod:
   - Wybierając **Utwórz autonomiczny pakiet instalacyjny** z menu kontekstowego pakietu instalacyjnego.
   - Klikając odnośnik **Utwórz autonomiczny pakiet instalacyjny** w obszarze roboczym pakietu instalacyjnego.

   Zostanie uruchomiony Kreator tworzenia autonomicznego pakietu instalacyjnego. Postępuj zgodnie z instrukcjami kreatora.

   W ostatnim kroku kreatora wybierz metodę przesłania autonomicznego pakietu instalacyjnego na urządzenie klienckie.
5. Prześlij autonomiczny pakiet instalacyjny na urządzenie klienckie.
6. Uruchom autonomiczny pakiet instalacyjny na urządzeniu klienckim.

Aplikacja zostanie zainstalowana na urządzeniu klienckim z ustawieniami określonymi w pakiecie autonomicznym.

Po utworzeniu autonomicznego pakietu instalacyjnego, jest on automatycznie publikowany na serwerze sieciowym. Odnośnik do pobrania pakietu autonomicznego jest wyświetlany na liście utworzonych autonomicznych pakietów instalacyjnych. Jeśli to konieczne, możesz anulować publikację wybranego pakietu autonomicznego i opublikować go ponownie na serwerze sieciowym. Domyślnie, do pobrania autonomicznych pakietów instalacyjnych wykorzystywany jest port 8060.

Ustawienia pakietu instalacyjnego Agenta sieciowego

W celu skonfigurowania pakietu instalacyjnego Agenta sieciowego:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.

   Domyślnie folder **Zdalna instalacja** to podfolder folderu **Zaawansowane**.
2. Z menu kontekstowego pakietu instalacyjnego Agenta sieciowego wybierz **Właściwości**.

Zostanie otwarte okno właściwości pakietu instalacyjnego Agenta sieciowego.

Ogólne

Sekcja **Ogólne** wyświetla ogólne informacje o pakiecie instalacyjnym:

- Nazwa pakietu instalacyjnego
- Nazwę i wersję aplikacji, dla której został utworzony pakiet instalacyjny

- Rozmiar pakietu instalacyjnego
- Data utworzenia pakietu instalacyjnego
- Ścieżkę dostępu do folderu pakietu instalacyjnego

Ustawienia

Ta sekcja przedstawia ustawienia wymagane do zapewnienia właściwego działania Agenta sieciowego natychmiast po jego zainstalowaniu. Ustawienia w tej sekcji są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows.

W grupie ustawień **Folder docelowy** możesz wybrać folder na urządzeniu klienckim, w którym zostanie zainstalowany Agent sieciowy.

- **Zainstaluj w folderze domyślnym**

  Jeśli ta opcja jest zaznaczona, Agent sieciowy zostanie zainstalowany w folderze <Dysk>:\Program Files\Kaspersky Lab\NetworkAgent. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie.

  Domyślnie opcja ta jest zaznaczona.

- **Zainstaluj we wskazanym folderze**

  Jeżeli ta opcja jest zaznaczona, Agent sieciowy zostanie zainstalowany w folderze określonym w polu do wprowadzania danych.

W następującej grupie ustawień możesz określić hasło dla zadania zdalnej dezinstalacji Agenta sieciowego:

- **Użyj hasła dezinstalacyjnego**

  Jeśli ta opcja jest włączona, klikając przycisk **Modyfikuj** możesz wprowadzić hasło dezinstalacyjne (dostępne tylko dla Agenta sieciowego na urządzeniach działających pod kontrolą systemów operacyjnych Windows).

  Domyślnie opcja ta jest wyłączona.

- **Stan**

  Stan hasła: **Hasło zostało określone** lub **Hasło nie zostało określone**.

  Domyślnie hasło nie jest ustawione.

- **Chroń usługę Agenta sieciowego przed nieuprawnionym usuwaniem, zatrzymywaniem i zmianami ustawień**

  Gdy ta opcja pozostaje aktywna, po zainstalowaniu Agenta sieciowego na zarządzanym urządzeniu, składnik nie może zostać usunięty ani ponownie skonfigurowany bez wymaganych uprawnień. Usługa Agenta sieciowego nie może zostać zatrzymana. Ta opcja nie ma wpływu na kontrolery domeny.

  Włącz tę opcję, aby chronić Agenta sieciowego na stacjach roboczych obsługiwanych z uprawnieniami lokalnego administratora.

  Domyślnie opcja ta jest wyłączona.

- **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**

  Jeśli ta opcja jest włączona, wszystkie pobrane aktualizacje i poprawki dla Serwera administracyjnego, Agenta sieciowego, Konsoli administracyjnej, serwera iOS MDM zostaną zainstalowane automatycznie.

  Jeśli ta opcja jest wyłączona, wszystkie pobrane uaktualnienia i poprawki zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzono*. Uaktualnienia i łaty ze stanem *Nie zdefiniowano* nie zostaną zainstalowane.

Domyślnie opcja ta jest włączona.

Połączenie

W tej sekcji możesz skonfigurować połączenie Agenta sieciowego z Serwerem administracyjnym. Do nawiązania połączenia możesz użyć protokołu SSL lub UDP. W celu skonfigurowania połączenia, określ następujące ustawienia:

- **Serwer administracyjny**

  Adres urządzenia z zainstalowanym Serwerem administracyjnym.

- **Port**

  Numer portu używanego do nawiązywania połączenia.

- **Port SSL**

  Numer portu używanego do nawiązywania połączenia po protokole SSL.

- **Użyj certyfikatu Serwera**

  Jeśli ta opcja jest włączona, autoryzacja dostępu Agenta sieciowego do Serwera administracyjnego użyje pliku certyfikatu, który możesz określić, klikając przycisk **Przeglądaj**.

  Jeśli ta opcja jest wyłączona, plik certyfikatu zostanie pobrany z Serwera administracyjnego przy pierwszym połączeniu Agenta sieciowego z adresem określonym w polu **Adres serwera**.

  Nie jest zalecane wyłączenie tej opcji, ponieważ automatyczne odbieranie certyfikatu Serwera administracyjnego przez Agenta sieciowego po nawiązaniu połączenia z Serwerem administracyjnym jest uznawane z niebezpieczne.

  Domyślnie pole to jest zaznaczone.

- **Użyj SSL**

  Jeśli ta opcja jest włączona, połączenie z Serwerem administracyjnym jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

  Domyślnie opcja ta jest wyłączona. Zalecamy, aby nie wyłączać tej opcji, aby Twoje połączenie pozostało bezpieczne.

- **Użyj portu UDP**

  Jeżeli ta opcja jest włączona, Agent sieciowy nawiązuje połączenie z Serwerem administracyjnym poprzez port UDP. Pozwala to na zarządzanie urządzeniami klienckimi i otrzymywanie informacji o nich.

  Port UDP, który musi być otwarty na zarządzanych urządzeniach, na których jest zainstalowany Agent sieciowy. Dlatego zalecamy, aby nie wyłączać tej opcji.

  Domyślnie opcja ta jest włączona.

- **Numer portu UDP**

  W tym polu możesz określić port do łączenia Serwera administracyjnego z Agentem sieciowym przy użyciu protokołu UDP.

  Domyślny numer portu UDP to 15000.

- **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows**

  Jeśli ta opcja jest włączona, porty używane przez Agenta sieciowego są dodawane do listy wykluczeń Zapory sieciowej systemu Microsoft Windows.

Domyślnie opcja ta jest włączona.

- **Użyj serwera proxy**

  Jeżeli ta opcja jest włączona, określ parametry serwera proxy:

  - **Adres serwera proxy**
  - **Port serwera proxy**

  Jeżeli Twój serwer proxy wymaga uwierzytelnienia, włącz opcję **Uwierzytelnianie na serwerze proxy** oraz podaj **Nazwa użytkownika** i **Hasło** konta, w ramach którego nawiązywane jest połączenie z serwerem proxy. Zalecamy określenie poświadczeń konta, które ma minimalne uprawnienia wymagane tylko do uwierzytelnienia serwera proxy.

Ze względu na kompatybilność nie zaleca się określania ustawień połączenia proxy w ustawieniach pakietu instalacyjnego Agenta sieciowego.

Zaawansowane

W sekcji **Zaawansowane** możesz skonfigurować sposób korzystania z bramy połączenia. W tym celu możesz wykonać następujące czynności:

- Użyj Agenta sieciowego jako bramy połączenia w strefie zdemilitaryzowanej (DMZ), aby połączyć się z Serwerem administracyjnym, komunikować się z nim i bezpiecznie przechowywać dane w Agencie sieciowym podczas transmisji danych.
- Połącz się z Serwerem administracyjnym przy użyciu bramy połączenia, aby zmniejszyć liczbę połączeń z Serwerem administracyjnym. W takim przypadku wprowadź adres urządzenia, które będzie pełnić funkcję bramy połączenia w polu **Adres bramy połączenia**.
- Skonfiguruj połączenie dla Virtual Desktop Infrastructure (VDI), jeśli sieć obejmuje maszyny wirtualne. W tym celu wykonaj następujące czynności:

  - **Włącz tryb dynamiczny VDI**

    Jeżeli ta opcja jest włączona, tryb dynamiczny Virtual Desktop Infrastructure (VDI) będzie włączony dla Agenta sieciowego, zainstalowanego na maszynie wirtualnej.

    Domyślnie opcja ta jest wyłączona.

  - **Optymalizuj ustawienia dla VDI**

    Jeśli ta opcja jest włączona, w ustawieniach Agenta sieciowego będą wyłączone następujące funkcje:

    - Zbieranie informacji o zainstalowanym oprogramowaniu
    - Zbieranie informacji o sprzęcie
    - Zbieranie informacji o wykrytych lukach
    - Zbieranie informacji o wymaganych aktualizacjach

    Domyślnie opcja ta jest wyłączona.

- **Zezwól na uruchomienie narzędzia rejestracji użytkownika po instalacji Agenta sieciowego**

  Jeżeli ta opcja jest włączona, narzędzie rejestracji użytkownika jako właściciela urządzenia zostanie uruchomione po zainstalowaniu Agenta sieciowego. Domyślnie opcja ta jest wyłączona.

Dodatkowe składniki

W tej sekcji możesz wybrać dodatkowe komponenty do jednoczesnego zainstalowania z Agentem sieciowym.

Znaczniki

Sekcja **Znaczniki** wyświetla listę słów kluczowych (tagów), które mogą zostać dodane do urządzeń klienckich po zainstalowaniu Agenta sieciowego. Możesz dodawać i usuwać tagi do/z listy, a także zmieniać ich nazwy.

Jeśli pole obok tagu jest zaznaczone, ten tag zostanie automatycznie dodany do zarządzanych urządzeń podczas instalacji Agenta sieciowego.

Jeśli pole obok znacznika jest odznaczone, znacznik nie zostanie automatycznie dodany do zarządzanych urządzeń podczas instalacji Agenta sieciowego. Możesz ręcznie dodać ten tag do urządzeń.

Podczas usuwania tagu z listy zostanie on automatycznie usunięty ze wszystkich urządzeń, do których został dodany.

Historia rewizji

W tej sekcji możesz przejrzeć historię rewizji pakietu instalacyjnego. Możesz porównać rewizje, przejrzeć rewizje, zapisać rewizje do pliku oraz dodać i zmodyfikować opisy rewizji.

Ustawienia pakietu instalacyjnego Agenta sieciowego dostępne dla określonego systemu operacyjnego zostały podane w tabeli poniżej.

Ustawienia pakietu instalacyjnego Agenta sieciowego

Sekcja Właściwość	Windows	Mac	Linux
Ogólne	✓	✓	✓
Ustawienia	✓	—	—
Połączenie	✓	✓ (za wyjątkiem opcji **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows** i **Używaj wyłącznie automatycznego wykrywania serwera proxy**)	✓ (za wyjątkiem opcji **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows** i **Używaj wyłącznie automatycznego wykrywania serwera proxy**)
Zaawansowane	✓	✓	✓
Dodatkowe składniki	✓	✓	✓
Znaczniki	✓	✓ (za wyjątkiem reguł automatycznego znakowania)	✓ (za wyjątkiem reguł automatycznego znakowania)
Historia rewizji	✓	✓	✓

Przeglądanie Polityki prywatności

Polityka prywatności jest dostępna online pod adresem https://www.kaspersky.com/products-and-services-privacy-policy; jest również dostępna w trybie offline. Z Polityką prywatności możesz zapoznać się, na przykład, przed zainstalowaniem Agenta sieciowego.

W celu przeczytania Polityki prywatności w trybie offline:

1. Uruchom instalator Kaspersky Security Center.
2. W oknie instalatora przejdź do odnośnika **Wypakuj pakiety instalacyjne**.
3. Z listy, która zostanie otwarta, wybierz Agent sieciowy Kaspersky Security Center, a następnie kliknij **Dalej**.

Plik privacy_policy.txt pojawi się na Twoim urządzeniu, w określonym folderze, w podfolderze NetAgent.

Wdrażanie systemów zarządzania urządzeniami mobilnymi

Ta sekcja opisuje systemy wdrażania zarządzania urządzeniami mobilnymi poprzez protokoły iOS MDM i Kaspersky Endpoint Security.

Wdrażanie systemu zarządzania poprzez protokół iOS MDM

Kaspersky Security Center umożliwia zarządzanie urządzeniami mobilnymi działającymi pod kontrolą systemu iOS. Urządzenia mobilne iOS MDM to urządzenia mobilne iOS podłączone do serwera iOS MDM i zarządzane przez Serwer administracyjny.

Urządzenia mobilne łączy się z serwerem iOS MDM, wykonując następujące czynności:

1. Administrator instaluje serwer iOS MDM.
2. Administrator pobiera certyfikat usługi Apple Push Notification Service (APNs) (Otrzymywanie certyfikatu APNs, https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm).

   Certyfikat APN umożliwia Serwerowi administracyjnemu nawiązanie połączenia z serwerem APN w celu wysłania na urządzenia mobilne iOS MDM powiadomień push.
3. Administrator instaluje certyfikat APN na serwerze iOS MDM.
4. Administrator tworzy profil iOS MDM dla użytkownika urządzenia mobilnego iOS.

   Profil iOS MDM zawiera zbiór ustawień do łączenia urządzeń mobilnych iOS z Serwerem administracyjnym.

Po pobraniu profilu iOS MDM i zsynchronizowaniu urządzenia mobilnego iOS MDM z Serwerem administracyjnym, urządzenie zostanie wyświetlone w podfolderze **Mobile devices**, znajdującym się w folderze **Mobile Device Management** drzewa konsoli.

Instalowanie serwera iOS MDM

W celu zainstalowania serwera iOS MDM na urządzeniu lokalnym:

1. Uruchom plik wykonywalny setup.exe.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania.

   W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj serwer iOS MDM**, aby uruchomić kreator instalacji serwera iOS MDM.

2. Wybierz folder docelowy.

   Domyślny folder docelowy to <Dysk>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie w trakcie instalacji. Można zmienić folder docelowy przy użyciu przycisku **Przeglądaj**.

3. W oknie **Określ ustawienia połączenia z serwerem iOS MDM**, w polu **Port zewnętrzny do połączenia z usługą iOS MDM** określ port zewnętrzny do łączenia urządzeń mobilnych z usługą iOS MDM.

   Port zewnętrzny 5223 jest używany przez urządzenia mobilne do komunikacji z serwerem APN. Upewnij się, że port 5223 jest otwarty w zaporze sieciowej do łączenia z zakresem adresów 17.0.0.0/8.

   Domyślnie port 443 jest używany do łączenia z serwerem iOS MDM. Jeśli port 443 jest już używany przez inną usługę lub aplikację, można go zastąpić, na przykład portem 9443.

   Serwer iOS MDM używa portu zewnętrznego 2197 do wysyłania powiadomień na serwer APN.

   Serwery APN działają w trybie równoważenia obciążenia. Urządzenia mobilne nie zawsze łączą się z tymi samymi adresami IP do pobierania powiadomień. Zakres adresów 17.0.0.0/8 jest zarezerwowany dla Apple. Dlatego też zalecane jest określenie w ustawieniach Zapory sieciowej tego całego zakresu jako dozwolonego.

4. Jeśli chcesz ręcznie skonfigurować interakcję portów dla komponentów aplikacji, wybierz opcję **Określ porty lokalne ręcznie**, a następnie określ wartości następujących ustawień:

   - **Port do połączenia z Agentem sieciowym**. W tym polu określ port dla połączenia usługi iOS MDM z Agentem sieciowym. Domyślny numer portu to 9799.
   - **Port lokalny do połączenia z usługą iOS MDM**. W tym polu określ lokalny port dla połączenia Agenta sieciowego z usługą iOS MDM. Domyślny numer portu to 9899.

   > Zalecane jest użycie wartości domyślnych.

5. W oknie **Adres zewnętrzny Serwera urządzeń mobilnych**, w polu **Adres internetowy do zdalnego połączenia z Serwerem urządzeń mobilnych** określ adres urządzenia klienckiego, na którym zostanie zainstalowany serwer iOS MDM.

   Ten adres będzie używany do łączenia zarządzanych urządzeń mobilnych z usługą iOS MDM. To urządzenie klienckie powinno być dostępne dla podłączenia urządzeń iOS MDM.

   Możesz określić adres urządzenia klienckiego w jednym z poniższych formatów:

   - FQDN urządzenia (np. mdm.example.com)
   - Nazwa NetBIOS urządzenia

   > W pasku adresu nie musisz dodawać numeru portu i schematu URL, ponieważ te wartości zostaną dodane automatycznie.

Po zakończeniu działania kreatora, serwer iOS MDM zostanie zainstalowany na urządzeniu lokalnym. Serwer iOS MDM będzie wyświetlany w folderze **Zarządzanie urządzeniami mobilnymi**.

Instalowanie serwera iOS MDM w trybie cichym

Kaspersky Security Center umożliwia zainstalowanie serwera iOS MDM na urządzeniu lokalnym w trybie cichym, czyli bez interaktywnego wprowadzania ustawień instalacji.

W celu zainstalowania serwera iOS MDM na urządzeniu lokalnym w trybie cichym:

1. Przeczytaj Umowę licencyjną użytkownika końcowego. Użyj poniższego polecenia tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

2. Uruchom następujące polecenie:

   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <parametry_ustawień>"
   ```

   gdzie `parametry_ustawień` to lista ustawień i ich odpowiednich wartości oddzielonych spacjami (`PROP1=PROP1VAL PROP2=PROP2VAL`). Plik setup.exe zlokalizowany jest w folderze Server, który jest częścią pakietu dystrybucyjnego Kaspersky Security Center.

Nazwy i możliwe wartości parametrów, które mogą być wykorzystywane podczas instalacji serwera iOS MDM w trybie cichym, wyszczególnione są w tabeli poniżej. Parametry można określać w dowolnej kolejności.

Parametry instalacji serwera iOS MDM w trybie cichym

Nazwa parametru	Opis parametru	Dostępne wartości
Umowa licencyjna użytkownika końcowego	Akceptacja postanowień i warunków Umowy Licencyjnej Użytkownika Końcowego. Ten parametr jest obowiązkowy.	• 1 — W pełni przeczytałem(am), rozumiem i akceptuję warunki Umowy Licencyjnej Użytkownika Końcowego. • Inna wartość lub brak wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
DONT_USE_ANSWER_FILE	Określa, czy ma być używany plik XML z ustawieniami instalacji serwera iOS MDM. Plik XML znajduje się w pakiecie instalacyjnym lub jest przechowywany na Serwerze administracyjnym. Nie ma konieczności określania dodatkowej ścieżki do pliku. Ten parametr jest obowiązkowy.	• 1 — Nie używaj pliku XML z parametrami. • Inna wartość lub brak wartości — Użyj pliku XML z parametrami.
INSTALLDIR	Folder instalacyjny serwera iOS MDM. Ten parametr jest opcjonalny.	Wartość ciągu może być, na przykład: `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	Port lokalny dla połączenia usługi iOS MDM z Agentem sieciowym. Domyślny numer portu to 9799. Ten parametr jest opcjonalny.	Wartość numeryczna.
LOCALSERVERPORT	Port lokalny dla połączenia Agenta sieciowego z usługą iOS MDM. Domyślny numer portu to 9899. Ten parametr jest opcjonalny.	Wartość numeryczna.
EXTERNALSERVERPORT	Port dla połączenia urządzenia z serwerem iOS MDM. Domyślny numer portu to 443. Ten parametr jest opcjonalny.	Wartość numeryczna.
EXTERNAL_SERVER_URL	Zewnętrzny adres urządzenia klienckiego, na którym zostanie zainstalowany serwer iOS MDM. Ten adres będzie używany do łączenia zarządzanych urządzeń mobilnych z usługą iOS MDM. To urządzenie klienckie powinno być dostępne dla połączenia poprzez iOS MDM. Adres nie może zawierać schematu adresu URL oraz numeru portu, gdyż wartości te zostaną dodane automatycznie. Ten parametr jest opcjonalny.	• FQDN urządzenia (np. mdm.example.com) • Nazwa NetBIOS urządzenia • Adres IP urządzenia

Nazwa parametru	Opis parametru	Dostępne wartości
WORKFOLDER	Folder roboczy serwera iOS MDM. Jeśli nie wskazano folderu roboczego, dane zostaną zapisane w domyślnym folderze. Ten parametr jest opcjonalny.	Wartość ciągu może być, na przykład: `WORKFOLDER=\"C:\work\"`
MTNCY	Korzystanie z serwera iOS MDM przez kilka Serwerów wirtualnych. Ten parametr jest opcjonalny.	• 1 — Serwer iOS MDM zostanie użyty przez kilka wirtualnych Serwerów administracyjnych. • Inna wartość lub brak wartości — Serwer iOS MDM nie zostanie użyty przez kilka wirtualnych Serwerów administracyjnych.

Na przykład:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

Parametry instalacji serwera iOS MDM są opisane szczegółowo w sekcji „Instalowanie serwera iOS MDM".

Scenariusze instalowania serwera iOS MDM

Liczba kopii serwera iOS MDM przeznaczonych do zainstalowania może zostać wybrana w oparciu o dostępny sprzęt lub całkowitą liczbę urządzeń mobilnych.

Jednakże należy pamiętać, że zalecana maksymalna liczba urządzeń mobilnych dla pojedynczej instalacji Kaspersky Device Management for iOS wynosi 50 000. Aby zmniejszyć obciążenie, cała pula urządzeń może zostać rozesłana na kilka serwerów, na których jest zainstalowany serwer iOS MDM.

Autoryzacja urządzeń iOS MDM odbywa się poprzez certyfikaty użytkownika (każdy profil zainstalowany na urządzeniu zawiera certyfikat właściciela urządzenia). Dla serwera iOS MDM dostępne są dwa schematy wdrożenia:

- Uproszczony schemat instalacji
- Schemat zdalnej instalacji z użyciem delegowania protokołu Kerberos (KCD)

Uproszczony schemat instalacji

Podczas zdalnej instalacji serwera iOS MDM z użyciem uproszczonego schematu instalacji, urządzenia mobilne łączą się bezpośrednio z usługą sieciową iOS MDM. W tym przypadku certyfikaty użytkownika wydane przez Serwer administracyjny mogą być stosowane tylko do autoryzacji urządzeń. Integracja z infrastrukturą kluczy publicznych (PKI) jest niemożliwa dla certyfikatów użytkowników.

Schemat zdalnej instalacji z użyciem delegowania protokołu Kerberos (KCD)

Aby móc korzystać ze schematu wdrażania z Kerberos Constrained Delegation (KCD), muszą zostać spełnione następujące wymagania:

- Serwer administracyjny i serwer iOS MDM znajdują się w wewnętrznej sieci organizacji.
- Używany jest odwrotny serwer proxy obsługujący KCD.

Ten schemat instalacji obejmuje:

- Integracja z odwrotnym serwerem proxy obsługującym KCD
- Użycie KCD do autoryzacji urządzeń mobilnych
- Integrację z PKI do stosowania certyfikatów użytkownika

Podczas korzystania z tego schematu zdalnej instalacji należy:

- W Konsoli administracyjnej, w ustawieniach usługi sieciowej iOS MDM zaznaczyć pole **Zapewnij kompatybilność z Kerberos constrained delegation**.
- Jako certyfikat dla usługi sieciowej iOS MDM określ certyfikat niestandardowy, który został zdefiniowany, gdy usługa sieciowa iOS MDM została opublikowana na odwrotnym serwerze proxy.
- Certyfikaty użytkownika dla urządzeń iOS muszą być wystawione przez urząd certyfikacji (CA) domeny. Jeśli domena zawiera kilka głównych urzędów certyfikacji, certyfikaty użytkownika muszą być wystawione przez urząd certyfikacji, który został określony, gdy usługa sieciowa iOS MDM została opublikowana na odwrotnym serwerze proxy.

  Możesz zapewnić, że certyfikat użytkownika jest zgodny z wymaganiami wystawiania certyfikatów urzędu certyfikacji przy użyciu jednej z następujących metod:

  - Określ certyfikat użytkownika w kreatorze Nowego profilu iOS MDM oraz w kreatorze instalacji certyfikatu.
  - Zintegruj Serwer administracyjny z infrastrukturą kluczy publicznych domeny oraz zdefiniuj odpowiednie ustawienie w regułach wystawiania certyfikatów:

    1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.
    2. W obszarze roboczym folderu **Certyfikaty** kliknij przycisk **Konfiguruj reguły wydawania certyfikatów**, aby otworzyć okno **Reguły wydawania certyfikatu**.
    3. W sekcji **Integracja z PKI** skonfiguruj integrację z infrastrukturą kluczy publicznych.
    4. W sekcji **Wydawanie certyfikatów dla urządzeń mobilnych** określ źródło certyfikatów.

Poniżej znajduje się przykład konfiguracji delegowania protokołu Kerberos (KCD) z następującymi założeniami:

- Usługa sieciowa iOS MDM działa na porcie 443.
- Nazwa urządzenia z odwrotnym serwerem proxy to firewall.mydom.local.
- Nazwa urządzenia z usługą sieciową iOS MDM to iosmdm.mydom.local.
- Nazwa zewnętrznej publikacji usługi sieciowej iOS MDM to iosmdm.mydom.global.

Nazwa główna usługi dla http/iosmdm.mydom.local

W domenie należy zarejestrować nazwę główną usługi (SPN) dla urządzenia z usługą sieciową iOS MDM (iosmdm.mydom.local):

```
setspn -a http/iosmdm.mydom.local iosmdm
```

Konfiguracja właściwości domeny urządzenia z odwrotnym serwerem proxy (firewall.mydom.local)

Aby przeprowadzić ruch sieciowy, przełącz urządzenie z odwrotnym serwerem proxy (firewall.mydom.local) do usługi, która jest definiowana po SPN (http/iosmdm.mydom.local).

W celu przełączenia urządzenia z odwrotnego serwera proxy do usługi definiowanej po SPN (http/iosmdm.mydom.local), administrator musi wykonać następujące działania:

1. W przystawce Microsoft Management Console o nazwie „Użytkownicy i komputery usługi Active Directory" wybierz urządzenie z zainstalowanym odwrotnym serwerem proxy (firewall.mydom.local).

2. We właściwościach urządzenia, na zakładce **Delegowanie** ustaw przełącznik **Ufaj temu komputerowi w delegowaniu tylko do określonych usług** na **Użyj dowolnego protokołu uwierzytelniania**.

3. Dodaj SPN (http/iosmdm.mydom.local) do listy **Usługi, którym to konto może przedstawiać delegowane poświadczenia**.

Specjalny (niestandardowy) certyfikat dla opublikowanej usługi sieciowej (iosmdm.mydom.global)

Konieczne jest opublikowanie specjalnego (niestandardowego) certyfikatu dla usługi sieciowej iOS MDM na FQDN iosmdm.mydom.global i określić w Konsoli administracyjnej, w ustawieniach usługi sieciowej iOS MDM, że zastępuje on domyślny certyfikat.

Należy pamiętać, że kontener certyfikatów (plik z rozszerzeniem .p12 lub .pfx) musi także zawierać łańcuch certyfikatów głównych (klucze publiczne).

Publikowanie usługi sieciowej iOS MDM na odwrotnym serwerze proxy

Na odwrotnym serwerze proxy, dla ruchu przechodzącego z urządzenia mobilnego do portu 443 usługi iosmdm.mydom.global należy skonfigurować KCD na SPN (http/iosmdm.mydom.local), korzystając z certyfikatu opublikowanego dla FQDN (iosmdm.mydom.global). Nie można zapominać, że publikacja oraz opublikowana usługa sieciowa powinny korzystać z tego samego certyfikatu serwera.

Pobieranie certyfikatu APNs

Jeśli masz już certyfikat APNs, rozważ jego odnowienie zamiast utworzenie nowego. Po zastąpieniu istniejącego certyfikatu APNs nowo utworzonym, Serwer administracyjny utraci możliwość zarządzania aktualnie podłączonymi urządzeniami mobilnymi iOS.

Po utworzeniu Żądania podpisania certyfikatu (Certificate Signing Request - żądanie CSR) w pierwszym kroku kreatora certyfikatu APNs, jego prywatny klucz jest przechowywany w pamięci RAM Twojego urządzenia. Dlatego też wszystkie kroki kreatora muszą zostać zakończone w jednej sesji aplikacji.

W celu pobrania certyfikatu APNs:

1. W folderze **Zarządzanie urządzeniami mobilnymii** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**

2. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.

3. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera iOS MDM.

4. W oknie właściwości serwera iOS MDM wybierz sekcję **Certyfikaty**.

5. W sekcji **Certyfikaty**, w grupie ustawień **Certyfikat usługi Apple Push Notification** kliknij przycisk **Żądaj nowego**.

   Zostanie uruchomiony Kreator pobierania certyfikatu APNs i zostanie otwarte okno **Żądaj nowego**.

6. Utwórz Żądanie podpisania certyfikatu (zwane dalej CSR). W tym celu wykonaj następujące czynności:

   a. Kliknij przycisk **Utwórz CSR**.

   b. W otwartym oknie **Utwórz CSR** określ nazwę swojego żądania, nazwę firmy i oddziału, swoje miasto, region i kraj.

   c. Kliknij przycisk **Zapisz** i określ nazwę pliku, do którego zostanie zapisane Twoje żądanie CSR.

   Prywatny klucz certyfikatu zostanie zapisany w pamięci urządzenia.

7. Użyj swojego konta w serwisie CompanyAccount do wysłania pliku z CSR do Kaspersky w celu jego podpisania.

   > Podpisanie CSR będzie dostępne tylko po przesłaniu na portal CompanyAccount klucza umożliwiającego użycie funkcji Zarządzanie urządzeniami mobilnymi.

   Po przetworzeniu Twojego żądania online, otrzymasz plik CSR podpisany przez Kaspersky.

8. Wyślij podpisany plik CSR na stronę Apple Inc. przy użyciu losowego numeru Apple ID.

   > Zalecamy, aby nie używać osobistego numeru Apple ID. Utwórz dedykowany numer Apple ID, aby użyć go jako firmowego numeru ID. Po utworzeniu numeru Apple ID, skojarz go ze skrzynką pocztową firmy, a nie skrzynką pocztową pracownika.

   Po przetworzeniu Twojego żądania CSR w Apple Inc., otrzymasz publiczny klucz certyfikatu APNs. Zapisz plik na dysku.

9. Wyeksportuj certyfikat APNs wraz z prywatnym kluczem utworzonym podczas generowania żądania CSR w formacie PFX. Aby to zrobić:

   a. W oknie **Żądaj nowego certyfikatu APNs** kliknij przycisk **Zakończ CSR**.

   b. W oknie **Otwórz** wybierz plik z publicznym kluczem certyfikatu, otrzymany z Apple Inc. w wyniku przetworzenia żądania CSR, a następnie kliknij przycisk **Otwórz**.

      Zostanie uruchomiony proces eksportowania certyfikatu.

   c. W następnym oknie wprowadź hasło prywatnego klucza i kliknij **OK**.

      To hasło zostanie użyte do zainstalowania certyfikatu APN na serwerze iOS MDM.

   d. W oknie **Zapisz certyfikat APNs** określ nazwę pliku dla certyfikatu APNs, wybierz folder i kliknij **Zapisz**.

Prywatne i publiczne klucze certyfikatu zostaną połączone, a certyfikat APNs zostanie zapisany w formacie PFX. Teraz możesz zainstalować certyfikat APNs na serwerze iOS MDM.

Odnawianie certyfikatu APNs

W celu odnowienia certyfikatu APNs:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**
2. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.
3. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera iOS MDM.
4. W oknie właściwości serwera iOS MDM wybierz sekcję **Certyfikaty**.
5. W sekcji **Certyfikaty**, w grupie ustawień **Certyfikat usługi Apple Push Notification** kliknij przycisk **Odnów**.

   Zostanie uruchomiony Kreator odnawiania certyfikatu usługi Apple Push Notification i zostanie otwarte okno **Odnów certyfikat APNs**.
6. Utwórz Żądanie podpisania certyfikatu (zwane dalej CSR). W tym celu wykonaj następujące czynności:

   a. Kliknij przycisk **Utwórz CSR**.

   b. W otwartym oknie **Utwórz CSR** określ nazwę swojego żądania, nazwę firmy i oddziału, swoje miasto, region i kraj.

   c. Kliknij przycisk **Zapisz** i określ nazwę pliku, do którego zostanie zapisane Twoje żądanie CSR.

   Prywatny klucz certyfikatu zostanie zapisany w pamięci urządzenia.
7. Użyj swojego konta w serwisie CompanyAccount do wysłania pliku z CSR do Kaspersky w celu jego podpisania.

   > Podpisanie CSR będzie dostępne tylko po przesłaniu na portal CompanyAccount klucza umożliwiającego użycie funkcji Zarządzanie urządzeniami mobilnymi.

   Po przetworzeniu Twojego żądania online, otrzymasz plik CSR podpisany przez Kaspersky.
8. Wyślij podpisany plik CSR na stronę Apple Inc. przy użyciu losowego numeru Apple ID.

   > Zalecamy, aby nie używać osobistego numeru Apple ID. Utwórz dedykowany numer Apple ID, aby użyć go jako firmowego numeru ID. Po utworzeniu numeru Apple ID, skojarz go ze skrzynką pocztową firmy, a nie skrzynką pocztową pracownika.

   Po przetworzeniu Twojego żądania CSR w Apple Inc., otrzymasz publiczny klucz certyfikatu APNs. Zapisz plik na dysku.

9. Zażądaj klucza publicznego certyfikatu. W tym celu wykonaj następujące czynności:

    a. Przejdź do portalu Apple Push Certificates. Aby zalogować się w portalu, użyj identyfikatora Apple ID, otrzymanego przy pierwszym żądaniu certyfikatu.

    b. Na liście certyfikatów wybierz certyfikat, którego nazwa APSP (w formacie „APSP: <numer>") odpowiada nazwie APSP certyfikatu używanego przez serwer iOS MDM, a następnie kliknij przycisk **Odnów**.

    Certyfikat APNs zostanie odnowiony.

    c. Zapisz certyfikat utworzony na portalu.

10. Wyeksportuj certyfikat APNs wraz z prywatnym kluczem utworzonym podczas generowania żądania CSR w formacie PFX. W tym celu wykonaj następujące czynności:

    a. W oknie **Odnów certyfikat APNs** kliknij przycisk **Zakończ CSR**.

    b. W oknie **Otwórz** wybierz plik z publicznym kluczem certyfikatu, otrzymany z Apple Inc. w wyniku przetworzenia żądania CSR, a następnie kliknij przycisk **Otwórz**.

    Zostanie uruchomiony proces eksportowania certyfikatu.

    c. W następnym oknie wprowadź hasło prywatnego klucza i kliknij **OK**.

    To hasło zostanie użyte do zainstalowania certyfikatu APN na serwerze iOS MDM.

    d. W otwartym oknie **Odnów certyfikat APNs** określ nazwę pliku dla certyfikatu APNs, wybierz folder i kliknij **Zapisz**.

Prywatne i publiczne klucze certyfikatu zostaną połączone, a certyfikat APNs zostanie zapisany w formacie PFX.

Konfigurowanie zapasowego certyfikatu serwera iOS MDM

Funkcjonalność serwera iOS MDM umożliwia wystawienie certyfikatu zapasowego. Ten certyfikat jest przeznaczony do użycia w profilach iOS MDM, aby zapewnić bezproblemowe przełączanie zarządzanych urządzeń iOS po wygaśnięciu certyfikatu iOS MDM Server.

Jeśli Twój serwer iOS MDM używa domyślnego certyfikatu wystawionego przez Kaspersky, możesz wystawić certyfikat zapasowy (lub określić własny certyfikat niestandardowy jako zapasowy) przed wygaśnięciem certyfikatu serwera iOS MDM. Domyślnie certyfikat zapasowy jest wystawiany automatycznie 60 dni przed wygaśnięciem certyfikatu serwera iOS MDM. Zapasowy certyfikat serwera iOS MDM staje się certyfikatem głównym natychmiast po wygaśnięciu certyfikatu serwera iOS MDM. Klucz publiczny jest dystrybuowany do wszystkich zarządzanych urządzeń za pośrednictwem profili konfiguracyjnych, więc nie ma konieczności ręcznego przesyłania go.

W celu wystawienia certyfikatu zapasowego serwera iOS MDM lub określenia niestandardowego certyfikatu zapasowego:

1. W drzewie konsoli, w folderze **Zarządzanie urządzeniami mobilnymi** wybierz podfolder **Serwery urządzeń mobilnych**.

2. Na liście serwerów urządzeń mobilnych wybierz odpowiedni serwer iOS MDM, a następnie w prawej części okna kliknij przycisk **Konfiguruj Serwer iOS MDM**.

3. W oknie ustawień serwera iOS MDM wybierz sekcję **Certyfikaty**.

4. W sekcji ustawień **Certyfikat zapasowy** wykonaj jedną z następujących czynności:

   - Jeśli planujesz nadal korzystać z certyfikatu z podpisem własnym (czyli certyfikatu wystawionego przez Kaspersky):

     a. Kliknij przycisk **Wydanie**.

     b. W oknie **Data aktywacji**, które zostanie otwarte, wybierz jedną z dwóch opcji daty, kiedy należy zastosować certyfikat zapasowy:

        - Jeśli chcesz zastosować certyfikat zapasowy w momencie wygaśnięcia aktualnego certyfikatu, wybierz opcję **Kiedy aktualny certyfikat wygaśnie**.

        - Jeśli chcesz zastosować certyfikat zapasowy przed wygaśnięciem bieżącego certyfikatu, wybierz opcję **Po określonym czasie (w dniach)**. W polu wejściowym obok tej opcji określ czas, po upływie którego certyfikat zapasowy musi zastąpić aktualny certyfikat.

        > Okres ważności certyfikatu zapasowego, który określisz, nie może przekraczać okresu ważności bieżącego certyfikatu serwera iOS MDM.

     c. Kliknij przycisk **OK**.

     Zostanie utworzony zapasowy certyfikat serwera iOS MDM.

   - Jeśli planujesz używać niestandardowego certyfikatu wydanego przez urząd certyfikacji:

     a. Kliknij przycisk **Dodaj**.

     b. W otwartym oknie Eksploratora plików określ plik certyfikatu w formacie PEM, PFX lub P12 który jest przechowywany na urządzeniu, a następnie kliknij przycisk **Otwórz**.

     Twój niestandardowy certyfikat jest określony jako zapasowy certyfikat serwera iOS MDM.

Masz określony zapasowy certyfikat serwera iOS MDM. Szczegóły certyfikatu zapasowego są wyświetlane w sekcji ustawień **Certyfikat zapasowy** (nazwa certyfikatu, nazwa wystawcy, data wygaśnięcia i data zastosowania certyfikatu zapasowego, jeśli istnieje).

Instalowanie certyfikatu APNs na serwerze iOS MDM

Po otrzymaniu certyfikatu APNs, powinieneś zainstalować go na serwerze iOS MDM.

W celu zainstalowania certyfikatu APNs na serwerze iOS MDM:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**

2. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.

3. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera iOS MDM.

4. W oknie właściwości serwera iOS MDM wybierz sekcję **Certyfikaty**.

5. W sekcji **Certyfikaty**, w grupie ustawień **Certyfikat usługi Apple Push Notification** kliknij przycisk **Zainstaluj**.

6. Wybierz plik PFX, który zawiera certyfikat APN.

7. Wprowadź hasło klucza prywatnego, które zostało określone podczas eksportowania certyfikatu APNs.

Certyfikat APNs zostanie zainstalowany na serwerze iOS MDM. Szczegóły dotyczące certyfikatu będą wyświetlane w oknie właściwości serwera iOS MDM, w sekcji **Certyfikaty**.

Konfigurowanie dostępu do usługi Apple Push Notification

W celu zapewnienia poprawnego działania usługi sieciowej iOS MDM oraz reakcji urządzeń w odpowiednim momencie na polecenia administratora, w ustawieniach serwera iOS MDM należy określić certyfikat Apple Push Notification Service (zwany dalej certyfikatem APNs).

Podczas interakcji z Apple Push Notification (zwane dalej APNs) usługa sieciowa iOS MDM łączy się z zewnętrznym adresem api.push.apple.com poprzez port 2197 (wychodzący). Dlatego też, usługa sieciowa iOS MDM wymaga dostępu do portu TCP 2197 dla zakresu adresów 17.0.0.0/8. Ze strony urządzenia iOS możliwy jest dostęp do portu TCP 5223 dla zakresu adresów 17.0.0.0/8.

Jeśli chcesz uzyskać dostęp do APN ze strony usługi sieciowej iOS MDM poprzez serwer proxy, na urządzeniu z zainstalowaną usługą sieciową iOS MDM musisz wykonać następujące działania:

1. Dodaj do rejestru następujące wiersze:

   - W 32-bitowych systemach operacyjnych:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Nazwa Hosta Proxy>"
"ApnProxyPort"="<Port Proxy>"
"ApnProxyLogin"="<Login Proxy>"
"ApnProxyPwd"="<Hasło Proxy>"
```

   - W 64-bitowych systemach operacyjnych:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Nazwa Hosta Proxy>"
"ApnProxyPort"="<Port Proxy>"
"ApnProxyLogin"="<Login Proxy>"
"ApnProxyPwd"="<Hasło Proxy>"
```

2. Uruchom ponownie usługę sieciową iOS MDM.

Publikowanie i instalowanie certyfikatu współdzielonego na urządzeniu mobilnym

W celu opublikowania certyfikatu współdzielonego dla użytkownika:

1. Z drzewa konsoli, w folderze **Konta użytkowników** wybierz konto użytkownika.
2. Z menu kontekstowego konta użytkownika wybierz **Zainstaluj certyfikat**.

   Zostanie uruchomiony kreator instalacji certyfikatu. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora certyfikat zostanie utworzony i dodany do listy certyfikatów użytkownika.

Wydany certyfikat zostanie pobrany przez użytkownika wraz z pakietem instalacyjnym zawierającym profil iOS MDM.

Po podłączeniu urządzenia mobilnego do serwera iOS MDM, ustawienia profilu iOS MDM zostaną zastosowane na urządzeniu użytkownika. Administrator będzie mógł zarządzać urządzeniem po jego podłączeniu.

Urządzenie mobilne użytkownika podłączone do serwera iOS MDM jest wyświetlane w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi**.

Dodawanie urządzeń KES do listy zarządzanych urządzeń

W celu dodania urządzenia KES do listy zarządzanych urządzeń przy użyciu odnośnika do sklepu Google Play™:

1. Z drzewa konsoli wybierz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.
2. Wybierz konto użytkownika, którego urządzenie mobilne chcesz dodać do listy zarządzanych urządzeń.
3. W menu kontekstowym konta użytkownika wybierz **Dodaj urządzenie mobilne**.

   Zostanie uruchomiony kreator podłączania urządzenia mobilnego. W oknie **Źródło certyfikatu** musisz określić metodę tworzenia współdzielonego certyfikatu, którego Serwer administracyjny użyje do identyfikacji urządzenia mobilnego. Certyfikat współdzielony można określić na jeden z następujących sposobów:

   - Automatycznie utwórz certyfikat współdzielony przy użyciu narzędzi Serwera administracyjnego, a następnie wyślij certyfikat na urządzenie.
   - Wskaż plik współdzielonego certyfikatu.
4. W oknie **Typ urządzenia** wybierz **Odnośnik do Google Play**.

5. W oknie **Metoda powiadamiania użytkownika** zdefiniuj ustawienia powiadamiania użytkownika urządzenia mobilnego o utworzeniu certyfikatu (za pośrednictwem wiadomości SMS, poczty elektronicznej lub poprzez wyświetlenie informacji po zakończeniu działania kreatora).

6. W oknie z informacjami o certyfikacie kliknij przycisk **Zakończ**, aby zakończyć działanie kreatora.

Po zakończeniu działania kreatora, odnośnik oraz kod QR zostaną wysłane na urządzenie mobilne użytkownika, umożliwiając mu w ten sposób pobranie Kaspersky Endpoint Security ze sklepu Google Play. Użytkownik otwiera stronę sklepu Google Play poprzez kliknięcie odsyłacza lub przeskanowanie kodu QR. System operacyjny urządzenia wyświetla pytanie o zaakceptowanie instalacji Kaspersky Endpoint Security for Android. Po pobraniu i zainstalowaniu Kaspersky Endpoint Security for Android, urządzenie mobilne nawiązuje połączenie z Serwerem administracyjnym i pobiera współdzielony certyfikat. Po zainstalowaniu certyfikatu na urządzeniu mobilnym, urządzenie zostanie wyświetlone w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli.

Jeśli program Kaspersky Endpoint Security for Android jest już zainstalowany na urządzeniu, użytkownik musi otrzymać ustawienia połączenia z Serwerem Administracyjnym od administratora, a następnie samodzielnie wprowadzić je na urządzeniu. Po zdefiniowaniu ustawień połączenia, urządzenie mobilne łączy się z Serwerem Administracyjnym. Administrator wystawia certyfikat współdzielony dla urządzenia i wysyła użytkownikowi wiadomość e-mail lub wiadomość SMS z nazwą użytkownika i hasłem do pobrania certyfikatu. Użytkownik pobiera i instaluje współdzielony certyfikat. Po zainstalowaniu certyfikatu na urządzeniu mobilnym, urządzenie zostanie wyświetlone w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli. W tym przypadku program Kaspersky Endpoint Security for Android nie zostanie pobrany i ponownie zainstalowany.

Połączenie urządzeń KES z Serwerem administracyjnym

W zależności od metody używanej do łączenia urządzeń z Serwerem administracyjnym, dla Kaspersky Device Management for iOS istnieją dwa schematy zdalnej instalacji na urządzeniach KES:

- Schemat zdalnej instalacji z bezpośrednim połączeniem urządzeń z Serwerem administracyjnym
- Schemat wdrożenia obejmujący odwrotny serwer proxy obsługujący delegowanie protokołu Kerberos

Bezpośrednie połączenie urządzeń z Serwerem administracyjnym

Urządzenia KES mogą łączyć się bezpośrednio z portem 13292 Serwera administracyjnego.

W zależności od metody używanej do autoryzacji, dla połączenia urządzeń KES z Serwerem administracyjnym możliwe są dwie opcje:

- Łączenie urządzeń z użyciem certyfikatu użytkownika
- Łączenie urządzeń bez użycia certyfikatu użytkownika

Łączenie urządzeń z użyciem certyfikatu użytkownika

Podczas łączenia urządzeń z użyciem certyfikatu użytkownika, to urządzenie jest kojarzone z kontem użytkownika, do którego odpowiedni certyfikat został przypisany poprzez narzędzia Serwera administracyjnego.

W tym przypadku używane będzie dwukierunkowe uwierzytelnianie SSL (uwierzytelnianie obustronne). Serwer administracyjny i urządzenie będą uwierzytelniani przy użyciu certyfikatów.

Łączenie urządzeń bez użycia certyfikatu użytkownika

Podczas łączenia urządzenia bez użycia certyfikatu użytkownika, to urządzenie nie jest kojarzone z żadnym kontem użytkownika na Serwerze administracyjnym. Jednakże, gdy urządzenie pobierze dowolny certyfikat, to urządzenie zostanie skojarzone z kontem użytkownika, do którego odpowiedni certyfikat został przypisany poprzez narzędzia Serwera administracyjnego.

Podczas łączenia tego urządzenia z Serwerem administracyjnym zostanie zastosowane jednokierunkowe uwierzytelnianie SSL, co oznacza, że tylko Serwer administracyjny będzie uwierzytelniony przy użyciu certyfikatu. Po pobraniu przez urządzenie certyfikatu użytkownika, typ autoryzacji zmieni się na dwukierunkowe uwierzytelnianie SSL (uwierzytelnianie obustronne).

Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD)

Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD) uwzględnia:

- Integracja z odwrotnym serwerem proxy obsługującym KCD.
- Użycie delegowania protokołu Kerberos (zwane również KCD) do uwierzytelnia urządzeń mobilnych.
- Integrację z infrastrukturą kluczy publicznych (zwana również PKI) w celu zastosowania certyfikatów użytkownika.

Podczas korzystania z tego schematu połączenia należy pamiętać, że:

- Typem połączenia urządzeń KES z odwrotnym serwerem proxy ma być „dwukierunkowe uwierzytelnianie SSL", czyli urządzenie musi łączyć się z odwrotnym serwerem proxy poprzez swój własny certyfikat użytkownika. W tym celu należy zintegrować certyfikat użytkownika z pakietem instalacyjnym programu Kaspersky Endpoint Security for Android, który został zainstalowany na urządzeniu. Ten pakiet KES musi być utworzony przez Serwer administracyjny specjalnie dla tego urządzenia (użytkownika).
- Dla protokołu mobilnego powinieneś określić specjalny (niestandardowy) certyfikat zamiast domyślnego certyfikatu serwera:

  1. W oknie właściwości Serwera administracyjnego, w sekcji **Ustawienia** zaznacz pole **Otwórz port dla urządzeń mobilnych**, a następnie z listy rozwijalnej wybierz **Dodaj certyfikat**.
  2. W otwartym oknie określ ten sam certyfikat, który został ustawiony na odwrotnym serwerze proxy, gdy punkt dostępu do protokołu mobilnego został opublikowany na Serwerze administracyjnym.

- Certyfikaty użytkownika dla urządzeń KES muszą być wystawione przez urząd certyfikacji (CA) domeny. Należy pamiętać, że jeśli domena zawiera kilka głównych urzędów certyfikacji, certyfikaty użytkownika muszą być wystawione przez urząd certyfikacji, który został ustawiony w publikacji na odwrotnym serwerze proxy.

Możesz upewnić się, że certyfikat użytkownika jest zgodny z wyżej opisanymi wymaganiami przy użyciu jednej z następujących metod:

- Określ specjalny certyfikat użytkownika w kreatorze Nowego pakietu oraz kreatorze instalacji Certyfikatu.
- Zintegruj Serwer administracyjny z infrastrukturą kluczy publicznych domeny oraz zdefiniuj odpowiednie ustawienie w regułach wystawiania certyfikatów:

  1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.
  2. W obszarze roboczym folderu **Certyfikaty** kliknij przycisk **Konfiguruj reguły wydawania certyfikatów**, aby otworzyć okno **Reguły wydawania certyfikatu**.
  3. W sekcji **Integracja z PKI** skonfiguruj integrację z infrastrukturą kluczy publicznych.
  4. W sekcji **Wydawanie certyfikatów dla urządzeń mobilnych** określ źródło certyfikatów.

Poniżej znajduje się przykład konfiguracji delegowania protokołu Kerberos (KCD) z następującymi założeniami:

- Punkt dostępu do protokołu mobilnego na Serwerze administracyjnym jest ustawiony na porcie 13292.
- Nazwa urządzenia z odwrotnym serwerem proxy to firewall.mydom.local.
- Nazwa urządzenia z Serwerem administracyjnym to ksc.mydom.local.
- Nazwa zewnętrznej publikacji punktu dostępu do protokołu mobilnego to kes4mob.mydom.global.

Konto domeny dla Serwera administracyjnego

Należy utworzyć konto domeny (na przykład: KSCMobileSrvcUsr), z poziomu którego będzie uruchamiana usługa Serwera administracyjnego. Konto dla usługi Serwera administracyjnego można określić podczas instalacji Serwera administracyjnego lub poprzez narzędzie klsrvswch. Narzędzie klsrvswch znajduje się w folderze instalacyjnym Serwera administracyjnego. Domyślna ścieżka instalacji: <Disk>:\Program Files (x86)\ Kaspersky Lab\ Kaspersky Security Center.

Konto domeny musi zostać określone z następujących względów:

- Funkcja zarządzania urządzeniami KES jest integralną częścią Serwera administracyjnego.
- Aby zapewnić poprawne działanie delegowania protokołu Kerberos (KCD), strona odbierająca (czyli Serwer administracyjny) musi być uruchomiona z poziomu konta domeny.

Nazwa główna usługi dla http/kes4mob.mydom.local

W domenie, z poziomu konta KSCMobileSrvcUsr, dodaj SPN dla publikacji usługi protokołu mobilnego na porcie 13292 urządzenia z Serwerem administracyjnym. Dla urządzenia kes4mob.mydom.local z Serwerem administracyjnym będzie to wyglądało w następujący sposób:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Konfiguracja właściwości domeny urządzenia z odwrotnym serwerem proxy (firewall.mydom.local)

Aby przeprowadzić ruch sieciowy, przełącz urządzenie z odwrotnym serwerem proxy (firewall.mydom.local) do usługi, która jest definiowana po SPN (http/kes4mob.mydom.local:13292).

W celu przełączenia urządzenia z odwrotnym serwerem proxy do usługi definiowanej po SPN (http/kes4mob.mydom.local:13292), administrator musi wykonać następujące działania:

1. W przystawce Microsoft Management Console o nazwie „Użytkownicy i komputery usługi Active Directory" wybierz urządzenie z zainstalowanym odwrotnym serwerem proxy (firewall.mydom.local).

2. We właściwościach urządzenia, na zakładce **Delegowanie** ustaw przełącznik **Ufaj temu komputerowi w delegowaniu tylko do określonych usług** na **Użyj dowolnego protokołu uwierzytelniania**.

3. Na liście **Usługi, którym to konto może przedstawiać delegowane poświadczenia** dodaj SPN http/kes4mob.mydom.local:13292.

Specjalny (niestandardowy) certyfikat dla publikacji (kes4mob.mydom.global)

Aby opublikować protokół mobilny Serwera administracyjnego, należy wystawić specjalny (niestandardowy) certyfikat dla FQDN kes4mob.mydom.global, a także określić go w miejsce domyślnego certyfikatu serwera w ustawieniach protokołu mobilnego Serwera administracyjnego, w Konsoli administracyjnej. W tym celu, w oknie właściwości Serwera administracyjnego, w sekcji **Ustawienia** zaznacz pole **Otwórz port dla urządzeń mobilnych**, a następnie z listy rozwijalnej wybierz **Dodaj certyfikat**.

Należy pamiętać, że kontener certyfikatów serwera (plik z rozszerzeniem .p12 lub .pfx) musi także zawierać łańcuch certyfikatów głównych (klucze publiczne).

Konfiguracja publikacji na odwrotnym serwerze proxy

Na odwrotnym serwerze proxy, dla ruchu przechodzącego z urządzenia mobilnego do portu 13292 usługi kes4mob.mydom.global należy skonfigurować KCD na SPN (http/kes4mob.mydom.local:13292), korzystając z certyfikatu serwera opublikowanego dla FQDN kes4mob.mydom.global. Nie można zapominać, że publikacja oraz opublikowany punkt dostępu (port 13292 Serwera administracyjnego) powinny korzystać z tego samego certyfikatu serwera.

Korzystanie z Firebase Cloud Messaging

Aby zapewnić dostarczanie w odpowiednim momencie poleceń na urządzenia KES działające pod systemem operacyjnym Android, Kaspersky Security Center korzysta z mechanizmów powiadomień push. Powiadomienia push są wymieniane pomiędzy urządzeniami KES a Serwerem administracyjnym za pośrednictwem usługi Firebase Cloud Messaging (zwanej dalej FCM). W Konsoli administracyjnej Kaspersky Security Center możesz określić ustawienia Firebase Cloud Messaging do podłączania urządzeń KES do usługi.

Aby pobrać ustawienia Firebase Cloud Messaging, należy posiadać konto Google.

W celu włączenia korzystania z FCM:

1. W Konsoli administracyjnej wybierz węzeł **Zarządzanie urządzeniami mobilnymi** oraz folder **Urządzenia mobilne**.

2. Z otwartego menu kontekstowego folderu **Urządzenia mobilne** wybierz **Właściwości**.

3. We właściwościach folderu wybierz sekcję **Ustawienia Firebase Cloud Messaging**.

4. W polu **Numer projektu Firebase** podaj identyfikator nadawcy FCM.

5. W polu **Plik klucza prywatnego (w formacie JSON)** wybierz plik klucza prywatnego.

   Przy kolejnej synchronizacji z Serwerem administracyjnym, urządzenia KES, działające pod systemami operacyjnymi Android, zostaną połączone z Firebase Cloud Messaging.

Możesz zmodyfikować ustawienia Firebase Cloud Messaging, klikając przycisk **Resetuj ustawienia**.

Po przejściu do innego projektu Firebase musisz poczekać 10 minut na wznowienie FCM.

Usługa FCM działa w następujących zakresach adresów:

- Ze strony urządzenia KES dostęp jest wymagany do portów 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) oraz 5230 (HTTPS) dla następujących adresów:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Wszystkie adresy IP w ASN Google'a dla portu 15169
- Ze strony Serwera administracyjnego dostęp jest wymagany do portu 443 (HTTPS) dla następujących adresów:
  - fcm.googleapis.com
  - Wszystkie adresy IP w ASN Google'a dla portu 15169

Jeśli ustawienia serwera proxy (**Zaawansowane** / **Konfiguracja dostępu do internetu**) zostały określone we właściwościach Serwera administracyjnego w Konsoli administracyjnej, będą używane do interakcji z FCM.

Konfigurowanie FCM: pobieranie ID nadawcy i pliku klucza prywatnego

W celu skonfigurowania FCM:

1. Zarejestruj się na portalu Google.
2. Przejdź do konsoli Firebase.
3. Wykonaj jedną z poniższych czynności:
   - Aby utworzyć nowy projekt, kliknij **Utwórz projekt** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
   - Otwórz istniejący projekt.
4. Kliknij ikonę koła zębatego i wybierz opcję **Ustawienia projektu**.
   Zostanie otwarte okno **Ustawienia projektu**.
5. Wybierz zakładkę **Cloud Messaging**.
6. Pobierz odpowiedni identyfikator nadawcy z pola **ID nadawcy** w sekcji **Firebase Cloud Messaging API (V1)**.

7. Wybierz zakładkę **Konta usług** i kliknij **Wygeneruj nowy klucz prywatny**.

8. W oknie, które zostanie otwarte, kliknij opcję **Generuj klucz**, aby wygenerować i pobrać plik klucza prywatnego.

Usługa Firebase Cloud Messaging jest teraz skonfigurowana.

Integracja z infrastrukturą kluczy publicznych

Integracja z infrastrukturą kluczy publicznych (zwana również PKI) jest przeznaczona głównie do uproszenia wystawiania certyfikatów użytkownika domeny przez Serwer administracyjny.

Administrator może przypisać certyfikat domeny dla użytkownika w Konsoli administracyjnej. Można to zrobić przy użyciu jednej z następujących metod:

- Przydziel użytkownikowi specjalny (niestandardowy) certyfikat z pliku w kreatorze instalacji certyfikatu.
- Przeprowadź integrację z PKI i wskaż PKI jako źródło certyfikatów dla określonego typu certyfikatów lub dla wszystkich typów certyfikatów.

Ustawienia integracji z PKI są dostępne w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** po kliknięciu odnośnika **Zintegruj z infrastrukturą klucza publicznego**.

Ogólne zasady integracji z PKI dla publikacji certyfikatów użytkownika domeny

W Konsoli administracyjnej, w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** kliknij odnośnik **Zintegruj z infrastrukturą klucza publicznego**, aby określić konto domeny, które będzie używane przez Serwer administracyjny do wystawiania certyfikatów użytkownika domeny poprzez urząd certyfikacji domeny (zwany również kontem, z poziomu którego wykonywana jest integracja z PKI).

Należy pamiętać, że:

- Ustawienia integracji z PKI oferują możliwość określenia domyślnego szablonu dla wszystkich typów certyfikatów. Nie wolno też zapominać, że reguły wydawania certyfikatów (dostępne w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** po kliknięciu przycisku **Konfiguruj reguły wydawania certyfikatów**) pozwalają na określenie indywidualnego szablonu dla każdego typu certyfikatu.
- Specjalny certyfikat Agenta rejestracji (EA) powinien zostać zainstalowany na urządzeniu z Serwerem administracyjnym, w repozytorium certyfikatów konta, z poziomu którego wykonywana jest integracja z PKI. Certyfikat Agenta rejestracji (EA) jest wystawiany przez administratora urzędu certyfikacji domeny (CA).

Konto, z poziomu którego wykonywana jest integracja z PKI, musi spełniać następujące kryteria.

- Jest to użytkownik domeny.
- Jest to lokalny administrator urządzenia z Serwerem administracyjnym, z poziomu którego została zainicjowana integracja z PKI.
- Posiada uprawnienie do *Zalogowania w trybie usługi*.
- Urządzenie z zainstalowanym Serwerem administracyjnym musiało być wcześniej uruchomione przynajmniej raz z poziomu tego konta w celu utworzenia trwałego profilu użytkownika.

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (zwany również serwerem sieciowym) jest składnikiem Kaspersky Security Center. Serwer sieciowy został zaprojektowany do publikowania autonomicznych pakietów instalacyjnych, autonomicznych pakietów instalacyjnych dla urządzeń mobilnych, profili iOS MDM oraz plików z folderu współdzielonego.

Profile iOS MDM oraz utworzone pakiety instalacyjne są automatycznie publikowane na serwerze sieciowym, a następnie są usuwane po pierwszym pobraniu. Administrator może wysłać użytkownikowi nowy odnośnik w dowolny sposób, na przykład za pośrednictwem poczty elektronicznej.

Klikając odnośnik, użytkownik może pobrać żądane informacje na urządzenie mobilne.

Ustawienia serwera sieciowego

Jeśli wymagane jest dostrojenie serwera sieciowego, właściwości serwera sieciowego w Konsoli administracyjnej oferują możliwość zmiany portów dla HTTP (8060) i HTTPS (8061). Oprócz zmiany portów, możesz zastąpić certyfikat serwera dla HTTPS i zmienić FQDN serwera sieciowego dla HTTP.

Instalacja Kaspersky Security Center

Ta sekcja opisuje instalację modułów programu Kaspersky Security Center. Jeśli chcesz zainstalować aplikację lokalnie tylko na jednym urządzeniu, dostępne są dwie opcje instalacji:

- **Standardowa**. Ta opcja jest zalecana, jeśli chcesz wypróbować Kaspersky Security Center, na przykład, poprzez przetestowanie działania aplikacji w małym obszarze wewnątrz sieci firmowej. Podczas instalacji standardowej konfigurujesz tylko bazę danych. Możesz także zainstalować tylko domyślny zestaw wtyczek administracyjnych dla aplikacji Kaspersky. Możesz także użyć standardowej instalacji, jeśli już masz doświadczenie w pracy z Kaspersky Security Center i jesteś w stanie określić wszystkie odpowiednie ustawienia po standardowej instalacji.

- **Niestandardowa**. Ta opcja jest zalecana, jeśli planujesz zmodyfikować ustawienia Kaspersky Security Center, takie jak: ścieżka dostępu do folderu współdzielonego, konta i porty dla połączenia z Serwerem administracyjnym oraz ustawienia bazy danych. Instalacja niestandardowa umożliwia określenie, które wtyczki administracyjne Kaspersky mają zostać zainstalowane. Jeśli to konieczne, możesz uruchomić instalację niestandardową w trybie cichym.

Jeśli w sieci jest zainstalowany przynajmniej jeden Serwer administracyjny, Serwery mogą być zdalnie instalowane na innych urządzeniach poprzez zadanie zdalnej instalacji przy użyciu instalacji wymuszonej. Podczas tworzenia zadania zdalnej instalacji należy użyć pakietu instalacyjnego Serwera administracyjnego: ksc_<version_number>.<build number>_full_<localization language>.exe.

Użyj tego pakietu, jeśli chcesz zainstalować wszystkie komponenty niezbędne do zapewnienia pełnej funkcjonalności Kaspersky Security Center lub do zaktualizowania bieżących wersji tych komponentów.

Jeśli chcesz wdrożyć klaster trybu failover Kaspersky Security Center, musisz zainstalować Kaspersky Security Center na wszystkich węzłach klastra.

Przygotowanie do instalacji

Przed uruchomieniem instalacji wykonaj następujące czynności.

- **Sprawdź wymagania sprzętowe i programowe**

  Upewnij się, że sprzęt i oprogramowanie urządzenia spełniają wymagania dla Serwera administracyjnego i Konsoli administracyjnej.

- **Wybierz i zainstaluj system zarządzania bazą danych (DBMS)**

  Kaspersky Security Center przechowuje swoje informacje w bazie danych zarządzanej przez DBMS. Zainstaluj DBMS w sieci przed Kaspersky Security Center (dowiedz się więcej o tym, jak wybrać DBMS). Jeśli zdecydujesz się zainstalować PostgreSQL lub Postgres Pro DBMS, podaj hasło dla superużytkownika. Jeśli hasło nie zostanie określone, Serwer administracyjny może nie być w stanie połączyć się z bazą danych.

  Zaleca się zainstalowanie Serwera administracyjnego na serwerze dedykowanym zamiast na kontrolerze domeny. Jeśli instalujesz Kaspersky Security Center na serwerze, który działa jako kontroler domeny tylko do odczytu (RODC), Microsoft SQL Server (SQL Express) nie może zostać zainstalowany lokalnie (na tym samym urządzeniu). W tym przypadku zalecane jest zdalne zainstalowanie Microsoft SQL Server (SQL Express) (na innym urządzeniu) lub tego, którego używasz — MySQL, MariaDB, lub PostgreSQL — jeśli musisz zainstalować system DBMS lokalnie.

- **Przygotuj foldery dla Serwera administracyjnego, Agenta sieciowego i Konsoli administracyjnej**

  Należy zainstalować Serwer administracyjny, Agenta sieciowego i Konsolę administracyjną w folderach, dla których uwzględnianie wielkości liter jest wyłączone. Dodatkowo, uwzględnianie wielkości liter musi być wyłączone dla folderu współdzielonego Serwera administracyjnego oraz ukrytego folderu Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\adminkit).

- **Usuń starego Agenta sieciowego**

  Wersja serwerowa Agenta sieciowego zostanie zainstalowana na urządzeniu wraz z Serwerem administracyjnym. Serwer administracyjny nie może być zainstalowany wraz ze zwykłą wersją Agenta sieciowego. Jeśli serwerowa wersja Agenta sieciowego jest już zainstalowana na Twoim urządzeniu, usuń ją i ponownie uruchom instalację Serwera administracyjnego. Aby uzyskać szczegółowe informacje na temat wersji serwerowej Agenta sieciowego, zobacz Zmiany w systemie po instalacji Kaspersky Security Center.

- **Sprawdź konta**

  Instalacja Kaspersky Security Center wymaga uprawnień administratora na urządzeniu, na którym ma być ona przeprowadzona.

  Kaspersky Security Center obsługuje zarządzane konta usług i konta usług zarządzane przez grupę. Jeśli te typy kont są używane w Twojej domenie i chcesz określić jedno z nich jako konto dla usługi serwera administracyjnego, najpierw zainstaluj to konto na tym samym urządzeniu, na którym chcesz zainstalować serwer administracyjny. Szczegółowe informacje na temat instalacji zarządzanych kont usług na urządzeniu lokalnym można znaleźć w oficjalnej dokumentacji firmy Microsoft.

Konta do pracy z DBMS

Aby zainstalować Serwer administracyjny i pracować z nim, potrzebujesz konta Windows, z poziomu którego uruchomisz instalator Serwera administracyjnego (zwanego dalej także instalatorem), konta Windows, z poziomu którego uruchomisz usługę Serwera administracyjnego oraz konto wewnętrzne DBMS, aby uzyskać dostęp do DBMS. Możesz tworzyć nowe konta lub korzystać z istniejących. Wszystkie te konta wymagają określonych uprawnień. Zestaw wymaganych kont i ich uprawnień zależy od następujących kryteriów:

- Typ DBMS:
  - Microsoft SQL Server (z uwierzytelnieniem Windows lub uwierzytelnieniem SQL Server)
  - MySQL lub MariaDB
  - PostgreSQL lub Postgres Pro
- Lokalizacja DBMS:
  - **Lokalny DBMS**. *Lokalny system DBMS* to system DBMS zainstalowany na tym samym urządzeniu co Serwer administracyjny.
  - **Zdalny DBMS**. *Zdalny system DBMS* to system DBMS zainstalowany na innym urządzeniu.
- Metoda tworzenia bazy danych Serwera administracyjnego:
  - **Automatyczne**. Podczas instalacji Serwera administracyjnego możesz automatycznie utworzyć bazę danych Serwera administracyjnego (zwaną dalej także bazą danych Serwera) przy użyciu instalatora.
  - **Ręcznie**. Możesz użyć aplikacji innej firmy (na przykład SQL Server Management Studio) lub skryptu, aby utworzyć pustą bazę danych. Następnie możesz określić tę bazę danych jako bazę danych Serwera podczas instalacji Serwera administracyjnego.

Przestrzegaj zasady najmniejszych uprawnień, gdy przyznajesz prawa i uprawnienia do kont. Oznacza to, że przyznane uprawnienia powinny wystarczyć tylko do wykonania wymaganych działań.

Poniższe tabele zawierają informacje o uprawnieniach systemowych i DBMS, które należy nadać kontom przed zainstalowaniem i uruchomieniem Serwera administracyjnego.

Microsoft SQL Server z uwierzytelnianiem Windows

Jeśli wybierzesz SQL Server jako DBMS, możesz użyć uwierzytelniania Windows, aby uzyskać dostęp do SQL Server. Skonfiguruj uprawnienia systemowe konta Windows używanego do uruchamiania instalatora oraz konta Windows używanego do uruchamiania usługi Serwera administracyjnego. W SQL Server utwórz loginy do obu tych kont Windows. W zależności od metody tworzenia bazy danych Serwera, nadaj tym kontom wymagane uprawnienia SQL Server, jak opisano w poniższej tabeli. Aby uzyskać więcej informacji na temat konfigurowania uprawnień kont, zobacz Konfigurowanie kont do pracy z SQL Server (uwierzytelnianie Windows).

DBMS: Microsoft SQL Server (w tym Express Edition) z uwierzytelnianiem systemu Windows

	Automatyczne tworzenie bazy danych (przez instalator)	Ręczne tworzenie bazy danych (przez Administratora)
Konto, z poziomu którego uruchomiony jest instalator	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.
Uprawnienia konta, z poziomu którego uruchomiony jest instalator	• Uprawnienia systemowe: uprawnienia lokalnego administratora. • Uprawnienia SQL Server: • Rola na poziomie serwera: sysadmin.	• Uprawnienia systemowe: uprawnienia lokalnego administratora. • Uprawnienia SQL Server: • Rola na poziomie serwera: publiczna. • Rola członka bazy danych w bazie danych serwera: db_owner, publiczna. • Domyślny schemat bazy danych serwera: dbo.
Konto usługi Serwera administracyjnego	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS. • Lokalny DBMS: • Konto Windows wybrane przez administratora. • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS. • Lokalny DBMS: • Konto Windows wybrane przez administratora. • Konto w formacie KL-AK-*, które instalator tworzy automatycznie (w tym przypadku nie zalecamy generowania konta KL-AK-*).
Uprawnienia dla konta usługi Serwera administracyjnego	• Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator. • Uprawnienia SQL Server: wymagane uprawnienia, przypisane przez instalator.	• Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator. • Uprawnienia SQL Server: • Rola na poziomie serwera: publiczna. • Rola członka bazy danych w bazie danych serwera: db_owner, publiczna. • Domyślny schemat bazy danych serwera: dbo.

Microsoft SQL Server z uwierzytelnieniem SQL Server

Jeśli wybierzesz SQL Server jako DBMS, możesz użyć uwierzytelniania Serwery SQL, aby uzyskać dostęp do SQL Server. Skonfiguruj uprawnienia systemowe konta Windows używanego do uruchamiania instalatora oraz konta Windows używanego do uruchamiania usługi Serwera administracyjnego. W SQL Server utwórz login z hasłem, aby użyć go do uwierzytelnienia. Następnie nadaj temu kontu SQL Server wymagane uprawnienia wymienione w poniższej tabeli. Aby uzyskać więcej informacji na temat konfigurowania uprawnień kont, zobacz Konfigurowanie kont do pracy z SQL Server (uwierzytelnienie SQL Server).

DBMS: Microsoft SQL Server (w tym Express Edition) z uwierzytelnianiem SQL Server

	Automatyczne tworzenie bazy danych (przez instalator)	Ręczne tworzenie bazy danych (przez Administratora)
Konto, z poziomu którego uruchomiony jest instalator	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.

	Automatyczne tworzenie bazy danych (przez instalator)	Ręczne tworzenie bazy danych (przez Administratora)
Uprawnienia konta, z poziomu którego uruchomiony jest instalator	Uprawnienia systemowe: uprawnienia lokalnego administratora.	Uprawnienia systemowe: uprawnienia lokalnego administratora.
Konto usługi Serwera administracyjnego	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS. • Lokalny DBMS: • Konto Windows wybrane przez administratora. • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS. • Lokalny DBMS: • Konto użytkownika Windows wybrane przez administratora. • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.
Uprawnienia dla konta usługi Serwera administracyjnego	Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.	Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.
Prawa logowania używane do uwierzytelniania SQL Server	Uprawnienia SQL Server wymagane do utworzenia bazy danych i zainstalowania Serwera administracyjnego: • Rola na poziomie serwera: publiczna. • Rola członka bazy danych w *głównej* bazie danych: db_owner. • Domyślny schemat *głównej* bazy danych: dbo. • Uprawnienia: • PODŁĄCZ DOWOLNĄ BAZĘ DANYCH • PODŁĄCZ SQL • UTWÓRZ DOWOLNĄ BAZĘ DANYCH • PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH • VIEW SERVER STATE (jeśli włączona jest opcja **Always On**) Uprawnienia SQL Server wymagane do pracy z Serwerem administracyjnym: • Rola na poziomie serwera: publiczna. • Rola członka bazy danych w bazie danych serwera: db_owner. • Domyślny schemat bazy danych serwera: dbo. • Uprawnienia: • PODŁĄCZ SQL • PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH • VIEW SERVER STATE (jeśli włączona jest opcja **Always On**) • WYŚWIETL DOWOLNĄ DEFINICJĘ	Uprawnienia SQL Server: • Rola na poziomie serwera: publiczna. • Rola członka bazy danych w bazie danych serwera: db_owner. • Domyślny schemat bazy danych serwera: dbo. • Uprawnienia: • PODŁĄCZ SQL • PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH • WYŚWIETL DOWOLNĄ DEFINICJĘ

Konfigurowanie uprawnień SQL Server do odzyskiwania danych Serwera administracyjnego

Aby przywrócić dane Serwera administracyjnego z kopii zapasowej, uruchom narzędzie klbackup z poziomu konta Windows użytego do zainstalowania Serwera administracyjnego. Przed uruchomieniem narzędzia klbackup na serwerze SQL Server nadaj uprawnienia do logowania do serwera SQL skojarzonego z tym kontem systemu Windows. Uprawnienia SQL Server różnią się w zależności od wersji Serwera administracyjnego. W przypadku Serwera administracyjnego w wersji 14.2 lub nowszej możesz nadać rolę na poziomie serwera sysadmin lub rolę na poziomie serwera dbcreator.

Uprawnienia SQL Server do odzyskiwania bazy danych Serwera administracyjnego

Serwer administracyjny w wersji 14.2 lub nowszej	Inne wersje Serwera administracyjnego
• Uprawnienia SQL Server: • Rola na poziomie serwera: dbcreator. • Uprawnienia: • WYŚWIETL DOWOLNĄ DEFINICJĘ Przed uruchomieniem narzędzia klbackup określ flagę serwera KLSRV_SKIP_ADJUSTING_DBMS_ACCESS. Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na katalog za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\ Kaspersky Lab\ Kaspersky Security Center. Następnie wykonaj następujące polecenie w wierszu poleceń: `klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL i MariaDB

Jeśli wybierzesz MySQL lub MariaDB jako DBMS, utwórz wewnętrzne konto DBMS i nadaj temu kontu wymagane uprawnienia wymienione w poniższej tabeli. Instalator i usługa Serwera administracyjnego używają tego wewnętrznego konta DBMS do uzyskiwania dostępu do DBMS. Należy pamiętać, że sposób tworzenia bazy danych nie wpływa na zestaw wymaganych uprawnień. Aby uzyskać więcej informacji na temat konfigurowania uprawnień konta, zobacz Konfigurowanie kont do pracy z MySQL i MariaDB.

DBMS: MySQL i MariaDB

	Automatyczne lub ręczne tworzenie bazy danych
Konto, z poziomu którego uruchomiony jest instalator	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.
Uprawnienia konta, z poziomu którego uruchomiony jest instalator	Uprawnienia systemowe: uprawnienia lokalnego administratora.
Konto usługi Serwera administracyjnego	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS. • Lokalny DBMS: • Konto Windows wybrane przez administratora. • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.
Uprawnienia dla konta usługi Serwera administracyjnego	Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.
Uprawnienia konta wewnętrznego DBMS	Uprawnienia dotyczące schematu: • Baza danych Serwera administracyjnego: ALL (oprócz GRANT OPTION). • Schematy systemowe (mysql i sys): SELECT, SHOW VIEW. • Procedura składowana sys.table_exists: EXECUTE (jeśli używasz MariaDB 10.5 lub wcześniejszej jako DBMS, nie musisz nadawać uprawnienia EXECUTE). Globalne uprawnienia dla wszystkich schematów: PROCESS, SUPER.

Szczegółowe informacje na temat przenoszenia danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela można znaleźć w temacie Przenoszenie danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela w systemach DBMS MySQL i MariaDB.

Konfigurowanie uprawnień do odzyskiwania danych Serwera administracyjnego

Uprawnienia nadane wewnętrznemu kontu DBMS wystarczą do przywrócenia danych Serwera administracyjnego z kopii zapasowej. Aby rozpocząć przywracanie, uruchom narzędzie klbackup z poziomu konta Windows użytego do zainstalowania Serwera administracyjnego.

PostgreSQL lub Postgres Pro

Jeśli wybierzesz PostgreSQL lub Postgres Pro jako DBMS, możesz użyć *użytkownika Postgres* (domyślna rola Postgres) lub utworzyć nową rolę Postgres (zwaną dalej także rolą), aby uzyskać dostęp do DBMS. W zależności od metody tworzenia bazy danych Serwera, nadaj roli wymagane uprawnienia zgodnie z opisem w poniższej tabeli. Aby uzyskać więcej informacji na temat konfigurowania uprawnień roli, zobacz Konfigurowanie kont do pracy z PostgreSQL lub Postgres Pro.

DBMS: PostgreSQL lub Postgres Pro

	Automatyczne tworzenie bazy danych		Ręczne tworzenie bazy danych
Konto, z poziomu którego uruchomiony jest instalator	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.		• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.
Uprawnienia konta, z poziomu którego uruchomiony jest instalator	Uprawnienia systemowe: uprawnienia lokalnego administratora.		Uprawnienia systemowe: uprawnienia lokalnego administratora.
Konto usługi Serwera administracyjnego	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS. • Lokalny DBMS: • Konto Windows wybrane przez administratora. • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.		• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS. • Lokalny DBMS: • Konto Windows wybrane przez administratora. • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.
Uprawnienia dla konta usługi Serwera administracyjnego	Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.		Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.
Uprawnienia roli Postgres	Użytkownik *Postgres* nie wymaga dodatkowych uprawnień.	Uprawnienia nowej roli: `CREATEDB`.	Do nowej roli: • Uprawnienia w bazie danych Serwera administracyjnego: `ALL`. • Uprawnienia do wszystkich tabel w schemacie publicznym: `ALL`. • Uprawnienia do wszystkich sekwencji w schemacie publicznym: `ALL`.

Konfigurowanie uprawnień do odzyskiwania danych Serwera administracyjnego

Aby przywrócić dane Serwera administracyjnego z kopii zapasowej, uruchom narzędzie klbackup z poziomu konta Windows użytego do zainstalowania Serwera administracyjnego. Należy pamiętać, że rola Postgres używana do uzyskiwania dostępu do DBMS musi mieć uprawnienia właściciela do bazy danych Serwera administracyjnego.

Konfigurowanie kont do pracy z SQL Server (uwierzytelnianie Windows)

Wymagania wstępne

Przed przypisaniem uprawnień do kont wykonaj następujące czynności:

1. Upewnij się, że logujesz się do systemu na konto administratora lokalnego.
2. Zainstaluj środowisko do pracy z SQL Server.
3. Upewnij się, że posiadasz konto Windows, z poziomu którego zainstalujesz Serwer administracyjny.
4. Upewnij się, że posiadasz konto Windows, z poziomu którego uruchomisz Serwer administracyjny.
5. Na SQL Server utwórz login konta Windows używanego do uruchamiania instalatora Serwera administracyjnego (zwanego dalej instalatorem). Utwórz również login dla konta Windows używanego do uruchamiania usługi Serwera administracyjnego.

Jeśli korzystasz z SQL Server Management Studio, na stronie **Ogólne** okna właściwości logowania wybierz opcję **Uwierzytelnianie systemu Windows**.

Jeśli chcesz zainstalować Serwer administracyjny i SQL Server na urządzeniach, które znajdują się w oddzielnych domenach Windows, pamiętaj, że te domeny muszą mieć obustronne relacje zaufania, aby zapewnić poprawne działanie Serwera administracyjnego, w tym uruchamianie zadań i stosowanie zasad. Aby uzyskać informacje o kontach wymaganych do pracy z różnymi DBMS i uprawnieniach kont, zobacz Konta do pracy z DBMS.

Konfigurowanie kont do instalacji Serwera administracyjnego (automatyczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. W SQL Server przypisz rolę sysadmin na poziomie serwera do loginu konta Windows używanego do uruchomienia instalatora.
2. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.
3. Uruchom instalator Serwera administracyjnego.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.
4. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.
5. Wybierz Microsoft SQL Server jako system DBMS przechowujący bazę danych Serwera administracyjnego.
6. Wybierz tryb Uwierzytelniania systemu Microsoft Windows, aby nawiązać połączenie między Serwerem administracyjnym a serwerem SQL za pośrednictwem konta Windows.

7. Określ nazwę konta Windows, aby uruchomić usługę Serwera administracyjnego.

   Możesz wybrać konto użytkownika systemu Windows, dla którego wcześniej utworzono login SQL Server. Alternatywnie możesz automatycznie utworzyć nowe konto Windows w formacie KL-AK-* za pomocą instalatora. W takim przypadku instalator automatycznie utworzy login SQL Server do tego konta. Niezależnie od wyboru konta, instalator przypisuje wymagane uprawnienia systemowe oraz uprawnienia SQL Server do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji tworzona jest baza danych Serwera, a wszystkie wymagane uprawnienia systemowe i uprawnienia SQL Server są przypisywane do konta usługi Serwera administracyjnego. Serwer administracyjny jest gotowy do użycia.

Konfigurowanie kont do instalacji Serwera administracyjnego (ręczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. Na SQL Server utwórz pustą bazę danych. Ta baza danych będzie używana jako baza danych Serwera administracyjnego (zwana dalej również bazą danych Serwera).

2. Dla obu loginów SQL Server utworzonych dla kont Windows określ rolę na poziomie serwera publicznego, a następnie skonfiguruj mapowanie do utworzonej bazy danych:

   - Rola na poziomie serwera: publiczna
   - Przynależność do roli bazy danych: db_owner, public
   - Domyślny schemat: dbo

3. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.

4. Uruchom instalator Serwera administracyjnego.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

5. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.

6. Wybierz Microsoft SQL Server jako system DBMS przechowujący bazę danych Serwera administracyjnego.

7. Określ nazwę utworzonej bazy danych jako nazwę bazy danych Serwera administracyjnego.

8. Wybierz tryb Uwierzytelniania systemu Microsoft Windows, aby nawiązać połączenie między Serwerem administracyjnym a serwerem SQL za pośrednictwem konta Windows.

9. Określ nazwę konta Windows, aby uruchomić usługę Serwera administracyjnego.

   Możesz wybrać konto użytkownika Windows, dla którego utworzono login SQL Server i wcześniej skonfigurowano prawa logowania.

Nie zalecamy automatycznego tworzenia nowego konta Windows w formacie KL-AK-*. W takim przypadku instalator tworzy nowe konto Windows, do którego nie utworzono i nie skonfigurowano konta SQL Server. Serwer administracyjny nie może użyć tego konta do uruchomienia usługi Serwera administracyjnego. Jeżeli konieczne jest utworzenie konta KL-AK-* Windows, nie uruchamiaj Konsoli administracyjnej po zakończeniu instalacji. Zamiast tego wykonaj następujące czynności:

1. Zatrzymaj usługę kladminserver.
2. Na SQL Server utwórz login SQL Server do utworzonego konta KL-AK-* Windows.
3. Przyznaj prawa do tego loginu SQL Server i skonfiguruj mapowanie do utworzonej bazy danych:
   - Rola na poziomie serwera: publiczna
   - Przynależność do roli bazy danych: db_owner, public
   - Domyślny schemat: dbo
4. Zrestartuj usługę kladminserver, a następnie uruchom Konsolę administracyjną.

Po zakończeniu instalacji Serwer administracyjny użyje utworzonej bazy danych do przechowywania danych Serwera. Serwer administracyjny jest gotowy do użycia.

Konfigurowanie kont do pracy z SQL Server (uwierzytelnianie SQL Server)

Wymagania wstępne

Przed przypisaniem uprawnień do kont wykonaj następujące czynności:

1. Upewnij się, że logujesz się do systemu na konto administratora lokalnego.
2. Zainstaluj środowisko do pracy z SQL Server.
3. Upewnij się, że posiadasz konto Windows, z poziomu którego zainstalujesz Serwer administracyjny.
4. Upewnij się, że posiadasz konto Windows, z poziomu którego uruchomisz Serwer administracyjny.
5. W SQL Server włącz tryb uwierzytelniania SQL Server.

   Jeśli korzystasz z programu SQL Server Management Studio, w oknie Właściwości programu SQL Server na stronie **Zabezpieczenia** wybierz opcję **Tryb uwierzytelniania programu SQL Server i systemu Windows**.

6. W SQL Server utwórz login z hasłem. Instalator Serwera administracyjnego (zwany dalej także instalatorem) oraz usługa Serwera administracyjnego będą używać tego konta SQL Server do uzyskiwania dostępu do SQL Server.

   Jeśli korzystasz z SQL Server Management Studio, na stronie **Ogólne** okna właściwości logowania wybierz opcję **Uwierzytelnianie SQL Server.**

Jeśli chcesz zainstalować Serwer administracyjny i SQL Server na urządzeniach, które znajdują się w oddzielnych domenach Windows, pamiętaj, że te domeny muszą mieć obustronne relacje zaufania, aby zapewnić poprawne działanie Serwera administracyjnego, w tym uruchamianie zadań i stosowanie zasad. Aby uzyskać informacje o kontach wymaganych do pracy z różnymi DBMS i uprawnieniach kont, zobacz Konta do pracy z DBMS.

Konfigurowanie kont do instalacji Serwera administracyjnego (automatyczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. W SQL Server zamapuj konto SQL Server na domyślną *główną* bazę danych. *Główna* baza danych będzie używana jako baza danych Serwera administracyjnego (zwana dalej również bazą danych Serwera). Główna *baza* danych jest używana do mapowania, dopóki instalator nie utworzy bazy danych Serwera. Przyznaj następujące prawa i uprawnienia do konta SQL Server:

   - Rola na poziomie serwera: publiczna
   - Rola członka bazy danych w *głównej* bazie danych: db_owner
   - Domyślny schemat *głównej* bazy danych: dbo
   - Uprawnienia:
     - PODŁĄCZ DOWOLNĄ BAZĘ DANYCH
     - PODŁĄCZ SQL
     - UTWÓRZ DOWOLNĄ BAZĘ DANYCH
     - PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH

2. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.

3. Uruchom instalator.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

4. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.

5. Wybierz Microsoft SQL Server jako system DBMS przechowujący bazę danych Serwera administracyjnego.

6. Określ Nazwa bazy danych Serwera administracyjnego.

7. Wybierz tryb Uwierzytelniania SQL Server, aby nawiązać połączenie między Serwerem administracyjnym a SQL Server za pośrednictwem utworzonego konta SQL Server. Następnie określ poświadczenia konta SQL Server.

8. Określ nazwę konta Windows, aby uruchomić usługę Serwera administracyjnego.

   Możesz wybrać istniejące konto użytkownika Windows lub utworzyć nowe konto Windows w formacie KL-AK-* za pomocą instalatora. Niezależnie od wyboru konta instalator przypisuje wymagane uprawnienia systemowe do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji tworzona jest baza danych Serwera i wszystkie wymagane uprawnienia systemowe są przypisywane do konta usługi Serwera administracyjnego. Serwer administracyjny jest gotowy do użycia.

Możesz anulować mapowanie do *głównej* bazy danych, ponieważ instalator utworzył bazę danych Serwera i skonfigurował mapowanie do tej bazy danych podczas instalacji Serwera administracyjnego.

Ponieważ automatyczne tworzenie bazy danych wymaga większych uprawnień niż normalna praca z Serwerem administracyjnym, możesz cofnąć niektóre uprawnienia. Na SQL Server wybierz konto SQL Server, a następnie nadaj następujące uprawnienia do pracy z Serwerem administracyjnym:

- Rola na poziomie serwera: publiczna
- Rola członka bazy danych w bazie danych serwera: db_owner
- Domyślny schemat bazy danych serwera: dbo
- Uprawnienia:
  - PODŁĄCZ SQL
  - PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH

Konfigurowanie kont do instalacji Serwera administracyjnego (ręczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. Na SQL Server utwórz pustą bazę danych. Ta baza danych będzie używana jako baza danych Serwera administracyjnego.
2. W SQL Server przyznaj następujące prawa i uprawnienia do konta SQL Server:
   - Rola na poziomie serwera: publiczna.
   - Rola członka bazy danych w utworzonej bazie danych: db_owner.
   - Domyślny schemat utworzonej bazy danych: dbo.
   - Uprawnienia:
     - PODŁĄCZ SQL
     - PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH
3. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.
4. Uruchom instalator.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

5. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.
6. Wybierz Microsoft SQL Server jako system DBMS przechowujący bazę danych Serwera administracyjnego.
7. Określ nazwę utworzonej bazy danych jako nazwę bazy danych Serwera administracyjnego.
8. Wybierz tryb Uwierzytelniania SQL Server, aby nawiązać połączenie między Serwerem administracyjnym a SQL Server za pośrednictwem utworzonego konta SQL Server. Następnie określ poświadczenia konta SQL Server.
9. Określ nazwę konta Windows, aby uruchomić usługę Serwera administracyjnego.

   Możesz wybrać istniejące konto użytkownika Windows lub utworzyć nowe konto Windows w formacie KL-AK-* za pomocą instalatora. Niezależnie od wyboru konta instalator przypisuje wymagane uprawnienia systemowe do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji Serwer administracyjny użyje utworzonej bazy danych do przechowywania danych Serwera administracyjnego. Wszystkie wymagane uprawnienia systemowe są przypisane do konta usługi Serwera administracyjnego. Serwer administracyjny jest gotowy do użycia.

Konfiguracja kont do pracy z MySQL i MariaDB

Wymagania wstępne

Przed przypisaniem uprawnień do kont wykonaj następujące czynności:

1. Upewnij się, że logujesz się do systemu na konto administratora lokalnego.
2. Zainstaluj środowisko do pracy z MySQL lub MariaDB.
3. Upewnij się, że posiadasz konto Windows, z poziomu którego zainstalujesz Serwer administracyjny.
4. Upewnij się, że posiadasz konto Windows, z poziomu którego uruchomisz Serwer administracyjny.

Konfigurowanie kont do instalacji Serwera administracyjnego

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. Uruchom środowisko do pracy z MySQL lub MariaDB na koncie root, które utworzono podczas instalacji DBMS.

2. Utwórz wewnętrzne konto DBMS z hasłem. Instalator Serwera administracyjnego (zwany dalej także instalatorem) oraz usługa Serwera administracyjnego będą używać tego wewnętrznego konta DBMS do uzyskiwania dostępu do DBMS. Nadaj temu kontu następujące uprawnienia:

   - Uprawnienia dotyczące schematu:
     - Baza danych Serwera administracyjnego: ALL (oprócz `GRANT OPTION`)
     - Schematy systemowe (mysql i sys): `SELECT`, `SHOW VIEW`
     - Procedura składowana sys.table_exists: `EXECUTE`
   - Globalne uprawnienia dla wszystkich schematów: `PROCESS`, `SUPER`

   Aby utworzyć wewnętrzne konto DBMS i nadać mu wymagane uprawnienia, uruchom poniższy skrypt (w tym skrypcie login DBMS to *KSCAdmin*, a nazwa bazy danych Serwera administracyjnego to *kav*):

   ```
   /* Utwórz użytkownika o nazwie KSCAdmin */
   CREATE USER 'KSCAdmin'
   /* Określ hasło KSCAdmin */
   IDENTIFIED BY '<hasło>';
   ```

   Jeśli używasz MySQL 8.0 lub starszego jako DBMS, pamiętaj, że dla tych wersji uwierzytelnianie „Caching SHA2 password" nie jest obsługiwane. Zmień domyślne uwierzytelnianie z „Caching SHA2 password" na „Native password MySQL":

   - Aby utworzyć konto DBMS korzystające z uwierzytelniania „Natywne hasło MySQL", wykonaj następujące polecenie:

     ```
     CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<hasło>';
     ```

   - Aby zmienić uwierzytelnianie dla istniejącego konta DBMS, wykonaj następujące polecenie:

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<hasło>';
     ```

   ```
   /* Przyznaj uprawnienia KSCAdmin */
   GRANT USAGE ON *.* TO 'KSCAdmin';
   GRANT ALL ON kav.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
   GRANT PROCESS ON *.* TO 'KSCAdmin';
   GRANT SUPER ON *.* TO 'KSCAdmin';
   ```

Jeśli używasz MariaDB 10.5 lub wersji starszej jako DBMS, nie musisz nadawać uprawnienia EXECUTE. W takim przypadku wyklucz następujące polecenie ze skryptu: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`.

3. Aby wyświetlić listę uprawnień nadanych kontu DBMS, uruchom następujący skrypt:

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. Aby utworzyć bazę danych Serwera administracyjnego, uruchom następujący skrypt (w tym skrypcie nazwa bazy danych Serwera administracyjnego to *kav*):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   Użyj tej samej nazwy bazy danych co określona w skrypcie tworzącym konto DBMS.

5. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.

6. Uruchom instalator.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

7. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.

8. Wybierz MySQL lub MariaDB jako system DBMS przechowujący bazę danych Serwera administracyjnego.

9. Określ Nazwa bazy danych Serwera administracyjnego. Użyj tej samej nazwy bazy danych co określona w skrypcie.

10. Określ poświadczenia konta DBMS utworzonego przez skrypt.

11. Określ nazwę konta Windows, aby uruchomić usługę Serwera administracyjnego.

    Możesz wybrać istniejące konto użytkownika systemu Windows lub automatycznie utworzyć nowe konto systemu Windows w formacie KL-AK-* za pomocą instalatora. Niezależnie od wyboru konta instalator przypisuje wymagane uprawnienia systemowe do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji baza danych Serwera administracyjnego jest tworzona i Serwer administracyjny jest gotowy do użycia.

Przenoszenie danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela w systemach DBMS MySQL lub MariaDB

W przypadku systemów DBMS MySQL i MariaDB dane można przechowywać w następujący sposób:

- Jako współdzielona przestrzeń tabel, gdy dane wszystkich baz danych użytkownika są przechowywane w jednym pliku (zwykle w pliku `ibdata1`).
- Jako przestrzeń tabel typu plik-tabela, gdy dla każdej tabeli tworzona jest oddzielna przestrzeń danych jako oddzielny plik.

Korzystanie ze współdzielonej przestrzeni tabel zwiększa ryzyko fragmentacji przestrzeni tabel. Ponieważ nie da się wykonać operacji `SHRINK`, plik w przestrzeni tabel współdzielonych może zająć około 90% miejsca na dysku. Ma to negatywny wpływ na wydajność podsystemu dyskowego. Dlatego też warto zdecydować się na przestrzeń tabel typu plik-tabela.

W tym artykule opisano sposób przenoszenia danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela. Jeśli systemy DBMS MySQL lub MariaDB są używane również przez inne aplikacje, należy przenieść bazy danych tych aplikacji do przestrzeni tabel typu plik-tabela.

> Zalecamy wykonywanie tej procedury tylko wtedy, gdy na potrzeby Serwera administracyjnego używany jest system DBMS MySQL lub MariaDB.
> Przeniesienie danych ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela może zwiększyć obciążenie podsystemu dyskowego.

Wymagania wstępne

Zanim zaczniesz, upewnij się, że:

- Utworzyłeś kopię zapasową danych Serwera administracyjnego, uruchamiając zadanie tworzenia kopii zapasowej danych lub narzędzie klbackup.
- Utworzyłeś kopię zapasową innych aplikacji, których bazy danych są zarządzane przez system DBMS MySQL lub MariaDB (jeśli dotyczy).
- Na urządzeniu z zainstalowanym systemem DBMS, na partycji z bazą danych, znajduje się wolna przestrzeń dyskowa.

Wymagana ilość miejsca na dysku wynosi 150% bieżącego całkowitego rozmiaru bazy danych (bieżący rozmiar pliku `ibdata1`).

Proces

Aby przenieść dane ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela:

1. Zatrzymaj usługę Serwer administracyjny Kaspersky Security Center i inne aplikacje korzystające z instancji systemu DBMS, dla którego chcesz wykonać tę procedurę.
2. Zaloguj się do systemu DBMS jako superużytkownik, a następnie w dowolnej dogodnej aplikacji uruchom skrypt `fix_tablespace.sql`.

   Możesz wyświetlać skrypty `fix_tablespace.sql` klikając te odnośniki:

   Wyświetl skrypt dla MySQL 5.7 i MariaDB 10.1+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
```

```
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Wyświetl skrypt dla MySQL 8.0+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Nie wolno przerywać wykonywania skryptu.
Jeśli nie wystąpiły błędy DBMS, ale przerwano wykonywanie skryptu, należy uruchomić skrypt ponownie albo przerwać wykonywanie czynności opisanych w tej procedurze, ponownie uruchomić usługę DBMS i przywrócić dane Serwera administracyjnego z kopii zapasowej.

3. W sekcji `[mysqld]` pliku my.cnf ustaw parametr `innodb_file_per_table` na `1`.

4. Uruchom ponownie usługę MySQL lub MariaDB.

5. Uruchom ponownie usługę Serwera administracyjnego Kaspersky Security Center.

Dane są przenoszone ze współdzielonej przestrzeni tabel do przestrzeni tabel typu plik-tabela.

Konfiguracja kont do pracy z PostgreSQL i Postgres Pro

Wymagania wstępne

Przed przypisaniem uprawnień do kont wykonaj następujące czynności:

1. Upewnij się, że logujesz się do systemu na konto administratora lokalnego.
2. Zainstaluj środowisko do pracy z PostgreSQL i Postgres Pro.
3. Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center 15.1.
4. Upewnij się, że posiadasz konto Windows, z poziomu którego zainstalujesz Serwer administracyjny.
5. Upewnij się, że posiadasz konto Windows, z poziomu którego uruchomisz Serwer administracyjny.

Konfigurowanie kont do instalacji Serwera administracyjnego (automatyczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. Uruchom środowisko do pracy z PostgreSQL i Postgres Pro.
2. Wybierz rolę Postgres, aby uzyskać dostęp do DBMS. Możesz wybrać jedną z następujących opcji:
   - Użytkownik *Postgres* (domyślna rola Postgres).

     Jeśli używasz użytkownika *Postgres*, nie musisz nadawać mu dodatkowych uprawnień.
   - Nowa rola Postgres.

     Jeśli chcesz użyć nowej roli Postgres, utwórz tę rolę, a następnie nadaj jej uprawnienie CREATEDB. W tym celu uruchom następujący skrypt (w tym skrypcie rolą jest *KSCAdmin*):

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<password>' CREATEDB;
     ```

     Utworzona rola będzie używana jako właściciel bazy danych Serwera administracyjnego (zwanej dalej również Bazą danych Serwera).
3. Zaloguj się do systemu z poziomu konta Windows używanego do uruchomienia instalatora Serwera administracyjnego (zwanego dalej także instalatorem).
4. Uruchom instalator.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.
5. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.

6. Wybierz PostgreSQL lub Postgres Pro jako system DBMS przechowujący bazę danych Serwera administracyjnego.

7. Określ Nazwa bazy danych Serwera. Instalator automatycznie utworzy bazę danych Serwera.

8. Określ poświadczenia roli Postgres.

9. Określ nazwę konta Windows, aby uruchomić usługę Serwera administracyjnego.

   Możesz wybrać istniejące konto użytkownika systemu Windows lub automatycznie utworzyć nowe konto systemu Windows w formacie KL-AK-* za pomocą instalatora. Niezależnie od wyboru konta instalator przypisuje wymagane uprawnienia systemowe do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji baza danych Serwera jest tworzona automatycznie i Serwer administracyjny jest gotowy do użycia.

Konfigurowanie kont do instalacji Serwera administracyjnego (ręczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. Uruchom środowisko do pracy z Postgres.

2. Zaloguj się jako użytkownik *Postgres* w bazie danych *Postgres*.

3. Utwórz nową rolę Postgres (w tym przykładzie jest to rola *KSCAdmin*):

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<password>';
   ```

4. Utwórz bazę danych serwera administracyjnego (w tym przykładzie, nazwa bazy danych Serwera administracyjnego to *KAV*):

   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

   Jeżeli pojawi się błąd „Nowe kodowanie (UTF8) jest niezgodne z kodowaniem bazy szablonów" utwórz bazę danych za pomocą polecenia:
   `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;`
   zamiast:
   `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";`

5. Następnie nadaj roli wszystkie uprawnienia w bazie danych Serwera administracyjnego:

   ```
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   Upewnij się, że rola ma domyślne uprawnienia CONNECT i TEMPORARY w bazie danych Serwera administracyjnego.

6. Nadaj następujące uprawnienia utworzonej roli Postgres:

   - Uprawnienia do wszystkich tabel w schemacie publicznym: ALL
   - Uprawnienia do wszystkich sekwencji w schemacie publicznym: ALL

   W tym celu zaloguj się jako użytkownik *Postgres* w bazie danych Serwera i uruchom następujący skrypt (w tym skrypcie rola to *KSCAdmin*):

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

7. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.
8. Uruchom instalator Serwera administracyjnego.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

9. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.
10. Wybierz PostgreSQL lub Postgres Pro jako system DBMS przechowujący bazę danych Serwera administracyjnego.
11. Określ Nazwa bazy danych Serwera. Użyj tej samej nazwy bazy danych co określona w skrypcie. Należy pamiętać, że w nazwie bazy danych rozróżniana jest wielkość liter.
12. Określ poświadczenia roli Postgres.
13. Określ nazwę konta Windows, aby uruchomić usługę Serwera administracyjnego.

    Możesz wybrać istniejące konto użytkownika systemu Windows lub automatycznie utworzyć nowe konto systemu Windows w formacie KL-AK-* za pomocą instalatora. Niezależnie od wyboru konta instalator przypisuje wymagane uprawnienia systemowe do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji Serwer administracyjny użyje utworzonej bazy danych do przechowywania danych Serwera administracyjnego. Serwer administracyjny jest gotowy do użycia.

Scenariusz: Autoryzacja Microsoft SQL Server

Informacje w tej sekcji są stosowane tylko do konfiguracji, w których Kaspersky Security Center używa Microsoft SQL Server jako systemu zarządzania bazą danych.

Aby chronić dane Kaspersky Security Center przesyłane do lub z bazy danych oraz dane przechowywane w bazie danych przed nieautoryzowanym dostępem, musisz zabezpieczyć komunikację między Kaspersky Security Center a SQL Server. Najbardziej rozsądny sposób zapewnienia bezpiecznej komunikacji to zainstalowanie Kaspersky Security Center i SQL Server na tym samym urządzeniu i używanie mechanizmu pamięci współużytkowanej dla obu aplikacji. We wszystkich pozostałych przypadkach zalecane jest użycie certyfikatu SSL lub TLS do autoryzacji instancji SQL Server. Możesz użyć certyfikatu z zaufanego urzędu certyfikacji lub certyfikatu z podpisem własnym. Zalecane jest użycie certyfikatu z zaufanego urzędu certyfikacji, ponieważ certyfikat z podpisem własnym zapewnia tylko ograniczoną ochronę.

Autoryzacja SQL Server odbywa się w etapach:

1. **Generowanie certyfikatu SSL lub TLS z podpisem własnym dla SQL Server zgodnie z wymaganiami certyfikatu**

   Jeśli już posiadasz certyfikat dla SQL Server, pomiń ten krok.

   Certyfikat SSL jest stosowany tylko do wersji SQL Server wcześniejszych niż 2016 (13.x). W SQL Server 2016 (13.x) i nowszych wersjach użyj certyfikatu TLS.

   Na przykład, aby wygenerować certyfikat TLS, wprowadź następujące polecenie w PowerShell:

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

   W poleceniu zamiast SQL_HOST_NAME należy wpisać nazwę hosta SQL Server, jeśli host znajduje się w domenie lub wpisz *w pełni kwalifikowaną nazwę domeny* (FQDN) hosta, jeśli host nie znajduje się w domenie. Taka sama nazwa — nazwa hosta lub FQDN — musi być określona jako nazwa instancji SQL Server w kreatorze instalacji Serwera administracyjnego.

2. **Dodawanie certyfikatu na instancji SQL Server**

   Instrukcje dla tego etapu zależą od platformy, na której uruchomiony jest SQL Server. Więcej informacji można znaleźć w oficjalnej dokumentacji:

   - Windows
   - Linux
   - Amazon Relational Database Service

   Aby użyć certyfikatu na klastrze typu failover, należy zainstalować certyfikat na każdym węźle klastra typu failover. Więcej informacji znajdziesz w dokumentacji Microsoft.

3. **Przypisywanie uprawnień konta usługi**

   Upewnij się, że konto usługi, z poziomu którego usługa SQL Server jest uruchomiona, posiada uprawnienie dostępu Pełna kontrola do kluczy prywatnych. Więcej informacji znajdziesz w dokumentacji Microsoft.

4. **Dodawanie certyfikatu do listy zaufanych certyfikatów dla Kaspersky Security Center**

   Na urządzeniu Serwer administracyjny dodaj certyfikat do listy zaufanych certyfikatów. Więcej informacji znajdziesz w dokumentacji Microsoft.

5. **Włączanie połączeń szyfrowanych między instancją SQL Server a Kaspersky Security Center**

   Na urządzeniu Serwera administracyjnego ustaw wartość `1` dla zmiennej środowiskowej `KLDBADO_UseEncryption`. Na przykład, w systemie Windows Server 2012 R2 możesz zmienić zmienne środowiskowe, klikając **Zmienne środowiskowe** na zakładce **Zaawansowane** okna **Właściwości systemu**. Dodaj nową zmienną, nazwij ją `KLDBADO_UseEncryption`, a następnie ustaw wartość `1`.

6. **Dodatkowa konfiguracja do użycia protokołu TLS 1.2**

   Jeśli używasz protokołu TLS 1.2, wówczas dodatkowo wykonaj następujące czynności:

   - Upewnij się, że zainstalowana wersja SQL Server to 64-bitowa aplikacja.
   - Zainstaluj sterownik Microsoft OLE DB Driver na urządzeniu Serwera administracyjnego. Więcej informacji znajdziesz w dokumentacji Microsoft.

- Na urządzeniu Serwera administracyjnego ustaw wartość `1` dla zmiennej środowiskowej `KLDBADO_UseMSOLEDBSQL`. Na przykład, w systemie Windows Server 2012 R2 możesz zmienić zmienne środowiskowe, klikając **Zmienne środowiskowe** na zakładce **Zaawansowane** okna **Właściwości systemu**. Dodaj nową zmienną, nazwij ją `KLDBADO_UseMSOLEDBSQL`, a następnie ustaw wartość `1`.

  Jeśli wersja sterownika OLE DB to 19 lub nowsza, ustaw również wartość `MSOLEDBSQL19` na zmienną środowiskową `KLDBADO_ProviderName`.

7. **Włączanie użycia protokołu TCP/IP na nazwanej instancji SQL Server**

   Jeśli używasz nazwanej instancji SQL Server, dodatkowo włącz użycie protokołu TCP/IP i przypisz numer portu TCP/IP do aparatu bazy danych SQL Server. Jeśli skonfigurujesz połączenie SQL Server w kreatorze instalacji Serwera administracyjnego, określ numer portu oraz nazwę hosta SQL Server w polu **Nazwa instancji SQL Server**.

Scenariusz: uwierzytelnianie serwera MySQL

Zalecamy użycie certyfikatu TLS do uwierzytelnienia serwera MySQL. Możesz użyć certyfikatu z zaufanego urzędu certyfikacji lub certyfikatu z podpisem własnym.

Serwer administracyjny obsługuje zarówno jednokierunkowe, jak i dwukierunkowe uwierzytelnianie SSL dla MySQL.

Włącz jednokierunkowe uwierzytelnianie SSL

Wykonaj poniższe kroki, aby skonfigurować jednokierunkowe uwierzytelnianie SSL dla MySQL:

1. **Wygeneruj certyfikat TLS z podpisem własnym dla serwera MySQL**

   W programie PowerShell zmień katalog na folder, w którym chcesz przechowywać certyfikaty. Wykonaj następujące polecenia:

```
$CertCA = New-SelfSignedCertificate `
-Subject "CN=CertCA" `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-NotAfter (Get-Date).AddDays(365)

$CertCABase64 = [System.Convert]::ToBase64String($CertCA.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeaf = New-SelfSignedCertificate `
-Subject "CN=CertLeaf" `
-Signer $CertCA `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-KeyExportPolicy Exportable `
-NotAfter (Get-Date).AddDays(365)

$CertLeafBase64 = [System.Convert]::ToBase64String($CertLeaf.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeafRSACng =
[System.Security.Cryptography.X509Certificates.RSACertificateExtensions]::GetRSAPrivateKey($CertLeaf)
$CertLeafKeyBytes =
$CertLeafRSACng.Key.Export([System.Security.Cryptography.CngKeyBlobFormat]::Pkcs8PrivateBlob)
$CertLeafKeyBase64 = [System.Convert]::ToBase64String($CertLeafKeyBytes,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertCAPemCert = @"
-----BEGIN CERTIFICATE-----
$CertCABase64
-----END CERTIFICATE-----
"@

$CertLeafPemKey = @"
-----BEGIN PRIVATE KEY-----
$CertLeafKeyBase64
-----END PRIVATE KEY-----
"@

$CertLeafPemCert = @"
-----BEGIN CERTIFICATE-----
$CertLeafBase64
-----END CERTIFICATE-----
"@

# Output to file

$CertCAPemCert | Out-File -FilePath ca-cert.pem -Encoding Ascii

$CertLeafPemKey | Out-File -FilePath server-key.pem -Encoding Ascii
$CertLeafPemCert | Out-File -FilePath server-cert.pem -Encoding Ascii
```

   Polecenia te tworzą certyfikaty dla bieżącego użytkownika i eksportują certyfikaty do formatu PEM. Do uwierzytelnienia serwera potrzebne są jedynie wyeksportowane pliki PEM. Aby usunąć utworzone certyfikaty z systemu Windows, wykonaj następujące polecenie w programie PowerShell:

```
certmgr.msc
```

   Znajdź utworzone certyfikaty w folderze **Osobiste** → **Certyfikaty** i usuń je.

2. **Utwórz plik flagi serwera**

Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Użyj narzędzia klscflag, aby utworzyć flagę serwera KLSRV_MYSQL_OPT_SSL_CA i jako jej wartość określ ścieżkę do certyfikatu.

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ścieżka do ca-cert.pem> -t s
```

3. **Skonfiguruj bazę danych**

   Określ certyfikaty w pliku my.cnf. Otwórz plik my.cnf w edytorze tekstu i dodaj następujące wiersze do sekcji [mysqld]:

```
[mysqld]
ssl-ca="...\mysqlcerts\ca-cert.pem"
ssl-cert="...\mysqlcerts\server-cert.pem"
ssl-key="...\mysqlcerts\server-key.pem"
```

Włącz dwukierunkowe uwierzytelnianie SSL

Wykonaj poniższe kroki, aby skonfigurować dwukierunkowe uwierzytelnianie SSL dla MySQL:

1. **Utwórz pliki flag serwera**

   Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Użyj narzędzia klscflag, aby utworzyć flagi serwera i jako ich wartości określ ścieżkę do plików certyfikatów:

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ścieżka do ca-cert.pem> -t s
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <ścieżka do server-cert.pem> -t s
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <ścieżka do server-key.pem> -t s
```

2. **Określ hasło (opcjonalnie)**

   Jeśli plik server-key.pem wymaga hasła, utwórz flagę KLSRV_MARIADB_OPT_TLS_PASPHRASE i podaj hasło jako jego wartość:

```
klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <hasło> -t s
```

3. **Skonfiguruj bazę danych**

   Określ certyfikaty w pliku my.cnf. Otwórz plik my.cnf w edytorze tekstu i dodaj następujące wiersze do sekcji [mysqld]:

```
[mysqld]
ssl-ca="...\ca-cert.pem"
ssl-cert="...\server-cert.pem"
ssl-key="...\server-key.pem"
```

Scenariusz: uwierzytelnianie serwera PostgreSQL

Zalecamy użycie certyfikatu TLS do uwierzytelnienia serwera PostgreSQL. Możesz użyć certyfikatu z zaufanego urzędu certyfikacji lub certyfikatu z podpisem własnym. Użyj certyfikatu z zaufanego urzędu certyfikacji, ponieważ certyfikat z podpisem własnym zapewnia tylko ograniczoną ochronę.

Serwer administracyjny obsługuje zarówno jednokierunkowe, jak i dwukierunkowe uwierzytelnianie SSL dla PostgreSQL.

Uwierzytelnianie serwera PostgreSQL odbywa się etapami:

1. **Wygeneruj certyfikat dla serwera PostgreSQL**

   W wieloplatformowym narzędziu opartym na OpenSSL wykonaj następujące polecenia:

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj "/CN=psql"
   ```

   ```
   chmod og-rwx psql.key
   ```

2. **Wygeneruj certyfikat dla Serwera administracyjnego**

   Uruchom następujące polecenia. Wartość CN powinna odpowiadać nazwie użytkownika, który łączy się z PostgreSQL w imieniu Serwera administracyjnego. Domyślnie nazwa użytkownika jest ustawiona na postgres.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
   ```

   ```
   chmod og-rwx postgres.key
   ```

3. **Skonfiguruj uwierzytelnianie certyfikatu klienta**

   Zmodyfikuj plik pg_hba.conf w następujący sposób:

   ```
   hostssl all all 0.0.0.0/0 md5
   ```

   Upewnij się, że plik pg_hba.conf nie zawiera rekordu rozpoczynającego się od `host`.

4. **Określ certyfikat PostgreSQL**

   Jednokierunkowe uwierzytelnianie SSL

   Zmodyfikuj plik postgresql.conf w następujący sposób (podaj poprawną ścieżkę do plików .crt i .key):

   ```
   listen_addresses ='localhost, server-ip'
   ```

   ```
   ssl = on
   ```

   ```
   ssl_cert_file = '<psql.crt>'
   ```

   ```
   ssl_key_file = '<psql.key>'
   ```

   Dwukierunkowe uwierzytelnianie SSL

   Zmodyfikuj plik postgresql.conf w następujący sposób (podaj poprawną ścieżkę do plików .crt i .key):

   ```
   listen_addresses ='localhost, server-ip'
   ```

   ```
   ssl = on
   ```

   ```
   ssl_ca_file = '<postgres.crt>'
   ```

   ```
   ssl_cert_file = '<psql.crt>'
   ```

   ```
   ssl_key_file = '<psql.key>'
   ```

5. **Uruchom ponownie demona PostgreSQL**

   Uruchom następujące polecenie:

   ```
   systemctl restart postgresql-14.service
   ```

6. **Określ flagę serwera dla Serwera administracyjnego**

   Jednokierunkowe uwierzytelnianie SSL

   Użyj narzędzia klscflag, aby utworzyć flagę serwera KLSRV_POSTGRES_OPT_SSL_CA i jako jej wartość określ ścieżkę do certyfikatu.

   Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Uruchom następujące polecenie:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <ścieżka do psql.crt> -t s
   ```

   Dwukierunkowe uwierzytelnianie SSL

   Użyj narzędzia klscflag, aby utworzyć flagi serwera i jako ich wartości określ ścieżkę do plików certyfikatów.

   Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Uruchom następujące polecenia:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <ścieżka do psql.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <ścieżka do postgres.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <ścieżka do postgres.key> -t s
   ```

   Jeśli `postgres.key` wymaga hasła, utwórz flagę KLSRV_POSTGRES_OPT_TLS_PASPHRASE i podaj hasło jako jego wartość:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <hasło> -t s
   ```

7. **Uruchom ponownie usługę Serwera administracyjnego**

Zalecenia dotyczące instalacji Serwera administracyjnego

Ta sekcja zawiera zalecenia dotyczące instalacji Serwera administracyjnego. Opisane są tu także scenariusze korzystania z folderu współdzielonego na urządzeniu z Serwerem administracyjnym w celu zainstalowania Agenta sieciowego na urządzeniach klienckich.

Tworzenie kont dla usług Serwera administracyjnego na klastrze typu failover

Domyślnie instalator automatycznie tworzy konta bez uprawnień dla usług Serwera administracyjnego. To zachowanie jest najwygodniejsze w przypadku instalacji Serwera administracyjnego na zwykłym urządzeniu.

Jednakże instalacja Serwera administracyjnego na klastrze typu failover wymaga innego scenariusza:

1. Dla usług Serwera administracyjnego utwórz konta domenowe bez uprawnień i przydziel je do globalnej grupy zabezpieczeń w domenie o nazwie KLAdmins.

2. W instalatorze Serwera administracyjnego określ konta domenowe, które zostały utworzone dla usług.

Określanie folderu współdzielonego

Podczas instalacji Serwera administracyjnego możesz określić lokalizację folderu współdzielonego. Określenie lokalizacji folderu współdzielonego jest także możliwe po instalacji, we właściwościach Serwera administracyjnego. Domyślnie folder współdzielony zostanie utworzony na urządzeniu z zainstalowanym Serwerem administracyjnym (z uprawnieniami do odczytu dla podgrupy **Wszyscy**). Jednakże w niektórych przypadkach (takich, jak duże obciążenie sieci, konieczność uzyskania dostępu z odizolowanej sieci) przydatne może być umiejscowienie folderu współdzielonego w dedykowanym zasobie plików.

Folder współdzielony jest sporadycznie używany podczas wdrożenia Agenta sieciowego.

Uwzględnianie wielkości liter dla folderu współdzielonego musi być wyłączone.

Zdalna instalacja przy użyciu narzędzi Serwera administracyjnego poprzez zasady grupy Active Directory

Jeśli urządzenia docelowe znajdują się w domenie systemu Windows (bez grup roboczych), wstępna zdalna instalacja (Agenta sieciowego i aplikacji zabezpieczającej na urządzeniach, które nie są jeszcze zarządzane) musi zostać przeprowadzona poprzez zasady grupy Active Directory. Instalacja odbywa się przy użyciu standardowego zadania zdalnej instalacji z programu Kaspersky Security Center. W przypadku sieci dużej skali, dobrym rozwiązaniem jest umieszczenie folderu współdzielonego w dedykowanym zasobie plików w celu zmniejszenia obciążenia podsystemu dyskowego urządzenia z Serwerem administracyjnym.

Zdalna instalacja poprzez dostarczenie ścieżki UNC do pakietu autonomicznego

Jeśli użytkownicy urządzeń w sieci organizacji posiadają uprawnienia administratora lokalnego, stosowana jest inna metoda wstępnej instalacji - poprzez utworzenie autonomicznego pakietu Agenta sieciowego (lub nawet pakietu Agenta sieciowego połączonego z aplikacją zabezpieczającą). Po utworzeniu pakietu autonomicznego, należy wysłać do użytkowników odsyłacz do tego pakietu, który jest przechowywany w folderze współdzielonym. Instalacja rozpocznie się w momencie, gdy użytkownik kliknie odsyłacz.

Aktualizowanie z folderu współdzielonego Serwera administracyjnego

W zadaniu aktualizacji aplikacji antywirusowej możesz skonfigurować aktualizację z folderu współdzielonego Serwera administracyjnego. Jeśli zadanie zostało przypisane do dużej liczby urządzeń, dobrym rozwiązaniem będzie umieszczenie folderu współdzielonego w dedykowanym zasobie plików.

Instalowanie obrazów systemów operacyjnych

Obrazy systemu operacyjnego są zawsze instalowane poprzez folder współdzielony: urządzenia sczytują obrazy systemu operacyjnego z folderu współdzielonego. Jeśli instalacja obrazów została zaplanowana na dużej liczbie urządzeń firmowych, dobrym rozwiązaniem będzie umieszczenie folderu współdzielonego w dedykowanym zasobie plików.

Określanie adresu Serwera administracyjnego

Podczas instalacji Serwera administracyjnego możesz określić adres Serwera administracyjnego. Podczas tworzenia pakietów instalacyjnych Agenta sieciowego ten adres będzie używany jako domyślny.

Jako adres Serwera administracyjnego możesz określić:

- Nazwę NetBIOS Serwera administracyjnego, która jest określona domyślnie
- W pełni kwalifikowana nazwa domeny (FQDN) Serwera administracyjnego, jeśli system nazw domen (DNS) w sieci organizacji został skonfigurowany i działa poprawnie
- Adres zewnętrzny, jeśli Serwer administracyjny jest zainstalowany w strefie zdemilitaryzowanej (DMZ)

Wówczas możliwa będzie zmiana adresu Serwera administracyjnego przy użyciu narzędzi Konsoli administracyjnej; adres nie zostanie zmieniony automatycznie w już utworzonych pakietach instalacyjnych Agenta sieciowego.

Instalacja standardowa

Standardowa instalacja to instalacja Serwera administracyjnego, która używa domyślnych ścieżek dostępu dla plików aplikacji, instaluje domyślny zestaw wtyczek i nie włącza Zarządzania urządzeniami mobilnymi.

W celu zainstalowania Serwera administracyjnego Kaspersky Security Center na urządzeniu lokalnym:

Uruchom plik wykonywalny ksc_<numer wersji>.<numer kompilacji>_full_<wersja językowa>.exe.

Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania. W oknie wyboru aplikacji kliknij odnośnik **Instaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

Krok 1. Przeglądanie treści Umowy licencyjnej i Polityki prywatności

W tym kroku kreatora instalacji należy przeczytać Umowę licencyjną zawieraną między Tobą a firmą Kaspersky, a także Politykę prywatności.

Zaoferowane zostanie także przejrzenie Umów licencyjnych i Polityk prywatności dla wtyczek zarządzających aplikacjami, dostępnych w pakiecie dystrybucyjnym Kaspersky Security Center.

Uważnie przeczytaj Umowę licencyjną i Politykę prywatności. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności, potwierdź to, zaznaczając odpowiednie pola wyboru.

Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól.

Jeśli nie akceptujesz warunków Umowy licencyjnej lub Polityki prywatności, anuluj instalację, klikając przycisk **Anuluj**.

Krok 2. Wybieranie metody instalacji

W oknie wyboru typu instalacji wybierz **Standardowa**.

Instalacja standardowa jest zalecana, jeśli chcesz wypróbować Kaspersky Security Center, na przykład, poprzez przetestowanie działania aplikacji w małym obszarze wewnątrz sieci firmowej. Podczas instalacji standardowej konfigurujesz tylko bazę danych. Nie określasz żadnych ustawień Serwera administracyjnego - używane są wartości domyślne. W instalacji standardowej nie ma możliwości wybrania wtyczek zarządzających do zainstalowania; instalowany jest tylko domyślny zestaw wtyczek. Podczas instalacji standardowej nie są tworzone pakiety instalacyjne dla urządzeń mobilnych. Jednakże możesz utworzyć je później w Konsoli administracyjnej.

Krok 3. Instalowanie Kaspersky Security Center Web Console

Ten krok jest wyświetlany tylko wtedy, gdy korzystasz z 64-bitowego systemu operacyjnego. W innym przypadku ten krok nie jest wyświetlany, ponieważ Kaspersky Security Center Web Console nie działa z 32-bitowymi systemami operacyjnymi.

Domyślnie zostanie zainstalowana zarówno konsola Kaspersky Security Center Web Console, jak i Konsola administracyjna oparta na MMC.

Jeśli chcesz zainstalować tylko Kaspersky Security Center Web Console:

1. Wybierz **Zainstaluj tylko tę**.
2. Z listy rozwijalnej wybierz **Konsola internetowa**.

Instalacja Kaspersky Security Center Web Console rozpocznie się automatycznie po zakończeniu instalacji Serwera administracyjnego.

Jeśli chcesz zainstalować tylko Konsolę administracyjną opartą na MMC:

1. Wybierz **Zainstaluj tylko tę**.
2. Z listy rozwijalnej wybierz **Konsola oparta na MMC**.

Krok 4. Wybieranie rozmiaru sieci

Określ rozmiar sieci, w której instalowany jest Kaspersky Security Center. W zależności od liczby urządzeń w sieci, kreator odpowiednio konfiguruje instalację i wygląd interfejsu aplikacji.

Poniższa tabela wymienia ustawienia instalacyjne aplikacji i ustawienia wyglądu interfejsu, w zależności od różnych rozmiarów sieci.

Zależność ustawień instalacji od wybranej skali sieci

Ustawienia	1–100 zarządzanych urządzeń	101–1000 zarządzanych urządzeń	1001–5000 zarządzanych urządzeń	Więcej niż 5000 zarządzanych urządzeń
Wyświetlanie w drzewie konsoli węzłów podrzędnych i wirtualnych Serwerów administracyjnych oraz wszystkich ustawień związanych z podrzędnymi i wirtualnymi Serwerami administracyjnymi (dostępne tylko w Konsoli administracyjnej opartej na MMC)	Niedostępne	Niedostępne	Dostępne	Dostępne
Wyświetl z sekcjami **Zabezpieczenia** w oknach właściwości Serwera administracyjnego i grup administracyjnych (dostępne tylko w Konsoli administracyjnej opartej na MMC)	Niedostępne	Niedostępne	Dostępne	Dostępne
Losowy czas uruchomienia dla zadania aktualizacji na urządzeniach klienckich	Niedostępne	Ponad 5 minut	Ponad 10 minut	Ponad 10 minut

Jeśli łączysz Serwer administracyjny z serwerem bazodanowym MySQL 5.7 lub SQL Express, nie jest zalecane zarządzanie przy pomocy aplikacji liczbą urządzeń większą niż 10 000. W przypadku systemu zarządzania bazą danych MariaDB maksymalna zalecana liczba zarządzanych urządzeń to 20 000.

Krok 5. Wybieranie bazy danych

W tym kroku kreatora wybierz jeden z następujących systemów zarządzania bazami danych (DBMS), który będzie używany do przechowywania bazy danych Serwera administracyjnego:

- **Microsoft SQL Server lub SQL Server Express**
- **MySQL lub MariaDB**
- **PostgreSQL lub Postgres Pro**

Zaleca się zainstalowanie Serwera administracyjnego na serwerze dedykowanym zamiast na kontrolerze domeny. Jeśli instalujesz Kaspersky Security Center na serwerze, który działa jako kontroler domeny tylko do odczytu (RODC), Microsoft SQL Server (SQL Express) nie może zostać zainstalowany lokalnie (na tym samym urządzeniu). W tym przypadku zalecane jest zdalne zainstalowanie Microsoft SQL Server (SQL Express) (na innym urządzeniu) lub tego, którego używasz — MySQL, MariaDB, lub PostgreSQL — jeśli musisz zainstalować system DBMS lokalnie.

Struktura bazy danych Serwera administracyjnego jest opisana w pliku klakdb.chm, umieszczonym w folderze instalacyjnym Kaspersky Security Center. Ten plik jest również dostępny w archiwum w portalu Kaspersky: klakdb.zip.

Krok 6. Konfigurowanie serwera SQL

W tym kroku kreatora określ następujące ustawienia połączenia, w zależności od wybranego systemu zarządzania bazą danych (DBMS):

- Jeśli w poprzednim kroku wybrałeś **Microsoft SQL Server lub SQL Server Express**:

  - W polu **Nazwa instancji serwera SQL** określ nazwę serwera SQL w sieci. Aby wyświetlić listę wszystkich serwerów SQL, które są w sieci, kliknij przycisk **Przeglądaj**. Domyślnie to pole jest puste.

    Jeśli nawiążesz połączenie z serwerem SQL za pośrednictwem portu niestandardowego, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

    ```
    SQL_Server_host_name,1433
    ```

    Jeśli chronisz komunikację między Serwerem administracyjnym a serwerem SQL przy pomocy certyfikatu, w polu **Nazwa instancji serwera SQL** określ taką samą nazwę hosta, jaka była użyta w momencie generowania certyfikatu. Jeśli użyjesz nazwanej instancji serwera SQL, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

    ```
    SQL_Server_name,1433
    ```

    Jeśli używasz kilku instancji serwera SQL na tym samym hoście, wówczas dodatkowo określ nazwę instancji oddzieloną lewym ukośnikiem, na przykład:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Jeśli serwer SQL w sieci firmowej ma włączoną funkcję Always On, określ nazwę odbiornika grupy dostępności w polu **Nazwa instancji serwera SQL**. Zauważ, że Serwer administracyjny obsługuje tylko tryb dostępności zatwierdzania synchronicznego, gdy włączona jest funkcja Always On.

  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

  Jeśli chcesz ręcznie zainstalować serwer SQL na urządzeniu, na którym instalujesz Kaspersky Security Center, będziesz musiał zatrzymać instalację i uruchomić ją ponownie po zainstalowaniu serwera SQL. Obsługiwane wersje serwerów SQL są wymienione w wymaganiach systemowych.

  W przypadku, gdy ręcznie instalujesz serwer SQL na zdalnym urządzeniu, nie będzie potrzeby przerywania pracy kreatora instalacji Kaspersky Security Center. Zainstaluj serwer SQL i wznów instalację Kaspersky Security Center.

- Jeśli w poprzednim kroku wybrano **MySQL lub MariaDB**:

  - W polu **Nazwa instancji serwera SQL** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.

  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 3306.

  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

- Jeśli w poprzednim kroku wybrano **PostgreSQL lub Postgres Pro**:
  - W polu **Serwer PostgreSQL lub Postgres Pro** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.
  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 5432.
  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

Krok 7. Wybieranie trybu uwierzytelniania

Określ tryb uwierzytelniania, który będzie używany, gdy Serwer administracyjny połączy się z systemem zarządzania bazami danych (DBMS).

W zależności od wybranego DBMS, możesz wybrać jeden z następujących trybów uwierzytelniania:

- Dla SQL Express lub Microsoft SQL Server wybierz jedną z następujących opcji:
  - **Tryb uwierzytelniania Microsoft Windows**. Weryfikacja uprawnień wykorzystuje konto używane do uruchamiania Serwera administracyjnego.
  - **Tryb uwierzytelniania serwera SQL**. Jeśli wybierzesz tę opcję, do weryfikacji uprawnień zostanie użyte konto określone w oknie. Wypełnij pola **Konto** i **Hasło**.

    Aby zobaczyć wprowadzone hasło, kliknij i przytrzymaj przycisk **Pokaż**.

  W przypadku obu trybów uwierzytelniania aplikacja sprawdza, czy baza danych jest dostępna. Jeśli baza danych nie jest dostępna, zostanie wyświetlony komunikat o błędzie, a Ty będziesz musiał dostarczyć poprawne dane uwierzytelniające.

  Jeśli baza danych Serwera administracyjnego jest przechowywana na innym urządzeniu, a konto Serwera administracyjnego nie ma uprawnień dostępu do serwera bazy danych, podczas instalowania lub aktualizowania Serwera administracyjnego musisz użyć trybu uwierzytelniania serwera SQL. Może to mieć miejsce, gdy urządzenie przechowujące bazę danych znajduje się poza domeną lub gdy Serwer administracyjny jest instalowany z poziomu konta SystemLokalny.

- W przypadku MySQL, MariaDB, PostgreSQL lub Postgres Pro określ konto i hasło.

Krok 8. Wypakowywanie i instalowanie plików na dysku twardym

Po skonfigurowaniu instalacji modułów Kaspersky Security Center, możesz rozpocząć instalację plików na dysku twardym.

Jeśli instalacja wymaga dodatkowych programów, kreator instalacji powiadomi Cię o tym w oknie **Instalacja wymaganego oprogramowania** przed rozpoczęciem instalacji Kaspersky Security Center. Wymagane programy są instalowane automatycznie po kliknięciu przycisku **Dalej**.

W ostatnim kroku możesz wybrać, którą konsolę uruchomić do pracy z Kaspersky Security Center:

- **Uruchom Konsolę administracyjną MMC**
- **Uruchom Kaspersky Security Center Web Console**

  Ta opcja jest dostępna tylko wtedy, gdy w jednym z poprzednich kroków wybrano instalację Kaspersky Security Center Web Console.

Możesz także kliknąć **Zakończ**, aby zamknąć kreator bez rozpoczynania pracy z Kaspersky Security Center. Możesz rozpocząć pracę później w dowolnym momencie.

Przy pierwszym uruchomieniu Konsoli administracyjnej lub Kaspersky Security Center Web Console możesz przeprowadzić wstępną konfigurację aplikacji.

Po zakończeniu pracy kreatora instalacji, na dysku twardym są instalowane następujące moduły aplikacji:

- Serwer administracyjny (wraz z serwerową wersją Agenta sieciowego)
- Konsola administracyjna oparta na konsoli Microsoft Management Console
- Kaspersky Security Center Web Console (jeśli zdecydowano się na instalację)
- Wtyczki do zarządzania aplikacjami dostępne w pakiecie dystrybucyjnym

Dodatkowo, zostanie zainstalowany Microsoft Windows Installer 4.5, jeśli nie był wcześniej zainstalowany.

Instalacja niestandardowa

Instalacja niestandardowa to instalacja Serwera administracyjnego, w trakcie której zostaniesz poproszony o wybranie składników, które mają zostać zainstalowane, i określenie folderu, w którym aplikacja ma zostać zainstalowana.

Korzystając z tego typu instalacji, możesz skonfigurować bazę danych i Serwer administracyjny, a także zainstalować składniki, które nie znajdują się w instalacji standardowej, lub wtyczki administracyjne dla różnych aplikacji zabezpieczających firmy Kaspersky. Możesz także włączyć Zarządzanie urządzeniami mobilnymi.

W celu zainstalowania Serwera administracyjnego Kaspersky Security Center na urządzeniu lokalnym:

Uruchom plik wykonywalny ksc_<numer wersji>.<numer kompilacji>_full_<wersja językowa>.exe.

Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania. W oknie wyboru aplikacji kliknij odnośnik **Instaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

Krok 1. Przeglądanie treści Umowy licencyjnej i Polityki prywatności

W tym kroku kreatora instalacji należy przeczytać Umowę licencyjną zawieraną między Tobą a firmą Kaspersky, a także Politykę prywatności.

Zaoferowane zostanie także przejrzenie Umów licencyjnych i Polityk prywatności dla wtyczek zarządzających aplikacjami, dostępnych w pakiecie dystrybucyjnym Kaspersky Security Center.

Uważnie przeczytaj Umowę licencyjną i Politykę prywatności. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności, potwierdź to, zaznaczając odpowiednie pola wyboru.

Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól.

Jeśli nie akceptujesz warunków Umowy licencyjnej lub Polityki prywatności, anuluj instalację, klikając przycisk **Anuluj**.

Krok 2. Wybieranie metody instalacji

W oknie wyboru typu instalacji określ **Niestandardowa**.

W instalacji niestandardowej możliwe jest zmodyfikowanie ustawień Kaspersky Security Center, takich jak: ścieżka dostępu do folderu współdzielonego, konta i porty dla połączenia z Serwerem administracyjnym oraz ustawienia bazy danych. Instalacja niestandardowa umożliwia określenie, które wtyczki zarządzające Kaspersky mają zostać zainstalowane. Podczas instalacji niestandardowej możesz utworzyć pakiety instalacyjne dla urządzeń mobilnych, włączając odpowiednią opcję.

Krok 3. Wybieranie składników do zainstalowania

Wybierz moduły Serwera administracyjnego Kaspersky Security Center, które chcesz zainstalować:

- **Zarządzanie urządzeniami mobilnymi**. Zaznacz to pole, jeśli musisz utworzyć pakiety instalacyjne dla urządzeń mobilnych, gdy uruchomiony jest kreator instalacji Kaspersky Security Center. Możesz także ręcznie utworzyć pakiety instalacyjne dla urządzeń mobilnych, po zainstalowaniu Serwera administracyjnego, korzystając z narzędzi Konsoli administracyjnej.

- **Agent SNMP**. Składnik ten pobiera dane statystyczne dla Serwera administracyjnego za pośrednictwem protokołu SNMP. Moduł jest dostępny tylko wtedy, gdy aplikacja jest instalowana na urządzeniu, na którym zainstalowany jest SNMP.

  > Po zainstalowaniu Kaspersky Security Center, pliki .mib, potrzebne do zbierania danych statystycznych, zostaną umieszczone w podfolderze SNMP folderu instalacyjnego aplikacji.

Agent sieciowy i Konsola administracyjna nie są wyświetlane na liście modułów. Moduły te są instalowane automatycznie, nie możesz anulować ich instalacji.

W tym kroku musisz określić folder instalacyjny komponentów Serwera administracyjnego. Domyślnie moduły są instalowane w folderze <Dysk>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie w trakcie instalacji. Można zmienić folder docelowy przy użyciu przycisku **Przeglądaj**.

Krok 4. Instalowanie Kaspersky Security Center Web Console

Ten krok jest wyświetlany tylko wtedy, gdy korzystasz z 64-bitowego systemu operacyjnego. W innym przypadku ten krok nie jest wyświetlany, ponieważ Kaspersky Security Center Web Console nie działa z 32-bitowymi systemami operacyjnymi.

Domyślnie zostanie zainstalowana zarówno konsola Kaspersky Security Center Web Console, jak i Konsola administracyjna oparta na MMC.

Jeśli chcesz zainstalować tylko Kaspersky Security Center Web Console:

1. Wybierz **Zainstaluj tylko tę**.
2. Z listy rozwijalnej wybierz **Konsola internetowa**.

Instalacja Kaspersky Security Center Web Console rozpocznie się automatycznie po zakończeniu instalacji Serwera administracyjnego.

Jeśli chcesz zainstalować tylko Konsolę administracyjną opartą na MMC:

1. Wybierz **Zainstaluj tylko tę**.
2. Z listy rozwijalnej wybierz **Konsola oparta na MMC**.

Krok 5. Wybieranie rozmiaru sieci

Określ rozmiar sieci, w której instalowany jest Kaspersky Security Center. W zależności od liczby urządzeń w sieci, kreator odpowiednio konfiguruje instalację i wygląd interfejsu aplikacji.

Poniższa tabela wymienia ustawienia instalacyjne aplikacji i ustawienia wyglądu interfejsu, w zależności od różnych rozmiarów sieci.

Zależność ustawień instalacji od wybranej skali sieci

Ustawienia	1–100 zarządzanych urządzeń	101–1000 zarządzanych urządzeń	1001–5000 zarządzanych urządzeń	Więcej niż 5000 zarządzanych urządzeń
Wyświetlanie w drzewie konsoli węzłów podrzędnych i wirtualnych Serwerów administracyjnych oraz wszystkich ustawień związanych z podrzędnymi i wirtualnymi Serwerami administracyjnymi (dostępne tylko w Konsoli administracyjnej opartej na MMC)	Niedostępne	Niedostępne	Dostępne	Dostępne
Wyświetl z sekcjami **Zabezpieczenia** w oknach właściwości Serwera administracyjnego i grup administracyjnych (dostępne tylko w Konsoli administracyjnej opartej na MMC)	Niedostępne	Niedostępne	Dostępne	Dostępne
Losowy czas uruchomienia dla zadania aktualizacji na urządzeniach klienckich	Niedostępne	Ponad 5 minut	Ponad 10 minut	Ponad 10 minut

Jeśli łączysz Serwer administracyjny z serwerem bazodanowym MySQL 5.7 lub SQL Express, nie jest zalecane zarządzanie przy pomocy aplikacji liczbą urządzeń większą niż 10 000. W przypadku systemu zarządzania bazą danych MariaDB maksymalna zalecana liczba zarządzanych urządzeń to 20 000.

Krok 6. Wybieranie bazy danych

W tym kroku kreatora wybierz jeden z następujących systemów zarządzania bazami danych (DBMS), który będzie używany do przechowywania bazy danych Serwera administracyjnego:

- **Microsoft SQL Server lub SQL Server Express**
- **MySQL lub MariaDB**
- **PostgreSQL lub Postgres Pro**

Zaleca się zainstalowanie Serwera administracyjnego na serwerze dedykowanym zamiast na kontrolerze domeny. Jeśli instalujesz Kaspersky Security Center na serwerze, który działa jako kontroler domeny tylko do odczytu (RODC), Microsoft SQL Server (SQL Express) nie może zostać zainstalowany lokalnie (na tym samym urządzeniu). W tym przypadku zalecane jest zdalne zainstalowanie Microsoft SQL Server (SQL Express) (na innym urządzeniu) lub tego, którego używasz — MySQL, MariaDB, lub PostgreSQL — jeśli musisz zainstalować system DBMS lokalnie.

Struktura bazy danych Serwera administracyjnego jest opisana w pliku klakdb.chm, umieszczonym w folderze instalacyjnym Kaspersky Security Center. Ten plik jest również dostępny w archiwum w portalu Kaspersky: klakdb.zip.

Krok 7. Konfigurowanie serwera SQL

W tym kroku kreatora określ następujące ustawienia połączenia, w zależności od wybranego systemu zarządzania bazą danych (DBMS):

- Jeśli w poprzednim kroku wybrałeś **Microsoft SQL Server lub SQL Server Express**:
  - W polu **Nazwa instancji serwera SQL** określ nazwę serwera SQL w sieci. Aby wyświetlić listę wszystkich serwerów SQL, które są w sieci, kliknij przycisk **Przeglądaj**. Domyślnie to pole jest puste.

Jeśli nawiążesz połączenie z serwerem SQL za pośrednictwem portu niestandardowego, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

```
SQL_Server_host_name,1433
```

Jeśli chronisz komunikację między Serwerem administracyjnym a serwerem SQL przy pomocy certyfikatu, w polu **Nazwa instancji serwera SQL** określ taką samą nazwę hosta, jaka była użyta w momencie generowania certyfikatu. Jeśli użyjesz nazwanej instancji serwera SQL, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

```
SQL_Server_name,1433
```

Jeśli używasz kilku instancji serwera SQL na tym samym hoście, wówczas dodatkowo określ nazwę instancji oddzieloną lewym ukośnikiem, na przykład:

```
SQL_Server_name\SQL_Server_instance_name,1433
```

Jeśli serwer SQL w sieci firmowej ma włączoną funkcję Always On, określ nazwę odbiornika grupy dostępności w polu **Nazwa instancji serwera SQL**. Zauważ, że Serwer administracyjny obsługuje tylko tryb dostępności zatwierdzania synchronicznego, gdy włączona jest funkcja Always On.

- W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

Jeśli chcesz ręcznie zainstalować serwer SQL na urządzeniu, na którym instalujesz Kaspersky Security Center, będziesz musiał zatrzymać instalację i uruchomić ją ponownie po zainstalowaniu serwera SQL. Obsługiwane wersje serwerów SQL są wymienione w wymaganiach systemowych.

W przypadku, gdy ręcznie instalujesz serwer SQL na zdalnym urządzeniu, nie będzie potrzeby przerywania pracy kreatora instalacji Kaspersky Security Center. Zainstaluj serwer SQL i wznów instalację Kaspersky Security Center.

- Jeśli w poprzednim kroku wybrano **MySQL lub MariaDB**:
  - W polu **Nazwa instancji serwera SQL** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.
  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 3306.
  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.
- Jeśli w poprzednim kroku wybrano **PostgreSQL lub Postgres Pro**:
  - W polu **Serwer PostgreSQL lub Postgres Pro** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.
  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 5432.
  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

Krok 8. Wybieranie trybu uwierzytelniania

Określ tryb uwierzytelniania, który będzie używany, gdy Serwer administracyjny połączy się z systemem zarządzania bazami danych (DBMS).

W zależności od wybranego DBMS, możesz wybrać jeden z następujących trybów uwierzytelniania:

- Dla SQL Express lub Microsoft SQL Server wybierz jedną z następujących opcji:

  - **Tryb uwierzytelniania Microsoft Windows**. Weryfikacja uprawnień wykorzystuje konto używane do uruchamiania Serwera administracyjnego.

  - **Tryb uwierzytelniania serwera SQL**. Jeśli wybierzesz tę opcję, do weryfikacji uprawnień zostanie użyte konto określone w oknie. Wypełnij pola **Konto** i **Hasło**.

    Aby zobaczyć wprowadzone hasło, kliknij i przytrzymaj przycisk **Pokaż**.

  W przypadku obu trybów uwierzytelniania aplikacja sprawdza, czy baza danych jest dostępna. Jeśli baza danych nie jest dostępna, zostanie wyświetlony komunikat o błędzie, a Ty będziesz musiał dostarczyć poprawne dane uwierzytelniające.

  Jeśli baza danych Serwera administracyjnego jest przechowywana na innym urządzeniu, a konto Serwera administracyjnego nie ma uprawnień dostępu do serwera bazy danych, podczas instalowania lub aktualizowania Serwera administracyjnego musisz użyć trybu uwierzytelniania serwera SQL. Może to mieć miejsce, gdy urządzenie przechowujące bazę danych znajduje się poza domeną lub gdy Serwer administracyjny jest instalowany z poziomu konta SystemLokalny.

- W przypadku MySQL, MariaDB, PostgreSQL lub Postgres Pro określ konto i hasło.

Krok 9. Wybieranie konta do uruchamiania Serwera administracyjnego

Wybierz konto, z poziomu którego Serwer administracyjny będzie uruchamiany jako usługa.

- **Utwórz konto automatycznie**. Aplikacja tworzy konto pod nazwą KL-AK-*, z którego zostanie uruchomiona usługa kladminserver.

  Możesz wybrać tę opcję, jeśli planujesz umieścić folder współdzielony i DBMS na tym samym urządzeniu co Serwer administracyjny.

- **Wybierz konto**. Usługa Serwera administracyjnego (kladminserver) zostanie uruchomiona z poziomu konta, które wybrałeś.

  Będziesz musiał wybrać konto domenowe, jeśli, na przykład, planujesz używać DBMS jako instancji serwera SQL w dowolnej wersji, w tym SQL Express, który znajduje się na innym urządzeniu, i/lub planujesz umieścić folder współdzielony na innym urządzeniu.

  Kaspersky Security Center obsługuje zarządzane konta usług (MSA) i konta usług zarządzane przez grupę (gMSA). Jeśli w Twojej domenie używane są tego typu konta, możesz wybrać jedno z nich jako konto dla usługi Serwera administracyjnego.

  Przed określeniem MSA lub gMSA musisz zainstalować konto na tym samym urządzeniu, na którym chcesz zainstalować serwer administracyjny. Jeśli konto nie zostało jeszcze zainstalowane, anuluj instalację Serwera administracyjnego, zainstaluj konto, a następnie uruchom ponownie instalację Serwera administracyjnego. Szczegółowe informacje na temat instalacji zarządzanych kont usług na urządzeniu lokalnym można znaleźć w oficjalnej dokumentacji firmy Microsoft.

  Aby określić MSA lub gMSA:

  1. Kliknij przycisk **Przeglądaj**.

  2. W otwartym oknie kliknij przycisk **Typ obiektu**.

3. Wybierz typ **Konto dla usług** i kliknij **OK**.

4. Wybierz odpowiednie konto i kliknij **OK**.

Wybrane konto musi posiadać różne uprawnienia, w zależności od systemu DBMS, którego planujesz używać.

W celach bezpieczeństwa nie należy przydzielać stanu uprzywilejowanego do konta, z poziomu którego uruchamiasz Serwer administracyjny.

Konta Serwera administracyjnego nie można później zmienić. Aby móc korzystać z innego konta Serwera administracyjnego, należy ponownie zainstalować klaster trybu failover.

Krok 10. Wybieranie konta do uruchamiania usług Kaspersky Security Center

Wybierz konto, z poziomu którego usługi Kaspersky Security Center będą uruchomione na tym urządzeniu:

- **Utwórz konto automatycznie**. Kaspersky Security Center tworzy lokalne konto o nazwie KlScSvc na tym urządzeniu w grupie kladmins. Usługi Kaspersky Security Center zostaną uruchomione z poziomu utworzonego konta.

- **Wybierz konto**. Usługi Kaspersky Security Center będą uruchamiane z poziomu wybranego konta.

  Będziesz musiał wybrać konto domenowe, jeśli, na przykład, planujesz zapisywać raporty do folderu znajdującego się na innym urządzeniu lub jeśli jest to wymagane przez politykę bezpieczeństwa organizacji. Konieczne może być także wybranie konta domeny, jeśli instalujesz Serwer administracyjny na klastrze typu failover.

W celach bezpieczeństwa nie należy przydzielać stanu uprzywilejowanego do konta, z poziomu którego uruchamiane są usługi.

Usługa KSN proxy (ksnproxy), usługa Kaspersky activation proxy (klactprx) oraz usługa Kaspersky authentication portal (klwebsrv) będą uruchamiane z poziomu wybranego konta.

Krok 11. Wybieranie folderu współdzielonego

Określ lokalizację i nazwę foldera współdzielonego, który będzie wykorzystywany do następujących zadań:

- Przechowywania plików potrzebnych do przeprowadzenia zdalnej instalacji aplikacji (te pliki są kopiowanie na Serwer administracyjny podczas tworzenia pakietów instalacyjnych).

- Przechowywania uaktualnień pobranych ze źródła uaktualnień na Serwer administracyjny.

Udostępnianie plików (tylko do odczytu) będzie możliwe dla wszystkich użytkowników.

Możesz wybrać jedną z następujących opcji:

- **Utwórz folder współdzielony**. Utwórz nowy folder. W polu do wprowadzenia tekstu określ ścieżkę dostępu do folderu.

- **Wskaż istniejący folder współdzielony**. Wybierz folder współdzielony, który już istnieje.

Folder współdzielony może być folderem lokalnym na urządzeniu, które jest używane do instalacji, lub zdalnym folderem na dowolnym urządzeniu klienckim w obrębie sieci firmowej. Folder współdzielony można wybrać przez kliknięcie przycisku **Przeglądaj** lub ręczne wprowadzenie jego ścieżki w formacie UNC (na przykład \\server\Share) w odpowiednim polu.

Domyślnie instalator tworzy lokalny podfolder KLSHARE w folderze aplikacji zawierającym moduły Kaspersky Security Center.

W razie potrzeby folder udostępniony można zdefiniować później.

Krok 12. Konfigurowanie połączenia z Serwerem administracyjnym

Skonfiguruj połączenie z Serwerem administracyjnym:

- **Port**

  Numer portu używanego do nawiązywania połączenia z Serwerem administracyjnym.

  Domyślny numer portu to 14000.

- **Port SSL**

  Numer portu Secure Sockets Layer (SSL) używanego do nawiązywania bezpiecznego połączenia z Serwerem administracyjnym poprzez SSL.

  Domyślny numer portu to 13000.

- **Długość klucza szyfrowania**

  Wybierz długość klucza szyfrowania: 1024 bity lub 2048 bitów.

  Klucz szyfrowania o długości 1024 bitów w mniejszym stopniu obciąża procesor, ale jest uznawany za przestarzały, ponieważ nie zapewnia niezawodnego szyfrowania ze względu na swoją specyfikację techniczną. Dodatkowo, istniejący sprzęt okaże się niekompatybilny z certyfikatami SSL zawierającymi 1024-bitowe klucze.

  Klucz szyfrowania o długości 2048 bitów spełnia wszystkie najnowocześniejsze standardy szyfrowania. Jednakże użycie 2048-bitowego klucza szyfrowania może zwiększyć obciążenie procesora.

  Domyślnie wybrana jest opcja **2048 bitów (największe bezpieczeństwo)**.

Możesz także zmienić parametry połączenia z Serwerem administracyjnym później w następujący sposób:

- Możesz zmienić numery portów i portów SSL później w sekcji **Porty połączenia** we właściwościach Serwera administracyjnego. Aby uzyskać więcej informacji na temat portów połączenia Serwera administracyjnego, zobacz Porty używane przez Kaspersky Security Center.

- Możesz zmienić długość klucza szyfrowania podczas zastępowania certyfikatu Serwera administracyjnego narzędziem klsetsrvcert przy użyciu parametru `-o RsaKeyLen:<długość klucza>`.

Krok 13. Określanie adresu Serwera administracyjnego

Określ adres Serwera administracyjnego przy użyciu jednej z następujących metod:

- **Nazwa domeny DNS**. Metoda ta jest użyteczna, gdy sieć zawiera serwer DNS, którego urządzenia klienckie mogą użyć do uzyskania adresu Serwera administracyjnego.
- **Nazwa NetBIOS**. Metoda ta jest przydatna, gdy urządzenia klienckie uzyskują adres Serwera administracyjnego za pośrednictwem protokołu NetBIOS lub gdy w sieci dostępny jest serwer WINS.
- **Adres IP**. Metoda ta jest używana, gdy Serwer administracyjny posiada stały adres IP, który w przyszłości nie zostanie zmieniony.

Jeśli zainstalowano Kaspersky Security Center na aktywnym węźle klastra pracy awaryjnej Kaspersky Security Center i utworzyłeś dodatkową kartę sieciową podczas przygotowywania węzłów klastra, określ adres IP tej karty. W przeciwnym razie wpisz adres IP modułu równoważenia obciążenia innej firmy, którego używasz.

Krok 14. Adres Serwera administracyjnego dla podłączenia urządzeń mobilnych

Ten krok kreatora instalacji jest dostępny, jeśli moduł Zarządzanie urządzeniami mobilnymi został wybrany do zainstalowania.

W oknie **Adres do podłączenia urządzeń mobilnych** określ zewnętrzny adres Serwera administracyjnego dla podłączenia urządzeń mobilnych, które znajdują się poza siecią lokalną. Możesz określić adres IP lub system nazw domen (DNS) Serwera administracyjnego.

Krok 15. Wybieranie wtyczek do zarządzania aplikacjami

Wybierz wtyczki zarządzające aplikacjami, które mają być zainstalowane wraz z Kaspersky Security Center.

Aby ułatwić wyszukiwanie, wtyczki są podzielone na grupy w zależności od typu chronionych obiektów.

Krok 16. Wypakowywanie i instalowanie plików na dysku twardym

Po skonfigurowaniu instalacji modułów Kaspersky Security Center, możesz rozpocząć instalację plików na dysku twardym.

Jeśli instalacja wymaga dodatkowych programów, kreator instalacji powiadomi Cię o tym w oknie **Instalacja wymaganego oprogramowania** przed rozpoczęciem instalacji Kaspersky Security Center. Wymagane programy są instalowane automatycznie po kliknięciu przycisku **Dalej**.

W ostatnim kroku możesz wybrać, którą konsolę uruchomić do pracy z Kaspersky Security Center:

- **Uruchom Konsolę administracyjną MMC**
- **Uruchom Kaspersky Security Center Web Console**

  Ta opcja jest dostępna tylko wtedy, gdy w jednym z poprzednich kroków wybrano instalację Kaspersky Security Center Web Console.

Możesz także kliknąć **Zakończ**, aby zamknąć kreator bez rozpoczynania pracy z Kaspersky Security Center. Możesz rozpocząć pracę później w dowolnym momencie.

Przy pierwszym uruchomieniu Konsoli administracyjnej lub Kaspersky Security Center Web Console możesz przeprowadzić wstępną konfigurację aplikacji.

Wdrażanie klastra trybu failover Kaspersky Security Center

Ta sekcja zawiera zarówno ogólne informacje o klastrze trybu failover Kaspersky Security Center, jak i instrukcje dotyczące przygotowania i instalacji klastra trybu failover Kaspersky Security Center w Twojej sieci.

Scenariusz: Wdrażanie klastra trybu failover Kaspersky Security Center

Klaster trybu failover Kaspersky Security Center zapewnia wysoką dostępność Kaspersky Security Center i minimalizuje czas przestoju Serwera administracyjnego w przypadku awarii. Klaster trybu failover opiera się na dwóch identycznych instancjach Kaspersky Security Center, zainstalowanych na dwóch komputerach. Jedna z instancji pracuje jako węzeł aktywny, a druga jako węzeł pasywny. Węzeł aktywny zarządza ochroną urządzeń klienckich, natomiast węzeł pasywny jest przygotowany do przejęcia wszystkich funkcji węzła aktywnego w przypadku awarii węzła aktywnego. Gdy wystąpi awaria, węzeł pasywny staje się aktywny, a węzeł aktywny staje się pasywny.

Wymagania wstępne

Masz sprzęt spełniający wymagania dla klastra trybu failover.

Etapy

Wdrożenie aplikacji firmy Kaspersky odbywa się w krokach:

1. **Tworzenie konta dla usług Kaspersky Security Center**

   Utwórz nową grupę domen (w tym scenariuszu dla tej grupy jest używana nazwa 'KLAdmins'), a następnie nadaj grupie uprawnienia administratora lokalnego na obu węzłach i na serwerze plików. Następnie utwórz dwa nowe konta użytkowników domeny (w tym scenariuszu nazwy „ksc" i „rightless" są używane dla tych kont) i dodaj konta do grupy domeny KLAdmins.

   Dodaj konto użytkownika, pod którym zostanie zainstalowany Kaspersky Security Center, do wcześniej utworzonej grupy domeny KLAdmins.

2. **Przygotowanie serwera plików**

   Przygotuj serwer plików do pracy jako komponent klastra trybu failover Kaspersky Security Center. Upewnij się, że serwer plików spełnia wymagania sprzętowe i programowe, utwórz dwa foldery współdzielone dla danych Kaspersky Security Center i skonfiguruj uprawnienia dostępu do folderów współdzielonych.

   Instrukcje: Przygotowanie serwera plików dla klastra trybu failover Kaspersky Security Center

3. **Przygotowanie węzłów aktywnych i pasywnych**

   Przygotuj dwa urządzenia z identycznym sprzętem i oprogramowaniem do pracy jako węzły aktywne i pasywne.

   Instrukcje: Przygotowywanie węzłów dla klastra trybu failover Kaspersky Security Center

4. **Instalacja systemu zarządzania bazą danych (DBMS)**

   Wybierz dowolny z obsługiwanych systemów DBMS, a następnie zainstaluj system DBMS na dedykowanym urządzeniu. Informacje o sposobie zainstalowania systemu DBMS znajdziesz w jego dokumentacji.

5. **Instalacja Kaspersky Security Center**

   Zainstaluj Kaspersky Security Center w klastrze trybu failover na obu węzłach. Najpierw musisz zainstalować Kaspersky Security Center Linux na urządzeniu, które ma pełnić funkcję węzła aktywnego, a następnie zainstalować go na węźle pasywnym.

   Dodatkowo, możesz zainstalować Kaspersky Security Center Web Console na oddzielnym urządzeniu, które nie jest węzłem klastra.

   Instrukcje: Instalowanie Kaspersky Security Center na węzłach klastra trybu failover Kaspersky Security Center

6. **Testowanie klastra trybu failover**

   Sprawdź, czy poprawnie skonfigurowano klaster trybu failover i czy działa poprawnie. Na przykład, możesz zatrzymać jedną z usług Kaspersky Security Center na aktywnym węźle: kladminserver, klnagent, ksnproxy, klactprx lub klwebsrv. Po zatrzymaniu usługi zarządzanie ochroną musi zostać automatycznie przełączone na węzeł pasywny.

Wyniki

Wdrożony zostaje klaster trybu failover Kaspersky Security Center. Prosimy o zapoznanie się ze zdarzeniami, które prowadzą do przełączenia między aktywnym i pasywnym węzłem.

Informacje o klastrze trybu failover Kaspersky Security Center

Klaster trybu failover Kaspersky Security Center zapewnia wysoką dostępność Kaspersky Security Center i minimalizuje czas przestoju Serwera administracyjnego w przypadku awarii. Klaster trybu failover opiera się na dwóch identycznych instancjach Kaspersky Security Center, zainstalowanych na dwóch komputerach. Jedna z instancji pracuje jako węzeł aktywny, a druga jako węzeł pasywny. Węzeł aktywny zarządza ochroną urządzeń klienckich, natomiast węzeł pasywny jest przygotowany do przejęcia wszystkich funkcji węzła aktywnego w przypadku awarii węzła aktywnego. Gdy wystąpi awaria, węzeł pasywny staje się aktywny, a węzeł aktywny staje się pasywny.

Korzystanie z klastra trybu failover nie wpływa na obliczenia oparte na Poradniku dotyczącym rozmiarów.

Do rozwiązywania problemów użyj funkcji Dziennika zdarzeń aplikacji Kaspersky.

Geograficznie rozproszony klaster trybu failover Kaspersky Security Center nie jest obsługiwany. Wdrożenie klastra trybu failover Kaspersky Security Center jest możliwe tylko w obrębie jednej lokalizacji geograficznej.

Warunki przełączenia

Klaster trybu failover przełącza zarządzanie ochroną urządzeń klienckich z węzła aktywnego na węzeł pasywny, jeśli na węźle aktywnym wystąpi dowolne z następujących zdarzeń:

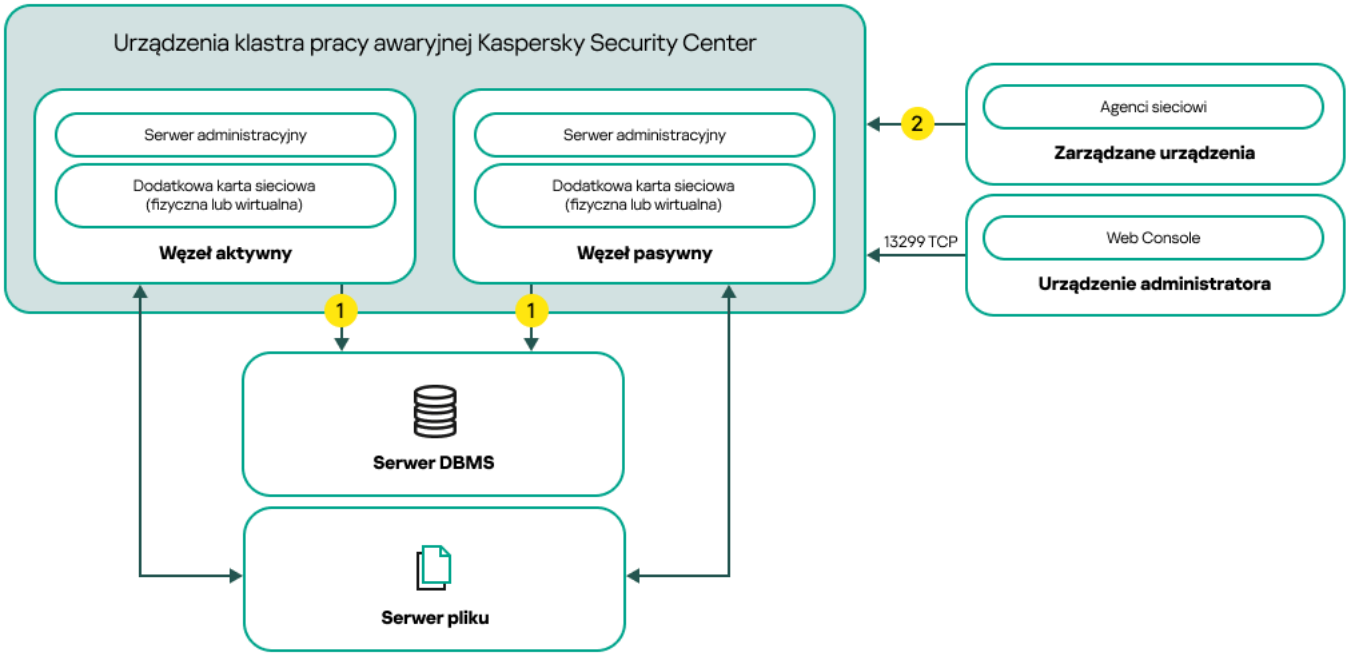
- Węzeł aktywny jest uszkodzony z powodu awarii oprogramowania lub sprzętu.
- Węzeł aktywny został tymczasowo zatrzymany na działania konserwacyjne.
- Przynajmniej jedna z usług (lub procesów) Kaspersky Security Center uległa awarii lub została celowo zamknięta przez użytkownika. Usługi Kaspersky Security Center są następujące: kladminserver, klnagent, klactprx i klwebsrv.
- Połączenie sieciowe między aktywnym węzłem a magazynem na serwerze plików zostało przerwane lub zakończone.

Klaster trybu failover Kaspersky Security Center automatycznie zarządza wszystkimi usługami Kaspersky Security Center. Nie należy ręcznie restartować usług.

Schematy wdrożeń

Możesz wybrać jeden z następujących schematów wdrożenia klastra pracy awaryjnej Kaspersky Security Center:

- Schemat wykorzystujący dodatkową kartę sieciową.
- Schemat korzystający z modułu równoważenia obciążenia innej firmy.

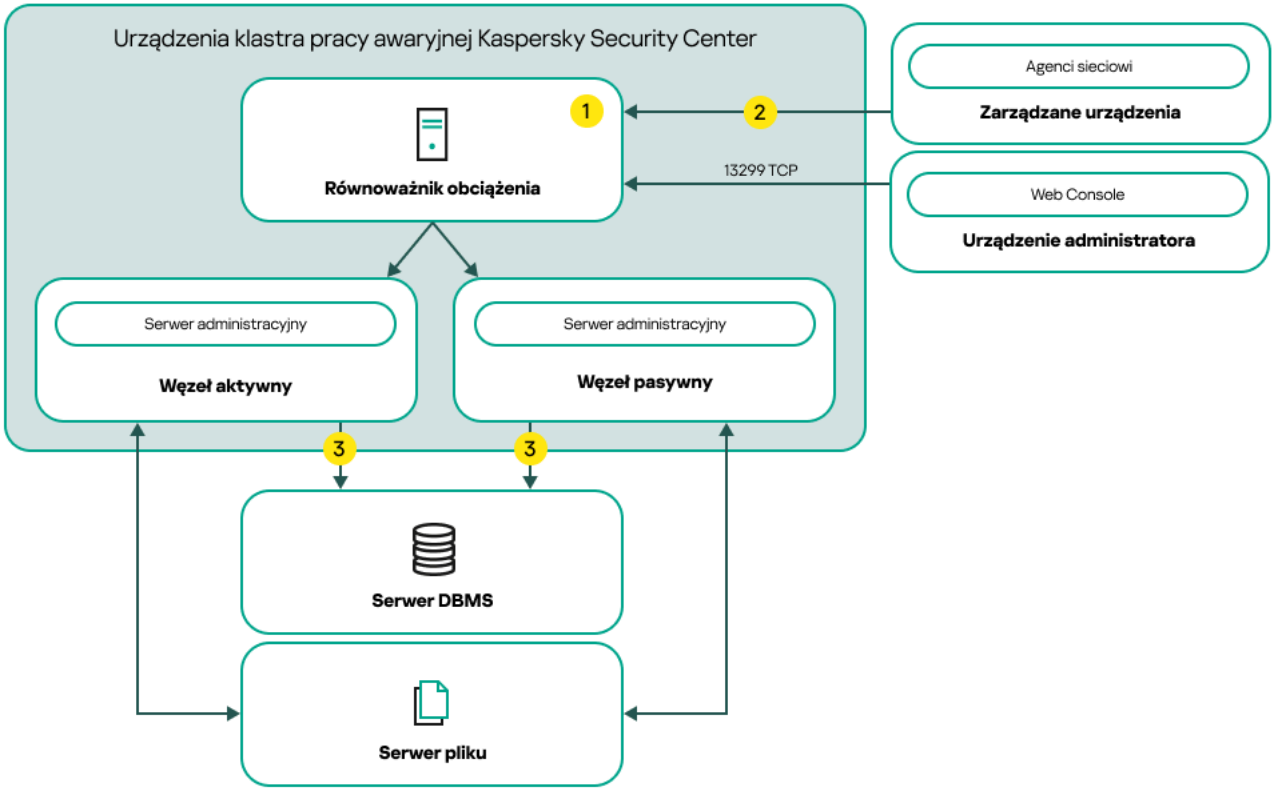


Schemat wykorzystujący dodatkową kartę sieciową

Legenda schematu:

1 Serwer administracyjny wysyła dane do bazy danych. Otwórz niezbędne porty na urządzeniu, na którym znajduje się baza danych, na przykład port 3306 dla MySQL Server lub port 1433 dla Microsoft SQL Server. Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

2 Na zarządzanych urządzeniach otwórz następujące porty: TCP 13000, UDP 13000 i TCP 17000.



Schemat korzystający z modułu równoważenia obciążenia innej firmy

Legenda schematu:

1 Na serwerze równoważenia obciążenia otwórz wszystkie porty Serwera administracyjnego: TCP 13000, UDP 13000, TCP 13299 i TCP 17000.

> Jeśli chcesz wykorzystać narzędzie klakaut do automatyzacji, musisz także otworzyć port TCP 13291.

2 Na zarządzanych urządzeniach otwórz następujące porty: TCP 13000, UDP 13000 i TCP 17000.

3 Serwer administracyjny wysyła dane do bazy danych. Otwórz niezbędne porty na urządzeniu, na którym znajduje się baza danych, na przykład port 3306 dla MySQL Server lub port 1433 dla Microsoft SQL Server. Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

Przygotowywanie serwera plików dla klastra trybu failover Kaspersky Security Center

Serwer plików działa jako wymagany składnik klastra trybu failover Kaspersky Security Center.

W celu przygotowania serwera plików:

1. Upewnij się, że serwer plików spełnia wymagania sprzętowe i programowe.
2. Upewnij się, że serwer plików i oba węzły (aktywny i pasywny) znajdują się w tej samej domenie lub serwer plików jest kontrolerem domeny.

3. Na serwerze plików utwórz dwa foldery współdzielone. Jeden z nich służy do przechowywania informacji o klastrze trybu failover. Drugi służy do przechowywania danych i ustawień Kaspersky Security Center. Ścieżki do folderów współdzielonych określisz podczas konfigurowania instalacji Kaspersky Security Center.

4. Przyznaj pełne uprawnienia dostępu (zarówno uprawnienia udziału, jak i uprawnienia NTFS) do utworzonych folderów współdzielonych dla następujących kont użytkowników i grup:

   - Grupa domen KLAdmins.
   - Konta użytkowników $<node1> i $<node2>. W tym przypadku <node1> oraz <node2> to nazwy urządzeń aktywnych i pasywnych węzłów.

Serwer plików jest przygotowany. Aby zainstalować klaster trybu failover Kaspersky Security Center, postępuj zgodnie z dalszymi instrukcjami w tym scenariuszu.

Przygotowywanie węzłów dla klastra trybu failover Kaspersky Security Center

Przygotuj dwa urządzenia do pracy jako węzły aktywne i pasywne dla klastra pracy awaryjnej Kaspersky Security Center.

W celu przygotowania węzłów dla klastra trybu failover Kaspersky Security Center:

1. Upewnij się, że masz dwa urządzenia, które spełniają wymagania sprzętowe i programowe. Te urządzenia będą działać jako aktywne i pasywne węzły klastra pracy awaryjnej.

2. Upewnij się, że serwer plików i oba węzły znajdują się w tej samej domenie.

3. Wykonaj jedną z poniższych czynności:

   - W każdym z węzłów skonfiguruj dodatkową kartę sieciową.

     Dodatkowa karta sieciowa może być fizyczna lub wirtualna. Jeśli chcesz użyć fizycznej karty sieciowej, podłącz ją i skonfiguruj za pomocą standardowych narzędzi systemu operacyjnego. Jeśli chcesz użyć wirtualnej karty sieciowej, utwórz ją za pomocą oprogramowania innej firmy.

     Upewnij się, że spełnione są następujące warunki:

     - Dodatkowe karty sieciowe są wyłączone.

       Dodatkowe karty sieciowe można utworzyć w stanie wyłączonym lub wyłączyć je po utworzeniu.

     - Dodatkowe karty sieciowe w obu węzłach muszą mieć ten sam adres IP.

   - Użyj modułu równoważenia obciążenia innej firmy. Na przykład, możesz użyć serwera nginx. W takim przypadku wykonaj następujące czynności:

     a. Zapewnij dedykowane urządzenie z systemem Linux z zainstalowanym nginx.

     b. Skonfiguruj moduł równoważenia obciążenia. Ustaw węzeł aktywny jako serwer główny, a węzeł pasywny jako serwer zapasowy.

c. Na serwerze nginx otwórz wszystkie porty Serwera administracyjnego: TCP 13000, UDP 13000, TCP 13299 i TCP 17000.

Jeśli chcesz wykorzystać narzędzie klakaut do automatyzacji, musisz także otworzyć port TCP 13291.

4. Uruchom ponownie oba węzły i serwer plików.

5. Zmapuj dwa foldery współdzielone, które utworzyłeś podczas kroku przygotowania serwera plików, do każdego z węzłów. Musisz zmapować foldery współdzielone jako dyski sieciowe. Podczas mapowania folderów możesz wybrać dowolne wolne litery dysków. Aby uzyskać dostęp do folderów współdzielonych, użyj poświadczeń konta użytkownika utworzonego w kroku 1 procedury scenariusza.

Węzły są przygotowane. Aby zainstalować klaster trybu failover Kaspersky, postępuj zgodnie z dalszymi instrukcjami scenariusza.

Instalowanie Kaspersky Security Center na węzłach klastra trybu failover Kaspersky Security Center

Kaspersky Security Center jest instalowany na obu węzłach klastra trybu failover Kaspersky Security Center oddzielnie. W pierwszej kolejności instalujesz aplikację na węźle aktywnym, a następnie na węźle pasywnym. Podczas instalacji wybierasz, który węzeł będzie aktywny, a który będzie pasywny.

Tylko użytkownik z grupy domen KLAdmins może zainstalować Kaspersky Security Center na każdym węźle.

W celu zainstalowania Kaspersky Security Center na aktywnym węźle klastra trybu failover Kaspersky Security Center:

1. Uruchom plik wykonywalny ksc_15.1_<numer kompilacji>_full_<wersja językowa>.exe.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania. W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

2. Uważnie przeczytaj Umowę licencyjną i Politykę prywatności. Jeśli zgadzasz się na wszystkie warunki Umowy licencyjnej i Polityki prywatności, w sekcji **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki oraz postanowienia następujących:** zaznacz następujące pola:

   - **Warunki i postanowienia tej Umowy licencyjnej użytkownika końcowego**
   - **Politykę prywatności opisującą zasady przetwarzania danych**

   Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól.

   Jeśli nie akceptujesz warunków Umowy licencyjnej lub Polityki prywatności, anuluj instalację, klikając przycisk **Anuluj**.

3. Wybierz **Węzeł podstawowy klastra trybu failover Kaspersky Security Center**, aby zainstalować aplikację na aktywnym węźle.

4. W oknie **Folder współdzielony** wykonaj następujące czynności:

   - W polach **Udział stanu** i **Udział danych** określ ścieżki do folderów współdzielonych, które utworzyłeś na serwerze plików podczas jego przygotowania.
   - W polach **Dysk udziału stanu** i **Dysk udziału danych** wybierz dyski sieciowe, na które zmapowałeś foldery współdzielone podczas przygotowania węzłów.
   - Wybierz tryb łączności klastra: za pośrednictwem dodatkowej karty sieciowej lub modułu równoważenia obciążenia innej firmy.

5. Wykonaj inne kroki instalacji niestandardowej, zaczynając od kroku 3.

   W kroku 13 określ adres IP dodatkowej karty sieciowej, jeśli utworzyłeś kartę podczas przygotowania węzłów klastra. W przeciwnym razie wpisz adres IP modułu równoważenia obciążenia innej firmy, którego używasz.

Kaspersky Security Center jest zainstalowany na aktywnym węźle.

W celu zainstalowania Kaspersky Security Center na pasywnym węźle klastra trybu failover Kaspersky Security Center:

1. Uruchom plik wykonywalny ksc_15.1_<numer kompilacji>_full_<wersja językowa>.exe.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania. W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

2. Uważnie przeczytaj Umowę licencyjną i Politykę prywatności. Jeśli zgadzasz się na wszystkie warunki Umowy licencyjnej i Polityki prywatności, w sekcji **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki oraz postanowienia następujących:** zaznacz następujące pola:

   - **Warunki i postanowienia tej Umowy licencyjnej użytkownika końcowego**
   - **Politykę prywatności opisującą zasady przetwarzania danych**

   Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól.

   Jeśli nie akceptujesz warunków Umowy licencyjnej lub Polityki prywatności, anuluj instalację, klikając przycisk **Anuluj**.

3. Wybierz **Węzeł pomocniczy klastra trybu failover Kaspersky Security Center**, aby zainstalować aplikację na pasywnym węźle.

4. W oknie **Folder współdzielony**, w polu **Udział stanu** podaj ścieżkę do folderu współdzielonego z informacjami o stanie klastra, który utworzyłeś na serwerze plików podczas jego przygotowania.

5. Kliknij przycisk **Zainstaluj**. Po zakończeniu instalacji kliknij przycisk **Zakończ**.

Kaspersky Security Center jest zainstalowany na pasywnym węźle. Teraz możesz przetestować klaster trybu failover Kaspersky Security Center, aby upewnić się, że został poprawnie skonfigurowany i działa poprawnie.

Ręczne uruchamianie i zatrzymywanie węzłów klastra

Konieczne może być zatrzymanie całego klastra trybu failover Kaspersky Security Center lub tymczasowe odłączenie jednego z węzłów klastra w celu konserwacji. W takim przypadku postępuj zgodnie z instrukcjami w tej sekcji. Nie próbuj uruchamiać ani zatrzymywać usług lub procesów związanych z klastrem trybu failover za pomocą innych środków. To może spowodować utratę danych.

Uruchamianie i zatrzymywanie całego klastra trybu failover w celu konserwacji

W celu uruchomienia lub zatrzymania całego klastra trybu failover:

1. Na aktywnym węźle przejdź do <Dysk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Otwórz wiersz polecenia, a następnie uruchom jedno z następujących poleceń:
   - Aby zatrzymać klaster, uruchom: `klfoc -stopcluster --stp klfoc`
   - Aby uruchomić klaster, uruchom: `klfoc -startcluster --stp klfoc`

   Klaster trybu failover jest uruchamiany lub zatrzymywany w zależności od uruchomionego polecenia.

Utrzymywanie jednego z węzłów

W celu utrzymania jednego z węzłów:

1. W węźle aktywnym zatrzymaj klaster trybu failover, używając polecenia `klfoc -stopcluster --stp klfoc`.
2. W węźle, który chcesz poddać działaniom konserwacyjnym, przejdź do <Dysk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
3. Otwórz wiersz poleceń, a następnie odłącz węzeł od klastra, uruchamiając polecenie `detach_node.cmd`.
4. W węźle aktywnym uruchom klaster trybu failover za pomocą polecenia `klfoc -startcluster --stp klfoc`.
5. Wykonaj działania konserwacyjne.
6. W węźle aktywnym zatrzymaj klaster trybu failover, używając polecenia `klfoc -stopcluster --stp klfoc`.
7. W węźle, na którym wykonywano działania konserwacyjne, przejdź do <Dysk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

8. Otwórz wiersz poleceń, a następnie dołącz węzeł do klastra, uruchamiając polecenie `attach_node.cmd`.

9. W węźle aktywnym uruchom klaster trybu failover za pomocą polecenia `klfoc -startcluster --stp klfoc`.

Węzeł jest utrzymywany i dołączany do klastra trybu failover.

Instalowanie Serwera administracyjnego na klastrze trybu failover Windows Server

Procedura instalacji Serwera administracyjnego w klastrze typu failover różni się zarówno od standardowej, jak i niestandardowej instalacji na urządzeniu autonomicznym.

> Klaster trybu failover Windows z rozproszonym geograficznie klastrem nie jest obsługiwany. Wdrożenie klastra trybu failover Windows Server jest możliwe tylko w obrębie jednej lokalizacji geograficznej, która zapewnia wysoką dostępność sieci i szybki czas reakcji między węzłami klastra.

Wykonaj procedurę opisaną w tej sekcji na węźle, który zawiera wspólny magazyn danych klastra.

W celu zainstalowania Serwera administracyjnego Kaspersky Security Center na klastrze:

Uruchom plik wykonywalny ksc_<numer wersji>.<numer kompilacji>_full_<wersja językowa>.exe.

Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania. W oknie wyboru aplikacji kliknij odnośnik **Instaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

Krok 1. Przeglądanie treści Umowy licencyjnej i Polityki prywatności

W tym kroku kreatora instalacji należy przeczytać Umowę licencyjną zawieraną między Tobą a firmą Kaspersky, a także Politykę prywatności.

Zaoferowane zostanie także przejrzenie Umów licencyjnych i Polityk prywatności dla wtyczek zarządzających aplikacjami, dostępnych w pakiecie dystrybucyjnym Kaspersky Security Center.

Uważnie przeczytaj Umowę licencyjną i Politykę prywatności. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności, potwierdź to, zaznaczając odpowiednie pola wyboru.

Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól.

Jeśli nie akceptujesz warunków Umowy licencyjnej lub Polityki prywatności, anuluj instalację, klikając przycisk **Anuluj**.

Krok 2. Wybieranie typu instalacji na klastrze

Wybierz typ instalacji na klastrze:

- **Klaster (zainstaluj na wszystkich węzłach klastra)**

To jest zalecana opcja. Jeśli wybierzesz tę opcję, Serwer administracyjny zostanie zainstalowany na wszystkich węzłach klastra jednocześnie.

Na etapie wyboru Konsoli administracyjnej do instalacji należy wybrać konsolę, która zostanie zainstalowana na bieżącym węźle klastra. Jeśli zainstalujesz konsolę tylko na węźle klastra, w przypadku awarii węzła utracisz dostęp do Serwera administracyjnego. Zalecamy, aby podczas tego kroku wybrać Konsolę administracyjną opartą na MMC do instalacji na wszystkich węzłach klastra. Po zainstalowaniu Serwera administracyjnego zainstaluj Kaspersky Security Center Web Console na oddzielnym urządzeniu, które nie jest węzłem klastra. Pozwala to na zarządzanie Serwerem administracyjnym przy użyciu Kaspersky Security Center Web Console, jeśli węzeł klastra ulegnie awarii.

- **Lokalnie (zainstaluj tylko na tym urządzeniu)**

  Jeśli wybierzesz tę opcję, Serwer administracyjny zostanie zainstalowany tylko na bieżącym węźle, tak jak na serwerze autonomicznym, a Serwer administracyjny nie będzie działał jako aplikacja typu cluster-aware. Na przykład, możesz chcieć wybrać tę opcję, aby zaoszczędzić współdzieloną przestrzeń dyskową, jeśli odporność na uszkodzenia nie jest potrzebna dla Serwera administracyjnego. W przypadku awarii bieżącego węzła, będziesz musiał zainstalować Serwer administracyjny na innym węźle i przywrócić stan Serwera administracyjnego z kopii zapasowej.

Dalsze kroki są takie same, jak w przypadku standardowej lub niestandardowej metody instalacji, począwszy od kroku wyboru metody instalacji.

Krok 3. Określanie nazwy wirtualnego Serwera administracyjnego

Określ nazwę sieciową nowego wirtualnego Serwera administracyjnego. Będziesz mógł użyć tej nazwy do połączenia Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console z Serwerem administracyjnym.

Określona nazwa musi różnić się od nazwy klastra.

Krok 4. Określanie szczegółów sieci wirtualnego Serwera administracyjnego

W celu określenia szczegółów sieci nowej instancji wirtualnego Serwera administracyjnego:

1. W sekcji **Sieć do użycia** wybierz sieć domeny, do której jest podłączony bieżący węzeł klastra.
2. Wykonaj jedną z poniższych czynności:
   - Jeśli w wybranej sieci, do przypisywania adresów IP używany jest protokół DHCP, wybierz opcję **Użyj DHCP**.
   - Jeśli w wybranej sieci nie jest używany protokół DHCP, określ wymagany adres IP.

     Podany adres IP musi różnić się od adresu IP klastra.
3. Kliknij **Dodaj**, aby zastosować określone ustawienia.

Będziesz mógł użyć automatycznie przypisanego lub określonego adresu IP do połączenia Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console z Serwerem administracyjnym.

Krok 5. Określanie grupy klastrów

Grupa klastrów to specjalny klaster typu failover, który zawiera wspólne zasoby dla wszystkich węzłów. Masz dwie opcje:

- Tworzenie nowej grupy klastrów.

  Ta opcja jest zalecana w większości przypadków. Nowa grupa klastrów będzie zawierać wszystkie wspólne zasoby związane z instancją Serwera administracyjnego.

- Wybieranie istniejącej grupy klastrów.

  Wybierz tę opcję, jeśli chcesz użyć wspólnego zasobu, który jest już skojarzony z istniejącą grupą klastrów. Na przykład, możesz chcieć użyć tej opcji, jeśli chcesz użyć magazynu skojarzonego z istniejącą grupą klastrów i jeśli nie ma innego dostępnego magazynu dla nowej grupy klastrów.

Krok 6. Wybieranie magazynu danych klastra

W celu wybrania magazynu danych klastra:

1. W sekcji **Dostępne repozytoria** wybierz magazyn danych, w którym zostaną zainstalowane wspólne zasoby instancji wirtualnego Serwera administracyjnego.

2. Jeśli wybrany magazyn danych zawiera kilka woluminów, w sekcji **Dostępne sekcje na dysku twardym** wybierz wymagany wolumin.

3. W sekcji **Ścieżka instalacji** wprowadź ścieżkę do wspólnego magazynu danych, w którym zostaną zainstalowane zasoby instancji wirtualnego Serwera administracyjnego.

Magazyn danych został wybrany.

Krok 7. Określanie konta do zdalnej instalacji

Podaj nazwę użytkownika i hasło, które będą używane do zdalnej instalacji instancji wirtualnego Serwera administracyjnego w pasywnym węźle klastra.

Określone konto musi mieć nadane uprawnienia administracyjne na wszystkich węzłach klastra.

Krok 8. Wybieranie składników do zainstalowania

Wybierz moduły Serwera administracyjnego Kaspersky Security Center, które chcesz zainstalować:

- **Zarządzanie urządzeniami mobilnymi**. Zaznacz to pole, jeśli musisz utworzyć pakiety instalacyjne dla urządzeń mobilnych, gdy uruchomiony jest kreator instalacji Kaspersky Security Center. Możesz także ręcznie utworzyć pakiety instalacyjne dla urządzeń mobilnych, po zainstalowaniu Serwera administracyjnego, korzystając z narzędzi Konsoli administracyjnej.

- **Agent SNMP**. Składnik ten pobiera dane statystyczne dla Serwera administracyjnego za pośrednictwem protokołu SNMP. Moduł jest dostępny tylko wtedy, gdy aplikacja jest instalowana na urządzeniu, na którym zainstalowany jest SNMP.

  Po zainstalowaniu Kaspersky Security Center, pliki .mib, potrzebne do zbierania danych statystycznych, zostaną umieszczone w podfolderze SNMP folderu instalacyjnego aplikacji.

Agent sieciowy i Konsola administracyjna nie są wyświetlane na liście modułów. Moduły te są instalowane automatycznie, nie możesz anulować ich instalacji.

W tym kroku musisz określić folder instalacyjny komponentów Serwera administracyjnego. Domyślnie moduły są instalowane w folderze <Dysk>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie w trakcie instalacji. Można zmienić folder docelowy przy użyciu przycisku **Przeglądaj**.

Krok 9. Wybieranie rozmiaru sieci

Określ rozmiar sieci, w której instalowany jest Kaspersky Security Center. W zależności od liczby urządzeń w sieci, kreator odpowiednio konfiguruje instalację i wygląd interfejsu aplikacji.

Poniższa tabela wymienia ustawienia instalacyjne aplikacji i ustawienia wyglądu interfejsu, w zależności od różnych rozmiarów sieci.

Zależność ustawień instalacji od wybranej skali sieci

Ustawienia	1–100 zarządzanych urządzeń	101–1000 zarządzanych urządzeń	1001–5000 zarządzanych urządzeń	Więcej niż 5000 zarządzanych urządzeń
Wyświetlanie w drzewie konsoli węzłów podrzędnych i wirtualnych Serwerów administracyjnych oraz wszystkich ustawień związanych z podrzędnymi i wirtualnymi Serwerami administracyjnymi (dostępne tylko w Konsoli administracyjnej opartej na MMC)	Niedostępne	Niedostępne	Dostępne	Dostępne
Wyświetl z sekcjami **Zabezpieczenia** w oknach właściwości Serwera administracyjnego i grup administracyjnych (dostępne tylko w Konsoli administracyjnej opartej na MMC)	Niedostępne	Niedostępne	Dostępne	Dostępne
Losowy czas uruchomienia dla zadania aktualizacji na urządzeniach klienckich	Niedostępne	Ponad 5 minut	Ponad 10 minut	Ponad 10 minut

Jeśli łączysz Serwer administracyjny z serwerem bazodanowym MySQL 5.7 lub SQL Express, nie jest zalecane zarządzanie przy pomocy aplikacji liczbą urządzeń większą niż 10 000. W przypadku systemu zarządzania bazą danych MariaDB maksymalna zalecana liczba zarządzanych urządzeń to 20 000.

Krok 10. Wybieranie bazy danych

W tym kroku kreatora wybierz jeden z następujących systemów zarządzania bazami danych (DBMS), który będzie używany do przechowywania bazy danych Serwera administracyjnego:

- **Microsoft SQL Server lub SQL Server Express**
- **MySQL lub MariaDB**
- **PostgreSQL lub Postgres Pro**

Zaleca się zainstalowanie Serwera administracyjnego na serwerze dedykowanym zamiast na kontrolerze domeny. Jeśli instalujesz Kaspersky Security Center na serwerze, który działa jako kontroler domeny tylko do odczytu (RODC), Microsoft SQL Server (SQL Express) nie może zostać zainstalowany lokalnie (na tym samym urządzeniu). W tym przypadku zalecane jest zdalne zainstalowanie Microsoft SQL Server (SQL Express) (na innym urządzeniu) lub tego, którego używasz — MySQL, MariaDB, lub PostgreSQL — jeśli musisz zainstalować system DBMS lokalnie.

Struktura bazy danych Serwera administracyjnego jest opisana w pliku klakdb.chm, umieszczonym w folderze instalacyjnym Kaspersky Security Center. Ten plik jest również dostępny w archiwum w portalu Kaspersky: klakdb.zip.

Krok 11. Konfigurowanie serwera SQL

W tym kroku kreatora określ następujące ustawienia połączenia, w zależności od wybranego systemu zarządzania bazą danych (DBMS):

- Jeśli w poprzednim kroku wybrałeś **Microsoft SQL Server lub SQL Server Express**:
  - W polu **Nazwa instancji serwera SQL** określ nazwę serwera SQL w sieci. Aby wyświetlić listę wszystkich serwerów SQL, które są w sieci, kliknij przycisk **Przeglądaj**. Domyślnie to pole jest puste.

    Jeśli nawiążesz połączenie z serwerem SQL za pośrednictwem portu niestandardowego, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

    ```
    SQL_Server_host_name,1433
    ```

    Jeśli chronisz komunikację między Serwerem administracyjnym a serwerem SQL przy pomocy certyfikatu, w polu **Nazwa instancji serwera SQL** określ taką samą nazwę hosta, jaka była użyta w momencie generowania certyfikatu. Jeśli użyjesz nazwanej instancji serwera SQL, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

    ```
    SQL_Server_name,1433
    ```

    Jeśli używasz kilku instancji serwera SQL na tym samym hoście, wówczas dodatkowo określ nazwę instancji oddzieloną lewym ukośnikiem, na przykład:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Jeśli serwer SQL w sieci firmowej ma włączoną funkcję Always On, określ nazwę odbiornika grupy dostępności w polu **Nazwa instancji serwera SQL**. Zauważ, że Serwer administracyjny obsługuje tylko tryb dostępności zatwierdzania synchronicznego, gdy włączona jest funkcja Always On.

  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

Jeśli chcesz ręcznie zainstalować serwer SQL na urządzeniu, na którym instalujesz Kaspersky Security Center, będziesz musiał zatrzymać instalację i uruchomić ją ponownie po zainstalowaniu serwera SQL. Obsługiwane wersje serwerów SQL są wymienione w wymaganiach systemowych.

W przypadku, gdy ręcznie instalujesz serwer SQL na zdalnym urządzeniu, nie będzie potrzeby przerywania pracy kreatora instalacji Kaspersky Security Center. Zainstaluj serwer SQL i wznów instalację Kaspersky Security Center.

- Jeśli w poprzednim kroku wybrano **MySQL lub MariaDB**:
  - W polu **Nazwa instancji serwera SQL** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.
  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 3306.
  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.
- Jeśli w poprzednim kroku wybrano **PostgreSQL lub Postgres Pro**:
  - W polu **Serwer PostgreSQL lub Postgres Pro** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.
  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 5432.

W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

Krok 12. Wybieranie trybu uwierzytelniania

Określ tryb uwierzytelniania, który będzie używany, gdy Serwer administracyjny połączy się z systemem zarządzania bazami danych (DBMS).

W zależności od wybranego DBMS, możesz wybrać jeden z następujących trybów uwierzytelniania:

- Dla SQL Express lub Microsoft SQL Server wybierz jedną z następujących opcji:
  - **Tryb uwierzytelniania Microsoft Windows**. Weryfikacja uprawnień wykorzystuje konto używane do uruchamiania Serwera administracyjnego.
  - **Tryb uwierzytelniania serwera SQL**. Jeśli wybierzesz tę opcję, do weryfikacji uprawnień zostanie użyte konto określone w oknie. Wypełnij pola **Konto** i **Hasło**.

    Aby zobaczyć wprowadzone hasło, kliknij i przytrzymaj przycisk **Pokaż**.

  W przypadku obu trybów uwierzytelniania aplikacja sprawdza, czy baza danych jest dostępna. Jeśli baza danych nie jest dostępna, zostanie wyświetlony komunikat o błędzie, a Ty będziesz musiał dostarczyć poprawne dane uwierzytelniające.

  Jeśli baza danych Serwera administracyjnego jest przechowywana na innym urządzeniu, a konto Serwera administracyjnego nie ma uprawnień dostępu do serwera bazy danych, podczas instalowania lub aktualizowania Serwera administracyjnego musisz użyć trybu uwierzytelniania serwera SQL. Może to mieć miejsce, gdy urządzenie przechowujące bazę danych znajduje się poza domeną lub gdy Serwer administracyjny jest instalowany z poziomu konta SystemLokalny.

W przypadku MySQL, MariaDB, PostgreSQL lub Postgres Pro określ konto i hasło.

Krok 13. Wybieranie konta do uruchamiania Serwera administracyjnego

Wybierz konto, z poziomu którego Serwer administracyjny będzie uruchamiany jako usługa.

- **Utwórz konto automatycznie**. Aplikacja tworzy konto pod nazwą KL-AK-*, z którego zostanie uruchomiona usługa kladminserver.

  Możesz wybrać tę opcję, jeśli planujesz umieścić folder współdzielony i DBMS na tym samym urządzeniu co Serwer administracyjny.

- **Wybierz konto**. Usługa Serwera administracyjnego (kladminserver) zostanie uruchomiona z poziomu konta, które wybrałeś.

  Będziesz musiał wybrać konto domenowe, jeśli, na przykład, planujesz używać DBMS jako instancji serwera SQL w dowolnej wersji, w tym SQL Express, który znajduje się na innym urządzeniu, i/lub planujesz umieścić folder współdzielony na innym urządzeniu.

  Kaspersky Security Center obsługuje zarządzane konta usług (MSA) i konta usług zarządzane przez grupę (gMSA). Jeśli w Twojej domenie używane są tego typu konta, możesz wybrać jedno z nich jako konto dla usługi Serwera administracyjnego.

  Przed określeniem MSA lub gMSA musisz zainstalować konto na tym samym urządzeniu, na którym chcesz zainstalować serwer administracyjny. Jeśli konto nie zostało jeszcze zainstalowane, anuluj instalację Serwera administracyjnego, zainstaluj konto, a następnie uruchom ponownie instalację Serwera administracyjnego. Szczegółowe informacje na temat instalacji zarządzanych kont usług na urządzeniu lokalnym można znaleźć w oficjalnej dokumentacji firmy Microsoft.

  Aby określić MSA lub gMSA:

  1. Kliknij przycisk **Przeglądaj**.
  2. W otwartym oknie kliknij przycisk **Typ obiektu**.
  3. Wybierz typ **Konto dla usług** i kliknij **OK**.
  4. Wybierz odpowiednie konto i kliknij **OK**.

Wybrane konto musi posiadać różne uprawnienia, w zależności od systemu DBMS, którego planujesz używać.

W celach bezpieczeństwa nie należy przydzielać stanu uprzywilejowanego do konta, z poziomu którego uruchamiasz Serwer administracyjny.

Konta Serwera administracyjnego nie można później zmienić. Aby móc korzystać z innego konta Serwera administracyjnego, należy ponownie zainstalować klaster trybu failover.

Krok 14. Wybieranie konta do uruchamiania usług Kaspersky Security Center

Wybierz konto, z poziomu którego usługi Kaspersky Security Center będą uruchomione na tym urządzeniu:

- **Utwórz konto automatycznie**. Kaspersky Security Center tworzy lokalne konto o nazwie KlScSvc na tym urządzeniu w grupie kladmins. Usługi Kaspersky Security Center zostaną uruchomione z poziomu utworzonego konta.

- **Wybierz konto**. Usługi Kaspersky Security Center będą uruchamiane z poziomu wybranego konta.

  Będziesz musiał wybrać konto domenowe, jeśli, na przykład, planujesz zapisywać raporty do folderu znajdującego się na innym urządzeniu lub jeśli jest to wymagane przez politykę bezpieczeństwa organizacji. Konieczne może być także wybranie konta domeny, jeśli instalujesz Serwer administracyjny na klastrze typu failover.

W celach bezpieczeństwa nie należy przydzielać stanu uprzywilejowanego do konta, z poziomu którego uruchamiane są usługi.

Usługa KSN proxy (ksnproxy), usługa Kaspersky activation proxy (klactprx) oraz usługa Kaspersky authentication portal (klwebsrv) będą uruchamiane z poziomu wybranego konta.

Krok 15. Wybieranie folderu współdzielonego

Określ lokalizację i nazwę foldera współdzielonego, który będzie wykorzystywany do następujących zadań:

- Przechowywania plików potrzebnych do przeprowadzenia zdalnej instalacji aplikacji (te pliki są kopiowanie na Serwer administracyjny podczas tworzenia pakietów instalacyjnych).

- Przechowywania uaktualnień pobranych ze źródła uaktualnień na Serwer administracyjny.

Udostępnianie plików (tylko do odczytu) będzie możliwe dla wszystkich użytkowników.

Możesz wybrać jedną z następujących opcji:

- **Utwórz folder współdzielony**. Utwórz nowy folder. W polu do wprowadzenia tekstu określ ścieżkę dostępu do folderu.

- **Wskaż istniejący folder współdzielony**. Wybierz folder współdzielony, który już istnieje.

Folder współdzielony może być folderem lokalnym na urządzeniu, które jest używane do instalacji, lub zdalnym folderem na dowolnym urządzeniu klienckim w obrębie sieci firmowej. Folder współdzielony można wybrać przez kliknięcie przycisku **Przeglądaj** lub ręczne wprowadzenie jego ścieżki w formacie UNC (na przykład \\server\Share) w odpowiednim polu.

Domyślnie instalator tworzy lokalny podfolder KLSHARE w folderze aplikacji zawierającym moduły Kaspersky Security Center.

W razie potrzeby folder udostępniony można zdefiniować później.

Krok 16. Konfigurowanie połączenia z Serwerem administracyjnym

Skonfiguruj połączenie z Serwerem administracyjnym:

- **Port**

  Numer portu używanego do nawiązywania połączenia z Serwerem administracyjnym.

  Domyślny numer portu to 14000.

- **Port SSL**

  Numer portu Secure Sockets Layer (SSL) używanego do nawiązywania bezpiecznego połączenia z Serwerem administracyjnym poprzez SSL.

  Domyślny numer portu to 13000.

- **Długość klucza szyfrowania**

  Wybierz długość klucza szyfrowania: 1024 bity lub 2048 bitów.

  Klucz szyfrowania o długości 1024 bitów w mniejszym stopniu obciąża procesor, ale jest uznawany za przestarzały, ponieważ nie zapewnia niezawodnego szyfrowania ze względu na swoją specyfikację techniczną. Dodatkowo, istniejący sprzęt okaże się niekompatybilny z certyfikatami SSL zawierającymi 1024-bitowe klucze.

  Klucz szyfrowania o długości 2048 bitów spełnia wszystkie najnowocześniejsze standardy szyfrowania. Jednakże użycie 2048-bitowego klucza szyfrowania może zwiększyć obciążenie procesora.

  Domyślnie wybrana jest opcja **2048 bitów (największe bezpieczeństwo)**.

Możesz także zmienić parametry połączenia z Serwerem administracyjnym później w następujący sposób:

- Możesz zmienić numery portów i portów SSL później w sekcji **Porty połączenia** we właściwościach Serwera administracyjnego. Aby uzyskać więcej informacji na temat portów połączenia Serwera administracyjnego, zobacz Porty używane przez Kaspersky Security Center.

- Możesz zmienić długość klucza szyfrowania podczas zastępowania certyfikatu Serwera administracyjnego narzędziem klsetsrvcert przy użyciu parametru `-o RsaKeyLen:<długość klucza>`.

Krok 17. Określanie adresu Serwera administracyjnego

Określ adres Serwera administracyjnego. Możesz wybrać jedną z następujących opcji:

- **Nazwa domeny DNS**. Metoda ta jest użyteczna, gdy sieć zawiera serwer DNS, którego urządzenia klienckie mogą użyć do uzyskania adresu Serwera administracyjnego.

- **Nazwa NetBIOS**. Metoda ta jest przydatna, gdy urządzenia klienckie uzyskują adres Serwera administracyjnego za pośrednictwem protokołu NetBIOS lub gdy w sieci dostępny jest serwer WINS.

- **Adres IP**. Metoda ta jest używana, gdy Serwer administracyjny posiada stały adres IP, który w przyszłości nie zostanie zmieniony.

Krok 18. Adres Serwera administracyjnego dla podłączenia urządzeń mobilnych

Ten krok kreatora instalacji jest dostępny, jeśli moduł Zarządzanie urządzeniami mobilnymi został wybrany do zainstalowania.

W oknie **Adres do podłączenia urządzeń mobilnych** określ zewnętrzny adres Serwera administracyjnego dla podłączenia urządzeń mobilnych, które znajdują się poza siecią lokalną. Możesz określić adres IP lub system nazw domen (DNS) Serwera administracyjnego.

Krok 19. Wypakowywanie i instalowanie plików na dysku twardym

Po skonfigurowaniu instalacji modułów Kaspersky Security Center, możesz rozpocząć instalację plików na dysku twardym.

Jeśli instalacja wymaga dodatkowych programów, kreator instalacji powiadomi Cię o tym w oknie **Instalacja wymaganego oprogramowania** przed rozpoczęciem instalacji Kaspersky Security Center. Wymagane programy są instalowane automatycznie po kliknięciu przycisku **Dalej**.

W ostatnim kroku możesz wybrać, którą konsolę uruchomić do pracy z Kaspersky Security Center:

- **Uruchom Konsolę administracyjną MMC**
- **Uruchom Kaspersky Security Center Web Console**

  Ta opcja jest dostępna tylko wtedy, gdy w jednym z poprzednich kroków wybrano instalację Kaspersky Security Center Web Console.

Możesz także kliknąć **Zakończ**, aby zamknąć kreator bez rozpoczynania pracy z Kaspersky Security Center. Możesz rozpocząć pracę później w dowolnym momencie.

Przy pierwszym uruchomieniu Konsoli administracyjnej lub Kaspersky Security Center Web Console możesz przeprowadzić wstępną konfigurację aplikacji.

Instalowanie Serwera administracyjnego w trybie cichym

Serwer administracyjny może zostać zainstalowany w trybie cichym, czyli bez interaktywnego wprowadzania ustawień instalacji.

W celu zainstalowania Serwera administracyjnego na urządzeniu lokalnym w trybie cichym:

1. Przeczytaj Umowę licencyjną użytkownika końcowego. Użyj poniższego polecenia tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.
2. Przeczytaj Politykę prywatności. Użyj poniższego polecenia tylko wtedy, gdy rozumiesz i zgadzasz się, żeby Twoje dane były zarządzane i przesyłane (w tym do innych krajów) w sposób opisany w Polityce prywatności.
3. Uruchom polecenie

   ```
   setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <parametry_ustawień>"
   ```

gdzie `setup_parameters` to lista parametrów i ich odpowiednich wartości oddzielonych spacjami (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). Plik setup.exe zlokalizowany jest w folderze Server, który jest częścią pakietu dystrybucyjnego Kaspersky Security Center.

Nazwy i możliwe wartości parametrów, które mogą być wykorzystywane podczas instalacji Serwera administracyjnego w trybie cichym, wyszczególnione są w tabeli poniżej.

Parametry instalacji Serwera administracyjnego w trybie cichym

Nazwa parametru	Opis parametru	Dostępne wartości
EULA	Akceptacja postanowień i warunków Umowy licencyjnej.	• 1 — W pełni przeczytałem(am), rozumiem i akceptuję warunki Umowy Licencyjnej Użytkownika Końcowego. • Inna wartość lub brak wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
PRIVACYPOLICY	Akceptacja postanowień i warunków Polityki prywatności.	• 1 — Jestem świadomy(a) i wyrażam zgodę na przetwarzanie oraz przesyłanie moich danych (również do innych krajów) zgodnie z Polityką prywatności. Potwierdzam, że w pełni przeczytałem(am) i rozumiem Politykę prywatności. • Inna wartość lub bez wartości — Nie akceptuję postanowień i warunków Polityki prywatności (instalacja nie zostanie wykonana).
INSTALLATIONMODETYPE	Typ instalacji Serwera administracyjnego.	• Standard — instalacja standardowa. • Custom — instalacja niestandardowa.
INSTALLDIR	Ścieżka do folderu instalacyjnego Serwera administracyjnego.	Wartość wiersza.
ADDLOCAL	Lista instalowanych komponentów Serwera administracyjnego (oddzielone przecinkami).	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Minimalna lista komponentów wystarczających do poprawnego zainstalowania Serwera administracyjnego: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`.
NETRANGETYPE	Rozmiar sieci (liczba urządzeń w sieci).	• NRT_1_100 — od 1 do 100 urządzeń. • NRT_100_1000 — od 101 do 1000 urządzeń. • NRT_GREATER_1000 — więcej niż 1000 urządzeń.
SRV_ACCOUNT_TYPE	Tryb określania konta, z poziomu którego Serwer administracyjny zostanie uruchomiony jako usługa.	• SrvAccountDefault — konto jest tworzone automatycznie. • SrvAccountUser — konto jest określane ręcznie. W tym przypadku należy określić wartości dla parametrów `SERVERACCOUNTNAME` i `SERVERACCOUNTPWD`.
SERVERACCOUNTNAME	Nazwa konta, z poziomu którego Serwer administracyjny zostanie uruchomiony jako usługa. Należy określić wartość dla parametru, jeśli istnieje SRV_ACCOUNT_TYPE=SrvAccountUser.	Wartość wiersza.

Nazwa parametru	Opis parametru	Dostępne wartości
SERVERACCOUNTPWD	Hasło do konta, z poziomu którego Serwer administracyjny będzie uruchamiany jako usługa. Należy określić wartość dla ustawienia, jeśli istnieje SRV_ACCOUNT_TYPE=SrvAccountUser.	Wartość wiersza.
SERVERCER	Długość klucza certyfikatu Serwera administracyjnego (bity).	• 1 — długość klucza certyfikatu Serwera administracyjnego wynosi 2048 bitów. • Bez wartości — długość klucza certyfikatu Serwera administracyjnego wynosi 1024 bity.
DBTYPE	Typ bazy danych, która będzie używana do przechowywania bazy danych Serwera administracyjnego. Ten parametr jest obowiązkowy.	• MySQL—używana będzie baza danych MySQL lub MariaDB. W tym przypadku należy określić wartości parametrów `MYSQLSERVERNAME`, `MYSQLSERVERPORT`, `MYSQLDBNAME`, `MYSQLACCOUNTNAME` i `MYSQLACCOUNTPWD`. • MSSQL—używana będzie baza danych Microsoft SQL Server (SQL Express). W tym przypadku należy określić wartości parametrów `MSSQLSERVERNAME`, `MSSQLDBNAME` i `MSSQLAUTHTYPE`. • POSTGRES — zostanie użyta baza danych PostgreSQL lub Postgres Pro. W tym przypadku należy określić wartości parametrów `POSTGRESSERVERNAME`, `POSTGRESSERVERPORT`, `POSTGRESDBNAME`, `POSTGRESACCOUNTNAME` i `POSTGRESACCOUNTPWD`.
MYSQLSERVERNAME	Pełna nazwa serwera SQL. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MySQL.	Wartość wiersza.
MYSQLSERVERPORT	Numer portu do nawiązania połączenia z serwerem SQL. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MySQL.	Wartość numeryczna.
MYSQLDBNAME	Nazwa bazy danych, która zostanie utworzona w celu przechowywania danych Serwera administracyjnego. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MySQL.	Wartość wiersza.
MYSQLACCOUNTNAME	Nazwa konta do łączenia z bazą danych. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MySQL.	Wartość wiersza.
MYSQLACCOUNTPWD	Hasło do konta do łączenia z bazą danych. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MySQL.	Wartość wiersza.
MSSQLSERVERNAME	Pełna nazwa serwera SQL. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MSSQL.	Wartość wiersza.
MSSQLDBNAME	Nazwa bazy danych. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MSSQL.	Wartość wiersza.
MSSQLAUTHTYPE	Typ uwierzytelniania podczas nawiązywania połączenia z serwerem SQL. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MSSQL.	• Windows—tryb uwierzytelniania Microsoft Windows. • SQLServer — tryb uwierzytelniania serwera SQL. W tym przypadku należy określić wartości dla parametrów `MSSQLACCOUNTNAME` i `MSSQLACCOUNTPWD`.
MSSQLACCOUNTNAME	Nazwa konta do nawiązania połączenia z serwerem SQL. Należy określić wartość dla parametru, jeśli istnieje MSSQLAUTHTYPE=SQLServer.	Wartość wiersza.
MSSQLACCOUNTPWD	Hasło do konta do nawiązania połączenia z serwerem SQL. Należy określić wartość dla parametru, jeśli istnieje MSSQLAUTHTYPE=SQLServer.	Wartość wiersza.
CREATE_SHARE_TYPE	Metoda określania folderu współdzielonego.	• Create—tworzy nowy folder współdzielony. W tym przypadku należy określić wartości parametrów `SHARELOCALPATH` i `SHAREFOLDERNAME`. • ChooseExisting — wybiera istniejący folder. W tym przypadku należy określić wartość parametru `EXISTSHAREFOLDERNAME`.
SHARELOCALPATH	Pełna ścieżka dostępu do folderu lokalnego. Należy określić wartość dla parametru, jeśli istnieje CREATE_SHARE_TYPE=Create	Wartość wiersza.

Nazwa parametru	Opis parametru	Dostępne wartości
SHAREFOLDERNAME	Nazwa sieciowa folderu współdzielonego. Należy określić wartość dla parametru, jeśli istnieje CREATE_SHARE_TYPE=Create.	Wartość wiersza.
EXISTSHAREFOLDERNAME	Pełna ścieżka dostępu do istniejącego folderu współdzielonego. Należy określić wartość dla parametru, jeśli istnieje CREATE_SHARE_TYPE=ChooseExisting.	Wartość wiersza.
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym.	Wartość numeryczna.
SERVERSSLPORT	Numer portu dla szyfrowanego połączenia z Serwerem administracyjnym przy użyciu protokołu SSL.	Wartość numeryczna.
SERVERADDRESS	Adres Serwera administracyjnego.	Wartość wiersza.
MOBILESERVERADDRESS	Adres Serwera administracyjnego dla podłączenia urządzeń mobilnych.	Wartość wiersza.

Szczegółowy opis parametrów instalacji Serwera administracyjnego znajduje się w sekcji Instalacja niestandardowa.

Instalowanie Konsoli administracyjnej na stacji roboczej administratora

Możesz oddzielnie zainstalować Konsolę administracyjną na stacji roboczej administratora i zarządzać Serwerem administracyjnym przez sieć przy pomocy tej Konsoli.

W celu zainstalowania Konsoli administracyjnej na stacji roboczej administratora:

1. Uruchom plik wykonywalny setup.exe.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania.

2. W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj wyłącznie Konsolę administracyjną Kaspersky Security Center**, aby uruchomić kreator instalacji Konsoli administracyjnej. Postępuj zgodnie z instrukcjami kreatora.

3. Wybierz folder docelowy. Domyślnie jest to <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie w trakcie instalacji. Można zmienić folder docelowy przy użyciu przycisku **Przeglądaj**.

4. W ostatnim oknie kreatora instalacji kliknij przycisk **Uruchom**, aby uruchomić instalację Konsoli administracyjnej.

Po zakończeniu pracy kreatora, Konsola administracyjna zostanie zainstalowana na stacji roboczej administratora.

W celu zainstalowania Konsoli administracyjnej na stacji roboczej administratora w trybie cichym:

1. Przeczytaj Umowę licencyjną użytkownika końcowego. Użyj poniższego polecenia tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej użytkownika końcowego.

2. W folderze `Distrib\Console` zestawu dystrybucyjnego Kaspersky Security Center uruchom plik setup.exe za pomocą następującego polecenia:

   ```
   setup.exe /s /v"EULA=1"
   ```

   Jeśli chcesz zainstalować wszystkie wtyczki zarządzające z folderu `Distrib\Console\Plugins` wraz z Konsolą administracyjną, uruchom następujące polecenie:

```
setup.exe /s /v"EULA=1" /pALL
```

Jeśli chcesz określić, które wtyczki zarządzające mają zostać zainstalowane z folderu `Distrib\Console\Plugins` wraz z Konsolą administracyjną, określ wtyczki po kluczu „/p" i oddziel je średnikiem:

```
setup.exe /s /v"EULA=1" /pP1;P2;P3
```

gdzie `P1`, `P2`, `P3` to nazwy wtyczek, które odpowiadają nazwom folderów wtyczek w folderze `Distrib\Console\Plugins`. Na przykład:

```
setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
```

Konsola administracyjna i wtyczki zarządzające (jeśli istnieją) zostaną zainstalowane na stacji roboczej administratora.

Po zainstalowaniu Konsoli administracyjnej musisz połączyć się z Serwerem administracyjnym. W tym celu uruchom Konsolę administracyjną i w otwartym oknie określ nazwę lub adres IP urządzenia, na którym został zainstalowany Serwer administracyjny, a także ustawienia konta używanego do nawiązywania połączenia. Po nawiązaniu połączenia z Serwerem administracyjnym możesz zarządzać systemem ochrony antywirusowej przy pomocy Konsoli administracyjnej.

Możesz usunąć Konsolę administracyjną przy pomocy standardowych narzędzi dodawania/usuwania z Microsoft Windows.

Zmiany w systemie po instalacji Kaspersky Security Center

Ikona Konsoli administracyjnej

Po zainstalowaniu Konsoli administracyjnej na urządzeniu, pojawi się jej ikona i będzie można jej użyć do uruchomienia Konsoli administracyjnej. Odszukaj Konsolę administracyjną w menu **Start** → **Programy** → **Kaspersky Security Center**.

Usługi Serwera administracyjnego i Agenta sieciowego

Serwer administracyjny i Agent sieciowy zostaną zainstalowane na urządzeniu jako usługi z właściwościami wymienionymi poniżej. Tabela zawiera również atrybuty innych usług, które są stosowane na urządzeniu po zainstalowaniu Serwera administracyjnego.

Właściwości usług Kaspersky Security Center

Moduł	Nazwa usługi	Wyświetlona nazwa usługi	Konto
Serwer administracyjny	kladminserver	Serwer administracyjny Kaspersky Security Center	Nieuprzywilejowane konto dedykowane lub zdefiniowane przez użytkownika w formacie KL-AK-*, utworzone podczas instalacji
Agent sieciowy	klnagent	Agent sieciowy Kaspersky Security Center	System lokalny
Serwer sieciowy umożliwiający dostęp do konsoli Kaspersky Security Center Web Console i zarządzanie siecią wewnętrzną organizacji	klwebsrv	Serwer sieciowy Kaspersky	Dedykowane konto bez uprawnień KlScSvc

Aktywacja serwera proxy	klactprx	Kaspersky activation proxy server	Dedykowane konto bez uprawnień KlScSvc
Serwer KSN proxy	ksnproxy	Serwer proxy Kaspersky Security Network	Dedykowane konto bez uprawnień KlScSvc

Jeśli instalujesz Kaspersky Security Center na węzłach klastra trybu failover Kaspersky Security Center, dostępna stanie się usługa klfocsvc_klfoc. Usługi klnagent_klfoc i klfocsvc_klfoc działają na lokalnym koncie systemowym. Usługa kladminserver_klfoc musi być uruchomiona na koncie „ksc", a inne usługi na koncie „rightless". Konta „ksc" i „rightless" należy dodać do grupy KLAdmins z uprawnieniami lokalnego administratora. Dla poprawnego działania Kaspersky Security Center do uruchamiania usług należy używać wyłącznie kont „ksc" i „rightless". Nie zalecamy korzystania z innych kont z tymi samymi uprawnieniami. Poniższa tabela zawiera właściwości usług, które są stosowane na urządzeniu po zainstalowaniu Serwera administracyjnego w klastrze trybu failover Kaspersky Security Center.

Właściwości usług Kaspersky Security Center zainstalowanych w klastrze trybu failover Kaspersky Security Center

Moduł	Nazwa usługi	Wyświetlona nazwa usługi	Konto
Serwer administracyjny	kladminserver_klfoc	Serwer administracyjny Kaspersky Security Center	ksc
Agent sieciowy	klnagent_klfoc	Agent sieciowy Kaspersky Security Center	System lokalny
Serwer sieciowy umożliwiający dostęp do konsoli Kaspersky Security Center Web Console i zarządzanie siecią wewnętrzną organizacji	klwebsrv_klfoc	Serwer sieciowy Kaspersky	rightless
Aktywacja serwera proxy	klactprx_klfoc	Kaspersky activation proxy server	rightless
Serwer KSN proxy	ksnproxy_klfoc	Serwer proxy Kaspersky Security Network	rightless
Klaster trybu failover Kaspersky Security Center	klfocsvc_klfoc	Klaster trybu failover Kaspersky Security Center	System lokalny

Usługi Kaspersky Security Center Web Console

Jeśli zainstalujesz Kaspersky Security Center Web Console na urządzeniu, zostaną zainstalowane następujące usługi (zobacz poniższą tabelę):

Usługi Kaspersky Security Center Web Console

Wyświetlona nazwa usługi	Konto
Kaspersky Security Center Service Web Console	NT Service/KSCSvcWebConsole
Kaspersky Security Center Web Console	Usługa sieciowa
Kaspersky Security Center Product Plugins Server	NT Service/KSCWebConsolePlugin
Usługa zarządzania Kaspersky Security Center Web Console	System lokalny
Kolejka wiadomości Kaspersky Security Center Web Console	NT Service/KSCWebConsoleMessageQueue

Wersja serwerowa Agenta sieciowego

Wersja serwerowa Agenta sieciowego zostanie zainstalowana na urządzeniu wraz z Serwerem administracyjnym. Wersja serwerowa Agenta sieciowego jest częścią Serwera administracyjnego i jest instalowana i usuwana wraz z Serwerem administracyjnym. Może ona współdziałać z lokalnie zainstalowanym Serwerem administracyjnym. Nie ma konieczności konfigurowania ustawień połączenia Agenta sieciowego z Serwerem administracyjnym: ustawienia te są implementowane poprzez funkcje programu, ponieważ składniki są instalowane na tym samym urządzeniu. Wersja serwerowa Agenta sieciowego jest instalowana z tymi samymi właściwościami co standardowa wersja Agenta i realizuje te same funkcje zarządzania aplikacją. Ta wersja będzie zarządzana przez zasadę grupy administracyjnej, do której należy urządzenie klienckie Serwera administracyjnego. Dla wersji serwerowej Agenta sieciowego wszystkie zadania są tworzone ze zbioru tych przeznaczonych dla Serwera administracyjnego, za wyjątkiem zadania zmiany Serwera.

Agent sieciowy nie może zostać zainstalowany oddzielnie na urządzeniu, na którym jest już zainstalowany Serwer administracyjny.

Możesz wyświetlić właściwości każdej usługi Serwera administracyjnego i Agenta sieciowego, jak również monitorować ich działanie przy pomocy standardowych narzędzi zarządzających Microsoft Windows: Zarządzanie komputerem\Usługi. Informacja o aktywności usługi Serwera administracyjnego Kaspersky jest przechowywana w dzienniku systemu Microsoft Windows, w oddzielnej gałęzi dziennika zdarzeń aplikacji Kaspersky na urządzeniu, na którym jest zainstalowany Serwer administracyjny.

Zalecamy unikanie ręcznego uruchamiania i zatrzymywania usług oraz pozostawiania niezmienionych kont usług w ustawieniach usług. Jeśli to konieczne, możesz zmodyfikować konto usługi Serwera administracyjnego przy użyciu narzędzia klsrvswch. Pamiętaj, że musisz uruchomić narzędzie klsrvswch na urządzeniu Serwera administracyjnego z poziomu konta z uprawnieniami administratora, które zostało użyte do instalacji Serwera administracyjnego.

Konta użytkowników i grupy bezpieczeństwa

Instalator Serwera administracyjnego domyślnie tworzy następujące konta:

- KL-AK-*: konto usługi Serwera administracyjnego
- KlScSvc: konto dla innych usług z puli Serwera administracyjnego
- KlPxeUser: konto do zdalnej instalacji systemów operacyjnych

Jeśli podczas działania instalatora wybrałeś inne konta dla usługi Serwera administracyjnego i innych usług, używane są określone konta.

Na urządzeniu z zainstalowanym Serwerem administracyjnym zostaną także automatycznie utworzone lokalne grupy zabezpieczeń o nazwach KLAdmins i KLOperators z ich odpowiednimi zestawami uprawnień.

Nie zaleca się instalacji Serwera administracyjnego na kontrolerze domeny; jeśli jednak instalujesz Serwer administracyjny na kontrolerze domeny, należy uruchomić instalator z uprawnieniami administratora. W tym przypadku instalator automatycznie tworzy grupy bezpieczeństwa domeny o nazwie KLAdmins i KLOperators. Jeśli instalujesz Serwer administracyjne na urządzeniu, które nie znajduje się w kontrolerze domeny, powinieneś uruchomić instalator z uprawnieniami lokalnego administratora. W tym przypadku instalator automatycznie tworzy lokalne grupy bezpieczeństwa o nazwie KLAdmins i KLOperators.

Podczas konfigurowania powiadamiania pocztą elektroniczną, konieczne może być utworzenie konta na serwerze pocztowym dla autoryzacji ESMTP.

Dezinstalowanie aplikacji

Możesz usunąć Kaspersky Security Center przy pomocy standardowych narzędzi dodawania/usuwania Microsoft Windows. Usuwanie aplikacji wymaga uruchomienia kreatora, który usunie wszystkie moduły aplikacji z urządzenia (łącznie z wtyczkami). Kreator sprawia, że domyślna przeglądarka otwiera stronę internetową z ankietą, na której możesz nam powiedzieć, dlaczego zdecydowałeś się zaprzestać korzystania z Kaspersky Security Center. Jeśli podczas działania kreatora nie wybrałeś do usunięcia folderu współdzielonego (KLSHARE), usuń go ręcznie po zakończeniu wszystkich zadań, które mają do niego dostęp.

Po usunięciu aplikacji, niektóre jej pliki mogą pozostać w folderze tymczasowym systemu.

Kreator tworzenia zadania usuwania aplikacji zasugeruje przechowywanie kopii zapasowej Serwera administracyjnego.

Gdy aplikacja zostanie usunięta z systemów Microsoft Windows 7 i Microsoft Windows 2008, może nastąpić przedwczesne zakończenie działania kreatora tworzenia zadania usuwania aplikacji. Można tego uniknąć przez wyłączenie w systemie operacyjnym Kontroli konta użytkownika (UAC) i ponowne uruchomienie usuwania aplikacji.

Informacje o aktualizacji Kaspersky Security Center

Ta sekcja zawiera informacje o tym, jak zaktualizować Kaspersky Security Center z poprzedniej wersji. Możesz zaktualizować Kaspersky Security Center na różne sposoby, w zależności od tego, czy Kaspersky Security Center został zainstalowany lokalnie, czy na węzłach klastra trybu failover Kaspersky Security Center.

Podczas aktualizacji równoczesne korzystanie z DBMS przez Serwer administracyjny i inną aplikację jest surowo zabronione.

Pamiętaj, że jeśli zaktualizujesz Serwer administracyjny do wersji 15.1, nie będzie można tworzyć nowych pakietów instalacyjnych Agenta sieciowego w wersji 15 lub wcześniejszej. Jednakże wcześniej utworzone pakiety instalacyjne będą dostępne.

Podczas, gdy aktualizujesz Kaspersky Security Center z poprzedniej wersji, wszystkie zainstalowane wtyczki obsługiwanych aplikacji Kaspersky są zachowywane. Wtyczka Serwera administracyjnego oraz wtyczka Agenta sieciowego są aktualizowane automatycznie (zarówno dla Konsoli administracyjnej, jak i dla Kaspersky Security Center Web Console).

Aktualizowanie Kaspersky Security Center z poprzedniej wersji

Następujący temat opisuje zalecane kroki przygotowania do uaktualnienia: Aktualizowanie Kaspersky Security Center i zarządzanych aplikacji zabezpieczających.

Możesz zainstalować Serwer administracyjny w wersji 15.1 na urządzeniu, na którym jest zainstalowana wcześniejsza wersja Serwera administracyjnego (począwszy od wersji 11 (11.0.0.1131b)). Podczas aktualizowania do wersji 15.1 wszystkie dane i ustawienia z poprzedniej wersji Serwera administracyjnego zostają zachowane.

Jeżeli podczas instalacji Serwera administracyjnego pojawią się problemy, będziesz mógł przywrócić poprzednią wersję Serwera administracyjnego przy pomocy kopii zapasowej danych Serwera administracyjnego utworzonej przed aktualizacją.

Jeśli w sieci zainstalowano przynajmniej jeden Serwer administracyjny w nowej wersji, inne Serwery administracyjne w sieci mogą zostać zaktualizowane przy pomocy zadania zdalnej instalacji, które korzysta z pakietu instalacyjnego Serwera administracyjnego.

Jeśli wdrożyłeś klaster typu failover Kaspersky Security Center, możesz również zaktualizować Kaspersky Security Center na jego węzłach.

W celu zaktualizowania wcześniejszej wersji Serwera administracyjnego do wersji 15.1:

1. Uruchom plik instalacyjny ksc_15.1_<numer wersji>_full_<wersja językowa>.exe dla wersji 15.1 (możesz pobrać ten plik ze strony internetowej Kaspersky).

2. W oknie, które zostanie otwarte, kliknij odnośnik **Zainstaluj Kaspersky Security Center**, aby uruchomić Kreatora instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

3. Przeczytaj treść Umowy licencyjnej i Polityki prywatności. Jeśli zgadzasz się na wszystkie warunki Umowy licencyjnej i Polityki prywatności, w sekcji **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki oraz postanowienia następujących:** zaznacz następujące pola:

   - **Warunki i postanowienia tej Umowy licencyjnej użytkownika końcowego**
   - **Politykę prywatności opisującą zasady przetwarzania danych**

   Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól. Kreator instalacji wyświetla pytanie o utworzenie kopii zapasowej danych Serwera administracyjnego dla wcześniejszej wersji.

   Kaspersky Security Center obsługuje odzyskiwanie danych z kopii zapasowej utworzonej za pomocą starszej wersji Serwera administracyjnego.

4. Jeżeli chcesz utworzyć kopię zapasową danych Serwera administracyjnego, określ to w otwartym oknie **Kopia zapasowa danych Serwera administracyjnego**.

   Kopia zapasowa jest tworzona przez narzędzie klbackup. Narzędzie to jest zawarte w pakiecie dystrybucyjnym aplikacji i znajduje się w głównym folderze instalacyjnym Kaspersky Security Center.

5. Zainstaluj Serwer administracyjny w wersji 15.1, postępując zgodnie z instrukcjami Kreatora instalacji.

   Jeśli pojawi się wiadomość, że usługa Kaspersky Security Center Web Console jest zajęta, w oknie kreatora kliknij przycisk **Ignoruj**.

Należy unikać przerywania działania kreatora instalacji. W przypadku anulowania aktualizacji na etapie instalacji Serwera administracyjnego może spowodować błąd zaktualizowanej wersji Kaspersky Security Center.

6. Dla urządzeń, na których jest instalowana wcześniejsza wersja Agenta sieciowego, utwórz i uruchom zadanie zdalnej instalacji nowej wersji Agenta sieciowego.

   Zalecamy aktualizację Agenta sieciowego dla systemu Linux do tej samej wersji co Kaspersky Security Center.

   Po zakończeniu wykonywania zadania zdalnej instalacji, wersja Agenta sieciowego zostanie zaktualizowana.

   Uruchom następujące polecenia na zasobach opartych na systemie Linux, aby usunąć zależności, które nie są już potrzebne:

   - W przypadku zasobów opartych na systemie Debianie uruchom dowolne z następujących poleceń:
     - `apt-get -y autoremove`
     - `apt -y autoremove`
   - W przypadku zasobów opartych na systemie RPM uruchom dowolne z następujących poleceń:
     - `dnf autoremove`
     - `yum autoremove`

Aktualizowanie Kaspersky Security Center na węzłach klastra trybu failover Kaspersky Security Center

Możesz zainstalować Serwer administracyjny w wersji 15.1 na każdym węźle klastra pracy awaryjnej Kaspersky Security Center, na którym jest zainstalowana wcześniejsza wersja Serwera administracyjnego (począwszy od wersji 13.2). Podczas aktualizowania do wersji 15.1 wszystkie dane i ustawienia z poprzedniej wersji Serwera administracyjnego zostają zachowane.

Jeśli wcześniej zainstalowałeś Kaspersky Security Center na urządzeniach lokalnie, możesz również zaktualizować Kaspersky Security Center na tych urządzeniach.

W celu zaktualizowania Kaspersky Security Center na węzłach klastra trybu failover Kaspersky Security Center:

1. Wykonaj następujące czynności na aktywnym węźle klastra:

   a. Uruchom plik wykonywalny ksc_15.1_<numer kompilacji>_full_<wersja językowa>.exe.

      Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky w celu aktualizacji. Kliknij odnośnik **Zainstaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

b. Przeczytaj treść Umowy licencyjnej i Polityki prywatności. Jeśli zgadzasz się na wszystkie warunki Umowy licencyjnej i Polityki prywatności, w sekcji **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki oraz postanowienia następujących:** zaznacz następujące pola:

- **Warunki i postanowienia tej Umowy licencyjnej użytkownika końcowego**
- **Politykę prywatności opisującą zasady przetwarzania danych**

Zaznacz oba pola wyboru, aby kontynuować instalację.

Jeśli nie akceptujesz Umowy licencyjnej lub Polityki prywatności, kliknij przycisk **Anuluj**, aby anulować aktualizację.

2. Wykonaj te same czynności na węźle pasywnym klastra pracy awaryjnej Kaspersky Security Center, co na węźle aktywnym.

3. Uruchom klaster.

W rezultacie zainstalowano Serwer administracyjny najnowszej wersji na węzłach klastra typu failover Kaspersky Security Center.

Aktualizowanie Kaspersky Security Center na węzłach klastra trybu failover Microsoft

Możesz zainstalować Serwer administracyjny w wersji 15.1 na każdym węźle klastra trybu failover Microsoft, na którym jest zainstalowana wcześniejsza wersja Serwera administracyjnego (począwszy od wersji 13.2). Podczas aktualizowania do wersji 15.1 wszystkie dane i ustawienia z poprzedniej wersji Serwera administracyjnego zostają zachowane.

Aby uaktualnić program Kaspersky Security Center na węzłach klastra trybu failover firmy Microsoft, wykonaj następujące czynności na dowolnym węźle klastra:

1. Uruchom plik wykonywalny ksc_15.1_<numer kompilacji>_full_<wersja językowa>.exe.

Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky w celu aktualizacji. Kliknij odnośnik **Zainstaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

2. Przeczytaj treść Umowy licencyjnej i Polityki prywatności. Jeśli zgadzasz się na wszystkie warunki Umowy licencyjnej i Polityki prywatności, w sekcji **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki oraz postanowienia następujących:** zaznacz następujące pola:

- **Warunki i postanowienia tej Umowy licencyjnej użytkownika końcowego**
- **Politykę prywatności opisującą zasady przetwarzania danych**

Zaznacz oba pola wyboru, aby kontynuować instalację.

Jeśli nie akceptujesz Umowy licencyjnej lub Polityki prywatności, kliknij przycisk **Anuluj**, aby anulować aktualizację.

3. W oknie **Typ instalacji na klastrze** wybierz opcję **Klaster (instalacja na wszystkich węzłach klastra)**.

   Następnie instalator konfiguruje i kończy uaktualnianie Serwera administracyjnego na wszystkich węzłach klastra. Podczas aktualizacji nie można zmienić ustawień Serwera administracyjnego.

W rezultacie zainstalowałeś najnowszą wersję Serwera administracyjnego na węzłach klastra trybu failover Microsoft.

Wstępna konfiguracja Kaspersky Security Center

Ta sekcja opisuje kroki, jakie musisz podjąć po zainstalowaniu Kaspersky Security Center, aby przeprowadzić jego wstępną konfigurację.

Przewodnik po zwiększaniu odporności

Przewodnik zwiększania bezpieczeństwa jest przeznaczony dla profesjonalistów, którzy instalują i administrują Kaspersky Security Center, a także dla tych, którzy zapewniają wsparcie techniczne organizacjom korzystającym z Kaspersky Security Center.

Przewodnik zwiększania bezpieczeństwa opisuje zalecenia i funkcje konfigurowania Kaspersky Security Center i jego komponentów, mające na celu zmniejszenie ryzyka związanego z jego włamaniem.

Przed rozpoczęciem konfiguracji utwórz kopię zapasową Serwera administracyjnego Kaspersky Security Center za pomocą zadania Kopia zapasowa danych Serwera administracyjnego lub narzędzia klbackup i zapisz ją w bezpiecznym miejscu.

Przewodnik zwiększania bezpieczeństwa zawiera następujące informacje:

- Wybór architektury Serwera administracyjnego
- Konfigurowanie bezpiecznego połączenia z Serwerem administracyjnym
- Konfigurowanie kont w celu uzyskania dostępu do Serwera administracyjnego
- Zarządzanie ochroną Serwera administracyjnego i urządzeń klienckich
- Konfigurowanie ochrony dla zarządzanych aplikacji
- Konserwacja Serwera administracyjnego
- Przesyłanie informacji do aplikacji firm trzecich

Przed rozpoczęciem pracy z Serwerem administracyjnym Kaspersky Security Center wyświetli monit o przeczytanie skróconej wersji Przewodnika zwiększania bezpieczeństwa.

Pamiętaj, że nie możesz korzystać z Serwera administracyjnego, dopóki nie potwierdzisz przeczytania Przewodnika zwiększania bezpieczeństwa.

Aby przeczytać Przewodnik zwiększania bezpieczeństwa:

1. Otwórz Konsolę administracyjną lub Kaspersky Security Center Web Console i zaloguj się do konsoli. Konsola sprawdza potwierdzenie przeczytania aktualnej wersji Przewodnika zwiększania bezpieczeństwa.

   Jeśli jeszcze nie znasz treści Przewodnika zwiększania bezpieczeństwa, otworzy się okno i wyświetli jego krótką wersję.

2. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz wyświetlić skróconą wersję Przewodnika po zwiększaniu odporności w formie dokumentu tekstowego, kliknij łącze **Otwórz w nowym oknie**.

   - Jeśli chcesz zobaczyć pełną wersję Przewodnika po zwiększaniu odporności, kliknij łącze **Otwórz podręcznik wzmacniania zabezpieczeń w Pomocy Online**.

3. Po przeczytaniu Przewodnika po zwiększaniu odporności zaznacz pole wyboru **Potwierdzam, że w pełni przeczytałem(-am) i rozumiem przewodnik wzmacniania zapezbieczeń**, a następnie kliknij przycisk **Zaakceptuj**.

Teraz możesz pracować z Serwerem administracyjnym.

Gdy pojawi się nowa wersja Przewodnika zwiększania bezpieczeństwa, Kaspersky Security Center wyświetli monit o jej przeczytanie.

Kreator wstępnej konfiguracji Serwera administracyjnego

Ta sekcja zawiera informacje o działaniu kreatora wstępnej konfiguracji Serwera administracyjnego.

Informacje o kreatorze wstępnej konfiguracji

Ta sekcja zawiera informacje o działaniu kreatora wstępnej konfiguracji Serwera administracyjnego.

Kreator wstępnej konfiguracji Serwera administracyjnego umożliwia utworzenie minimalnej ilości potrzebnych zadań i zasad, dostosowanie minimalnych ustawień, pobranie i zainstalowanie wtyczek dla zarządzanych aplikacji firmy Kaspersky, a także utworzenie pakietów instalacyjnych zarządzanych aplikacji firmy Kaspersky. Przy pierwszym uruchomieniu kreatora możesz wprowadzić w aplikacji następujące zmiany:

- Pobierz i zainstaluj wtyczki dla zarządzanych aplikacji. Po zakończeniu pracy kreatora wstępnej konfiguracji, lista zainstalowanych wtyczek zarządzających zostanie wyświetlona w sekcji **Zaawansowane → Szczegóły zainstalowanych wtyczek administrujących aplikacją** okna właściwości Serwera administracyjnego.

- Utwórz pakiety instalacyjne zarządzanych aplikacji firmy Kaspersky. Po zakończeniu pracy Kreatora wstępnej konfiguracji, pakiety instalacyjne Agenta sieciowego dla systemu for Windows i zarządzanych aplikacji firmy Kaspersky są wyświetlane na liście **Serwer administracyjny → Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

- Dodaj pliki klucza lub wprowadź kody aktywacyjne, które mogą być automatycznie przesyłane do urządzeń w grupach administracyjnych. Po zakończeniu pracy Kreatora wstępnej konfiguracji, informacje o kluczach licencyjnych są wyświetlane na liście **Serwer administracyjny → Licencje Kaspersky** oraz w sekcji **Klucze licencyjne** okna właściwości Serwera administracyjnego.

- Skonfigurować interakcję z Kaspersky Security Network (KSN).
- Skonfigurować dostarczanie powiadomień informujących o zdarzeniach występujących podczas działania Serwera administracyjnego i zarządzanych aplikacji (w celu zapewnienia poprawnego działania opcji dostarczania powiadomień, na Serwerze administracyjnym i wszystkich urządzeniach, na które mają być wysyłane powiadomienia, powinna być włączona usługa Posłaniec). Po zakończeniu pracy kreatora wstępnej konfiguracji, ustawienia powiadomień e-mail są wyświetlane w sekcji **Powiadamianie** okna właściwości Serwera administracyjnego.
- Dostosować ustawienia aktualizacji oraz ustawienia eliminowania luk dla aplikacji zainstalowanych na urządzeniach.
- Utworzyć zasadę ochrony dla stacji roboczych i serwerów, a także zadania skanowania w poszukiwaniu złośliwego oprogramowania, zadania pobierania aktualizacji i zadania tworzenia kopii zapasowej danych dla najwyższego poziomu hierarchii zarządzanych urządzeń. Po zakończeniu pracy kreatora wstępnej konfiguracji, utworzone zadania są wyświetlane na liście **Serwer administracyjny** → **Zadania**, zasady odpowiadające wtyczkom dla zarządzanych aplikacji są wyświetlane na liście **Serwer administracyjny** → **Zasady**.

Kreator wstępnej konfiguracji tworzy zasady dla zarządzanych aplikacji, takich jak Kaspersky Endpoint Security for Windows, dopóki te zasady nie zostały już utworzone dla grupy **Zarządzane urządzenia**. Kreator wstępnej konfiguracji tworzy zadania, jeśli zadania z tymi samymi nazwami nie istnieją dla grupy **Zarządzane urządzenia**.

W Konsoli administracyjnej Kaspersky Security Center automatycznie wyświetli pytanie o uruchomienie kreatora wstępnej konfiguracji po uruchomieniu go po raz pierwszy. Kreator wstępnej konfiguracji można również uruchomić ręcznie w dowolnym momencie.

Uruchamianie kreatora wstępnej konfiguracji Serwera administracyjnego

Po zainstalowaniu Serwera administracyjnego, przy pierwszym nawiązaniu połączenia z nim, aplikacja automatycznie wyświetli pytanie dotyczące uruchomienia kreatora wstępnej konfiguracji. Kreator wstępnej konfiguracji można również uruchomić ręcznie w dowolnym momencie.

W celu ręcznego uruchomienia kreatora wstępnej konfiguracji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego węzła wybierz **Wszystkie zadania** → **Kreator wstępnej konfiguracji Serwera administracyjnego**.

   kreator wyświetli pytanie o przeprowadzenie wstępnej konfiguracji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

Jeśli ponownie uruchomisz Kreator wstępnej konfiguracji, zadania i zasady utworzone przy poprzednim uruchomieniu kreatora nie mogą zostać ponownie utworzone.

Krok 1. Konfigurowanie serwera proxy

Określ ustawienia dostępu do Internetu dla Serwera administracyjnego. Należy skonfigurować dostęp do Internetu w taki sposób, aby korzystać z Kaspersky Security Network i pobierać aktualizacje antywirusowych baz danych dla Kaspersky Security Center i zarządzanych aplikacji Kaspersky.

Wybierz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest wybrana, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

- **Adres**

  Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

- **Numer portu**

  Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

- **Pomiń serwer proxy dla adresów lokalnych**

  Żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

- **Uwierzytelnianie na serwerze proxy**

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

- **Nazwa użytkownika**

  Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

- **Hasło**

  Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

  Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

Możesz skonfigurować dostęp do Internetu później, niezależnie od kreatora wstępnej konfiguracji.

Krok 2. Wybieranie metody aktywacji aplikacji

Wybierz jedną z poniższych opcji aktywacji Kaspersky Security Center:

- **Wprowadzając kod aktywacyjny**

  Kod aktywacyjny to unikatowa sekwencja 20 znaków alfanumerycznych. Możesz wprowadzić kod aktywacyjny w celu dodania klucza aktywującego Kaspersky Security Center. Możesz otrzymać kod aktywacyjny na adres e-mail, który określiłeś po zakupieniu Kaspersky Security Center.

  Aby aktywować aplikację za pomocą kodu aktywacyjnego, potrzebny jest dostęp do internetu w celu nawiązania połączenia z serwerami aktywacji Kaspersky.

  Jeśli wybrano tę opcję aktywacji, możesz włączyć opcję **Automatycznie roześlij klucz licencyjny do zarządzanych urządzeń**.

  Jeśli ta opcja jest włączona, klucz licencyjny zostanie automatycznie zainstalowany na zarządzanych urządzeniach.

  Jeśli ta opcja jest wyłączona, możesz wdrożyć klucz licencyjny na zarządzanych urządzeniach później, w węźle **Licencje Kaspersky** drzewa Konsoli administracyjnej.

Jeśli aktywacja poprzez podanie kodu aktywacyjnego nie powiodła się z jakiegokolwiek powodu, możesz aktywować aplikację poprzez podanie pliku klucza.

- **Określając plik klucza**

  Plik klucza to plik z rozszerzeniem .key, dostarczony przez firmę Kaspersky. Plik klucza jest przeznaczony do dodania klucza aktywującego aplikację.

  Metody uzyskiwania pliku klucza opisano w poniższej sekcji: O pliku klucza.

  Aby aktywować aplikację przy pomocy pliku klucza, nie musisz łączyć się z serwerami aktywacji Kaspersky.

  Jeśli wybrano tę opcję aktywacji, możesz włączyć opcję **Automatycznie roześlij klucz licencyjny do zarządzanych urządzeń**.

  Jeśli ta opcja jest włączona, klucz licencyjny zostanie automatycznie zainstalowany na zarządzanych urządzeniach.

  Jeśli ta opcja jest wyłączona, możesz wdrożyć klucz licencyjny na zarządzanych urządzeniach później, w węźle **Licencje Kaspersky** drzewa Konsoli administracyjnej.

- **Odraczając aktywację aplikacji**

  Aplikacja będzie działała z podstawową funkcjonalnością, bez Zarządzania urządzeniami mobilnymi oraz bez Zarządzania systemami.

Jeśli wybierzesz opcję odroczenia aktywacji aplikacji, będziesz mógł dodać klucz licencyjny w późniejszym czasie.

Krok 3. Wybór obszarów ochrony i systemów operacyjnych

Wybierz obszary ochrony i systemy operacyjne używane w Twojej sieci. Jeśli wybierzesz te opcje, określ filtry dla wtyczek zarządzających aplikacjami i pakietami dystrybucyjnymi na serwerach Kaspersky, które możesz pobrać do zainstalowania na urządzeniach klienckich w Twojej sieci. Wybierz opcje:

- **Obszary**

  Możesz wybrać następujące obszary ochrony:

  - **Stacje robocze**. Wybierz tę opcję, jeśli chcesz chronić stacje robocze w swojej sieci. Domyślnie zaznaczona jest opcja Stacja robocza.
  - **Serwery plików i magazyny**. Wybierz tę opcję, jeśli chcesz chronić serwery plików w swojej sieci.
  - **Urządzenia mobilne**. Wybierz tę opcję, jeśli chcesz chronić urządzenia mobilne należące do firmy lub pracowników firmy. Jeśli wybierzesz tę opcję, ale nie dostarczyłeś licencji z funkcją Zarządzanie urządzeniami mobilnymi, zostanie wyświetlona wiadomość informująca o konieczności dostarczenia licencji z funkcją Zarządzanie urządzeniami mobilnymi. Jeśli nie dostarczysz licencji, nie możesz korzystać z funkcji Urządzenia mobilne.
  - **Wirtualizacja**. Wybierz tę opcję, jeśli chcesz chronić maszyny wirtualne w swojej sieci.
  - **Kaspersky Anti-Spam**. Wybierz tę opcję, jeśli chcesz chronić serwery pocztowe w swojej organizacji przed spamem, szkodliwymi programami i oszukańczymi wiadomościami.

- **Systemy operacyjne**

  Możesz wybrać następujące platformy:

  - Microsoft Windows
  - Linux
  - macOS
  - Android
  - Inne

  Informacje na temat obsługiwanych systemów operacyjnych można znaleźć na stronie Wymagania sprzętowe i programowe.

Możesz wybrać pakiety aplikacji Kaspersky z listy dostępnych pakietów później, niezależnie od kreatora wstępnej konfiguracji. Aby uprościć wyszukiwanie potrzebnych pakietów, możesz przefiltrować listę dostępnych pakietów według następujących kryteriów:

- Obszar ochronny
- Rodzaj pobranego oprogramowania (pakiet dystrybucyjny, narzędzie, wtyczka lub wtyczka sieciowa)
- Wersja aplikacji Kaspersky
- Język lokalizacji aplikacji Kaspersky

Krok 4. Wybieranie wtyczek dla zarządzanych aplikacji

Wybierz wtyczki dla zarządzanych aplikacji, które mają zostać zainstalowane. Zostanie wyświetlona lista wtyczek znajdujących się na serwerach Kaspersky. Lista jest filtrowana zgodnie z opcjami wybranymi w poprzednim kroku kreatora. Domyślnie, pełna lista zawiera wtyczki we wszystkich językach. Aby wyświetlić tylko wtyczkę w określonym języku, wybierz język z listy rozwijalnej **Wskaż język dla Konsoli administracyjnej lub**. Lista wtyczek zawiera następujące kolumny:

- **Nazwa aplikacji**

  Zostały wybrane wtyczki zależne od obszarów ochrony i platform, które wybrano w poprzednim kroku.

- **Wersja aplikacji**

  Lista zawiera wtyczki we wszystkich wersjach umieszczone na serwerach Kaspersky. Domyślnie zostaną wybrane wtyczki w najnowszych wersjach.

- **Wersja językowa**

  Domyślnie wersja językowa wtyczki jest definiowana przez wersję językową Kaspersky Security Center, którą wybrałeś w momencie instalacji. Możesz określić inne wersje językowe na liście rozwijalnej **Wskaż język dla Konsoli administracyjnej lub**.

Po wybraniu wtyczek ich instalacja rozpoczyna się automatycznie w oddzielnym oknie. Aby zainstalować niektóre wtyczki, należy zaakceptować warunki Umowy licencyjnej użytkownika końcowego. Zapoznaj się z treścią Umowy licencyjnej użytkownika końcowego, wybierz opcję **Akceptuję warunki Umowy licencyjnej** i kliknij przycisk **Zainstaluj**. Jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego, wtyczka nie zostanie zainstalowana.

Po zakończeniu instalacji, zamknij okno instalacji.

Wtyczki do zarządzania można również wybrać później, niezależnie od kreatora wstępnej konfiguracji.

Krok 5. Pobieranie pakietów dystrybucyjnych i tworzenie pakietów instalacyjnych

Kaspersky Endpoint Security for Windows zawiera narzędzia do szyfrowania informacji przechowywanych na urządzeniach klienckich. Aby pobrać pakiet dystrybucyjny Kaspersky Endpoint Security for Windows potrzebny w Twojej organizacji, miej na uwadze ustawodawstwo kraju, w którym znajdują się urządzenia klienckie Twojej organizacji.

W oknie **Typ szyfrowania** wybierz jeden z następujących typów szyfrowania:

- Strong encryption (Silne szyfrowanie) (AES256). Ten typ szyfrowania używa klucza o długości 256 bitów.
- Lite encryption (AES56) (Szyfrowanie podstawowe). Ten typ szyfrowania używa klucza o długości 56 bitów.

Okno **Typ szyfrowania** jest wyświetlane tylko wtedy, gdy jako obszar ochrony wybrałeś **Stacje robocze**, a jako platformę **Microsoft Windows.**

Po wybraniu typu szyfrowania, zostanie wyświetlona lista pakietów dystrybucyjnych obu typów szyfrowania. Pakiet dystrybucyjny z wybranym typem szyfrowania zostanie wybrany z listy. Język pakietu dystrybucyjnego odpowiada językowi Kaspersky Security Center. Jeśli wersja językowa pakietu dystrybucyjnego Kaspersky Endpoint Security for Windows dla Kaspersky Security Center nie istnieje, zostanie wybrana angielska wersja językowa pakietu dystrybucyjnego.

Na liście możesz wybrać wersje językowe pakietów dystrybucyjnych, korzystając z listy rozwijalnej **Wskaż język dla Konsoli administracyjnej lub**.

Dystrybutory zarządzanych aplikacji mogą wymagać zainstalowania określonej minimalnej wersji Kaspersky Security Center.

Na liście możesz wybrać pakiet dystrybucyjny dowolnego typu szyfrowania, inny od tego wybranego w oknie **Typ szyfrowania**. Po wybraniu pakietu dystrybucyjnego Kaspersky Endpoint Security for Windows, rozpocznie się pobieranie pakietów dystrybucyjnych odpowiadających komponentom i platformom. Możesz monitorować proces pobierania w kolumnie **Stan pobierania**. Po zakończeniu pracy Kreatora wstępnej konfiguracji, pakiety instalacyjne Agenta sieciowego dla systemu for Windows i zarządzanych aplikacji firmy Kaspersky są wyświetlane na liście **Serwer administracyjny → Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

Aby zakończyć pobieranie niektórych pakietów dystrybucyjnych, należy zaakceptować Umowę licencyjną użytkownika końcowego. Jeśli klikniesz przycisk **Zaakceptuj**, zostanie wyświetlona treść Umowy licencyjnej użytkownika końcowego. Aby przejść do kolejnego kroku kreatora, należy zaakceptować warunki i postanowienia Umowy licencyjnej użytkownika końcowego oraz warunki i postanowienia Polityki prywatności Kaspersky. Wybierz opcje dotyczące Umowy licencyjnej użytkownika końcowego i Polityki prywatności Kaspersky, a następnie kliknij przycisk **Zaakceptuj wszystkie**. Jeśli nie akceptujesz warunków i postanowień, pobieranie pakietu zostanie anulowane.

Po zaakceptowaniu warunków i postanowień Umowy licencyjnej użytkownika końcowego oraz warunków i postanowień Polityki prywatności Kaspersky, pobieranie pakietów dystrybucyjnych będzie kontynuowane. Jeśli pobieranie zostanie zakończone, zostanie wyświetlony stan **Utworzono pakiet instalacyjny**. W późniejszym czasie możesz wykorzystać pakiety instalacyjne do wdrożenia aplikacji Kaspersky na urządzeniach klienckich.

Pakiety instalacyjne można tworzyć ręcznie, niezależnie od kreatora wstępnej konfiguracji. Przejdź do **Serwer administracyjny** → **Zaawansowane** → **Zdalna instalacja** → **Pakiety instalacyjne** w drzewie Konsoli administracyjnej.

Krok 6. Konfigurowanie użycia Kaspersky Security Network

Możesz uzyskać dostęp do baz danych reputacji Kaspersky Security Network, aby zapewnić szybsze reakcje aplikacji Kaspersky na zagrożenia, poprawić skuteczność niektórych komponentów ochrony i zmniejszyć ryzyko fałszywych alarmów.

Przeczytaj Oświadczenie KSN, które zostanie wyświetlone w oknie. Określ ustawienia przekazywania informacji o działaniach Kaspersky Security Center do bazy wiedzy Kaspersky Security Network. Wybierz jedną z następujących opcji:

- **Zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje zainstalowane na urządzeniach klienckich automatycznie prześlą szczegóły swoich działań do Kaspersky Security Network. Uczestnictwo w Kaspersky Security Network umożliwia szybsze aktualizowanie baz danych zawierających informacje o wirusach i innych zagrożeniach, co zapewnia szybszą reakcję na pojawiające się zagrożenia bezpieczeństwa.

- **Nie zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje nie dostarczą informacji do Kaspersky Security Network.

  Jeśli wybierzesz tę opcję, korzystanie z Kaspersky Security Network zostanie wyłączone.

Jeśli pobrano wtyczkę Kaspersky Endpoint Security for Windows, wyświetlane są oba Oświadczenia KSN — Oświadczenie KSN dla Kaspersky Security Center oraz Oświadczenie KSN dla Kaspersky Endpoint Security for Windows. Oświadczenia KSN dla innych zarządzanych aplikacji firmy Kaspersky, których wtyczki zostały pobrane, są wyświetlane w oddzielnych oknach i każe oświadczenie powinno być zaakceptowane (lub nie) oddzielnie.

Możesz także skonfigurować dostęp Serwera administracyjnego do Kaspersky Security Network (KSN) później w oknie właściwości Serwera administracyjnego Konsoli administracyjnej.

Krok 7. Konfigurowanie powiadomień e-mail

Skonfiguruj wysyłanie powiadomień o zdarzeniach zarejestrowanych podczas działania aplikacji firmy Kaspersky na zarządzanych urządzeniach. Ustawienia te będą używane jako ustawienia domyślne dla Serwera administracyjnego.

W celu skonfigurowania dostarczania powiadomień o zdarzeniach występujących w aplikacjach firmy Kaspersky użyj następujących ustawień:

- **Adresaci (adresy e-mail)**

  Adresy e-mail użytkowników, którym aplikacja będzie wysyłała powiadomienia. Możesz wprowadzić jeden lub więcej adresów; jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami.

- **Serwer SMTP**

  Adres lub adresy serwerów pocztowych Twojej organizacji.

Jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
- Nazwa DNS serwera SMTP

- **Port serwera SMTP**

  Numer portu komunikacji serwera SMTP. Jeśli korzystasz z kilku serwerów SMTP, połączenie z nimi jest nawiązywane przez określony port komunikacyjny. Domyślny numer portu to 25.

- **Użyj uwierzytelniania ESMTP**

  Włącza obsługę autoryzacji ESMTP. Po zaznaczeniu opcji, w polach **Nazwa użytkownika** i **Hasło** możesz określić ustawienia autoryzacji ESMTP. Domyślnie pole to nie jest zaznaczone.

- **Ustawienia**

  Określ następujące ustawienia:

  - **Temat** (podmiot wiadomości e-mail)
  - **Adres e-mail nadawcy**
  - **Ustawienia TLS dla serwera SMTP**

  Możesz określić ustawienia TLS dla serwera SMTP:

  Możesz wyłączyć korzystanie z TLS, użyć TLS, jeśli serwer SMTP obsługuje ten protokół lub możesz wymusić użycie tylko TLS. Jeśli zdecydujesz się używać tylko TLS, określ certyfikat do uwierzytelniania serwera SMTP i wybierz, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Dodatkowo, jeśli wybierzesz używanie tylko TLS, możesz określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

  - Odszukaj plik certyfikatu serwera SMTP:

  Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

  - Odszukaj plik certyfikatu klienta:

  Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

  - Certyfikat X-509:

  Określ plik z certyfikatem oraz plik z kluczem prywatnym. Możesz przesyłać te pliki w dowolnej kolejności. Po przesłaniu obu plików podaj hasło do odszyfrowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

  - Kontener pkcs12:

  Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

Możesz przetestować nowe ustawienia powiadomień e-mail, klikając przycisk **Wyślij wiadomość testową**.

Powiadomienia o zdarzeniach można skonfigurować później, niezależnie od kreatora wstępnej konfiguracji.

Krok 8. Konfigurowanie zarządzania aktualizacją

Skonfiguruj ustawienia zarządzania uaktualnieniami aplikacji zainstalowanych na urządzeniach klienckich.

> Możesz skonfigurować te ustawienia tylko wtedy, gdy dostarczyłeś klucz licencyjny z opcją Zarządzanie lukami i poprawkami.

W grupie ustawień **Wyszukiwanie aktualizacji oraz ich instalacja** możesz wybrać tryb wyszukiwania i instalacji uaktualnień Kaspersky Security Center:

- **Wyszukaj wymagane aktualizacje**

  Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie, jeśli ich nie ma.

  Opcja ta jest wybrana domyślnie.

- **Wyszukaj i zainstaluj wymagane aktualizacje**

  Zadania *Wyszukiwanie luk i wymaganych aktualizacji* i *Zainstaluj wymagane aktualizacje i napraw luki* są tworzone automatycznie, jeśli ich nie ma.

W grupie ustawień **Windows Server Update Services** możesz wybrać źródło synchronizacji aktualizacji:

- **Użyj źródeł aktualizacji zdefiniowanych w zasadzie domeny**

  Urządzenia klienckie pobiorą aktualizacje Windows Update zgodnie z ustawieniami zasad domeny. Zasada Agenta sieciowego jest tworzona automatycznie, jeśli jeszcze jej nie masz.

- **Użyj Serwera administracyjnego jako serwera WSUS**

  Urządzenia klienckie pobiorą aktualizacje Windows Update z Serwera administracyjnego. Zadanie *Wykonaj synchronizację Windows Update* i zasada Agenta sieciowego są tworzone automatycznie, jeśli jeszcze ich nie masz.

Zadania *Wyszukiwanie luk i wymaganych aktualizacji* oraz *Zainstaluj wymagane aktualizacje i napraw luki* możesz utworzyć niezależnie od kreatora wstępnej konfiguracji. Aby użyć Serwera administracyjnego jako serwera WSUS, utwórz zadanie Wykonaj synchronizację *Windows Update* i wybierz opcję **Użyj Serwera administracyjnego jako serwera WSUS** jako serwera WSUS w zasadzie Agenta sieciowego.

Krok 9. Wstępne konfigurowanie ochrony

Okno **Konfiguracja wstępnej ochrony** wyświetla listę zasad i zadań, które są tworzone automatycznie. Tworzone są następujące zasady i zadania:

- Zasada Agenta sieciowego Kaspersky Security Center
- Zasady dla zarządzanych aplikacji firmy Kaspersky, których wtyczki zarządzające zostały zainstalowane wcześniej

- Zadanie Konserwacja Serwera administracyjnego
- Zadanie Kopia zapasowa danych Serwera administracyjnego
- Zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego
- Zadanie Wyszukiwanie luk i wymaganych aktualizacji
- Zadanie Zainstaluj aktualizację

Przed przystąpieniem do następnego kroku kreatora poczekaj na zakończenie tworzenia zasad i zadań.

Jeśli pobrałeś i zainstalowałeś wtyczkę dla Kaspersky Endpoint Security for Windows 10 Service Pack 1 i nowszej wersji, aż do wersji 11.0.1, podczas tworzenia zasad i zadań zostanie otwarte okno dla wstępnej konfiguracji strefy zaufanej Kaspersky Endpoint Security for Windows. Aplikacja poprosi o dodanie producentów, którzy zostali zweryfikowani przez Kaspersky, do strefy zaufanej w celu wykluczenia ich aplikacji ze skanowania, aby zapobiec ich przypadkowemu zablokowaniu. Możesz teraz utworzyć zalecane wykluczenia lub utworzyć listę wykluczeń w późniejszym czasie, wybierając następujące elementy w drzewie konsoli: **Zasady** → Menu właściwości Kaspersky Endpoint Security → **Zaawansowana ochrona przed zagrożeniami** → **Strefa zaufana** → **Ustawienia** → **Dodaj**. Lista wykluczeń ze skanowania jest dostępna do edycji w dowolnym momencie podczas korzystania z aplikacji.

Działania na strefie zaufanej są wykonywane przy użyciu narzędzi zintegrowanych z Kaspersky Endpoint Security for Windows. Szczegółowe instrukcje dotyczące wykonywania działań oraz opis funkcji szyfrowania są dostępne w internetowym systemie pomocy dla Kaspersky Endpoint Security for Windows.

W celu zakończenia wstępnej konfiguracji strefy zaufanej i powrotu do kreatora kliknij **OK**.

Kliknij **Dalej**. Ten przycisk jest dostępny po utworzeniu wszystkich niezbędnych zasad i zadań.

Wymagane zadania i zasady można również utworzyć później, niezależnie od kreatora wstępnej konfiguracji.

Krok 10. Podłączanie urządzeń mobilnych

Jeśli wcześniej włączono obszar ochrony **Urządzenia mobilne** w ustawieniach kreatora, określ ustawienia połączenia firmowych urządzeń mobilnych zarządzanej organizacji. Jeśli nie włączyłeś obszaru ochrony **Urządzenia mobilne**, ten krok jest pomijany.

W tym kroku kreatora należy wykonać następujące czynności:

- Skonfigurować porty dla połączenia urządzeń mobilnych
- Skonfigurować uwierzytelnianie Serwera administracyjnego
- Utworzyć lub zarządzać certyfikatami
- Skonfigurować wydawanie, automatyczne aktualizowanie i szyfrowanie certyfikatów ogólnego typu
- Utworzyć regułę przenoszenia dla urządzeń mobilnych

W celu ustawienia portów dla połączenia urządzeń mobilnych:

1. Kliknij przycisk **Konfiguruj** po prawej stronie pola **Połączenie urządzenia mobilnego**.
2. Z listy rozwijalnej wybierz **Konfiguruj porty**.

   Zostanie otwarte okno właściwości Serwera administracyjnego, wyświetlające sekcję **Porty dodatkowe**.
3. W sekcji **Porty dodatkowe** możesz określić ustawienia połączenia urządzenia mobilnego:

   - **Port SSL do aktywacji przy użyciu serwera proxy**

     Numer portu SSL do połączenia Kaspersky Endpoint Security for Windows z serwerami aktywacji Kaspersky.

     Domyślny numer portu to 17000.

   - **Otwórz port dla urządzeń mobilnych**

     Port zostaje otwarty dla urządzeń mobilnych do połączenia z serwerem licencjonowania. Możesz zdefiniować numer portu i inne ustawienia w polach poniżej.

     Domyślnie opcja ta jest włączona.

   - **Port do synchronizacji urządzeń mobilnych**

     Numer portu, za pomocą którego urządzenia mobilne będą łączyć się z Serwerem administracyjnym i będą wymieniać z nim dane. Domyślny numer portu to 13292.

     Jeśli port 13292 jest używany do innych celów, można przypisać inny port.

   - **Port do aktywacji urządzeń mobilnych**

     Port do łączenia Kaspersky Endpoint Security for Android z serwerami aktywacji Kaspersky.

     Domyślny numer portu to 17100.

   - **Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS**

     Urządzenia chronione UEFI mogą nawiązywać połączenie z Serwerem administracyjnym.

   - **Port dla urządzeń chronionych UEFI i urządzeń KasperskyOS**

     Możesz zmienić numer portu, jeśli opcja **Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS** jest włączona. Domyślny numer portu to 13294.

   - **Otwórz port dla Prometeusza**

     Port dla żądań ściągnięcia Prometheus. Domyślny numer portu to 13296.
4. Kliknij **OK**, aby zapisać zmiany i powrócić do kreatora wstępnej konfiguracji.

Musisz skonfigurować autoryzację Serwera administracyjnego przez urządzenia mobilne i autoryzację urządzeń mobilnych przez Serwer administracyjny. Jeśli chcesz, możesz skonfigurować autoryzację później, oddzielnie od kreatora wstępnej konfiguracji.

W celu skonfigurowania autoryzacji Serwera administracyjnego przez urządzenia mobilne:

1. Kliknij przycisk **Konfiguruj** po prawej stronie pola **Połączenie urządzenia mobilnego**.
2. Z listy rozwijalnej wybierz **Konfiguruj uwierzytelnianie**.

   Zostanie otwarte okno właściwości Serwera administracyjnego, wyświetlające sekcję **Certyfikaty**.

3. Wybierz opcję uwierzytelniania dla urządzeń mobilnych w grupie ustawień **Uwierzytelnianie Serwera administracyjnego przez urządzenia mobilne** i wybierz opcję uwierzytelniania dla urządzeń chronionych UEFI w grupie ustawień **Uwierzytelnianie Serwera administracyjnego przez urządzenia chronione UEFI**.

   Jeśli Serwer administracyjny wymienia dane z urządzeniami klienckimi, jest uwierzytelniany za pomocą certyfikatu.

   Domyślnie Serwer administracyjny używa certyfikatu, który został utworzony podczas instalacji Serwera administracyjnego. Jeśli chcesz, możesz dodać nowy certyfikat.

W celu dodania nowego certyfikatu (opcjonalnie):

1. Wybierz **Inny certyfikat**.

   Pojawi się przycisk **Przeglądaj**.

2. Kliknij przycisk **Przeglądaj**.

3. W otwartym oknie określ ustawienia certyfikatu:

   - **Typ certyfikatu**

     Z listy rozwijalnej możesz wybrać typ certyfikatu:

     - **Certyfikat X.509**. Jeśli ta opcja jest zaznaczona, powinieneś określić prywatny klucz certyfikatu oraz otworzyć certyfikat:

       - **Klucz prywatny (.prk, .pem)**. W tym polu kliknij przycisk **Przeglądaj**, aby określić prywatny klucz certyfikatu w formacie PKCS #8 (*.prk).

       - **Klucz publiczny (.cer)**. W tym polu kliknij przycisk **Przeglądaj**, aby określić publiczny klucz certyfikatu w formacie PEM (*.cer).

     - **Kontener PKCS #12**. Jeśli wybierzesz tę opcję, możesz określić plik certyfikatu w formacie P12 lub PFX, klikając przycisk **Przeglądaj** i uzupełniając pole **Plik certyfikatu**.

   - Czas aktywacji:

     - **Natychmiast**

       Po kliknięciu **OK**, bieżący certyfikat zostanie natychmiast zastąpiony nowym.

       Wcześniej podłączone urządzenia mobilne nie będą mogły nawiązać połączenia z Serwerem administracyjnym.

     - **Po wygaśnięciu tego okresu, dni**

       Jeśli wybierzesz tę opcję, zostanie wygenerowany certyfikat zapasowy. Bieżący certyfikat zostanie zastąpiony nowym w ciągu określonej liczby dni. Data obowiązywania certyfikatu zapasowego jest wyświetlona w sekcji **Certyfikaty**.

       Zalecane jest zaplanowanie ponownej publikacji w przyszłości. Certyfikat rezerwowy należy pobrać na urządzenia mobilne przed upływem określonego terminu. Po zastąpieniu bieżącego certyfikatu nowym, wcześniej podłączone urządzenia mobilne, na których nie ma zapasowego certyfikatu, nie będą mogły nawiązać połączenia z Serwerem administracyjnym.

4. Kliknij przycisk **Właściwości**, aby wyświetlić ustawienia wybranego certyfikatu Serwera administracyjnego.

W celu ponownego wydania certyfikatu poprzez Serwer administracyjny:

1. Wybierz **Certyfikat wydany przez Serwer administracyjny**.
2. Kliknij przycisk **Wydaj ponownie**.
3. W otwartym oknie określ następujące ustawienia:
   - Adres połączenia:
     - **Użyj poprzedniego adresu połączenia**

       Adres Serwera administracyjnego, z którym łączą się urządzenia mobilne, pozostają niezmienione.

       Opcja ta jest wybrana domyślnie.
     - **Zmień adres połączenia na**

       Jeśli chcesz, żeby urządzenia mobilne nawiązywały połączenie z innym adresem, w tym polu określ odpowiedni adres.

       Jeśli adres dla podłączania urządzeń mobilnych został zmieniony, należy wydać nowy certyfikat. Stary certyfikat staje się nieważny na wszystkich podłączonych urządzeniach mobilnych. Poprzednio podłączone urządzenia nie będą mogły nawiązać połączenia z Serwerem administracyjnym, więc staną się niezarządzane.
   - Czas aktywacji:
     - **Natychmiast**

       Po kliknięciu **OK**, bieżący certyfikat zostanie natychmiast zastąpiony nowym.

       Wcześniej podłączone urządzenia mobilne nie będą mogły nawiązać połączenia z Serwerem administracyjnym.
     - **Po wygaśnięciu tego okresu, dni**

       Jeśli wybierzesz tę opcję, zostanie wygenerowany certyfikat zapasowy. Bieżący certyfikat zostanie zastąpiony nowym w ciągu określonej liczby dni. Data obowiązywania certyfikatu zapasowego jest wyświetlona w sekcji **Certyfikaty**.

       Zalecane jest zaplanowanie ponownej publikacji w przyszłości. Certyfikat rezerwowy należy pobrać na urządzenia mobilne przed upływem określonego terminu. Po zastąpieniu bieżącego certyfikatu nowym, wcześniej podłączone urządzenia mobilne, na których nie ma zapasowego certyfikatu, nie będą mogły nawiązać połączenia z Serwerem administracyjnym.
4. Kliknij **OK**, aby zapisać zmiany i powrócić do okna **Certyfikaty**.
5. Kliknij **OK**, aby zapisać zmiany i powrócić do kreatora wstępnej konfiguracji.

W celu skonfigurowania wydawania, automatycznej aktualizacji i szyfrowania certyfikatów ogólnego typu dla identyfikacji urządzeń mobilnych przez Serwer administracyjny:

1. Kliknij przycisk **Konfiguruj** po prawej stronie pola **Autoryzacja urządzenia mobilnego**.

   Zostanie otwarte okno **Reguły wydawania certyfikatu** wyświetlające sekcję **Wydawanie certyfikatów dla urządzeń mobilnych**.

2. W razie potrzeby określ następujące ustawienia w sekcji **Ustawienia wydawania**:

   - **Okres ważności certyfikatu, dni**

     Okres ważności certyfikatu w dniach. Domyślny czas życia certyfikatu wynosi 365 dni. Po upływie tego okresu, urządzenie mobilne nie będzie mogło połączyć się z Serwerem administracyjnym.

   - **Źródło certyfikatu**

     Wybierz źródło certyfikatów ogólnego typu dla urządzeń mobilnych: certyfikaty są wydawane przez Serwer administracyjny lub są określane ręcznie.

     Szablony certyfikatów można zmodyfikować, jeśli integracja z infrastrukturą kluczy publicznych (PKI) została skonfigurowana w sekcji **Integracja z PKI**. W takim przypadku dostępne są następujące pola wyboru szablonu:

   - **Szablon domyślny**

     Użyj certyfikatu wystawionego przez zewnętrzne źródło certyfikatu - Centrum certyfikacji - pod domyślnym szablonem.

     Domyślnie opcja ta jest zaznaczona.

   - **Inny szablon**

     Wybierz szablon używany do wydawania certyfikatów. Możesz określić szablony certyfikatów w domenie. Przycisk **Odśwież listę** zaktualizuje listę szablonów certyfikatów.

3. Jeśli to konieczne, określ następujące ustawienia automatycznego wystawiania certyfikatów w sekcji **Ustawienia aktualizacji automatycznych**:

   - **Odnów, gdy certyfikat wygaśnie za (dni)**

     Liczba dni pozostałych do wygaśnięcia bieżącego certyfikatu, w trakcie których Serwer administracyjny powinien opublikować nowy certyfikat. Na przykład, jeśli wartość pola to 4, Serwer administracyjny opublikuje nowy certyfikat na cztery dni przed wygaśnięciem bieżącego certyfikatu. Domyślna wartość to 7.

   - **Odnów certyfikat automatycznie, jeśli jest to możliwe**

     Wybierz tę opcję, aby automatycznie ponownie wystawić certyfikat na liczbę dni określoną w polu **Odnów, gdy certyfikat wygaśnie za (dni)**. Jeśli certyfikat został zdefiniowany ręcznie, nie można go automatycznie odnowić, a włączona opcja nie będzie działać.

     Domyślnie opcja ta jest wyłączona.

   Certyfikaty są automatycznie ponownie publikowane przez Urząd certyfikacji.

4. Jeśli to konieczne, w sekcji ustawień **Ochrona hasłem** określ ustawienia do odszyfrowywania certyfikatów podczas instalacji.

   Wybierz opcję **Pytaj o hasło podczas instalowania certyfikatów**, aby zażądać hasła użytkownika, jeśli certyfikat jest zainstalowany na urządzeniu mobilnym. Hasło jest używane tylko raz, podczas instalacji certyfikatu na urządzeniu mobilnym.

   Hasło zostanie wygenerowane automatycznie przez Serwer administracyjny i wysłane na podany adres e-mail. Możesz podać adres e-mail użytkownika lub własny adres e-mail, jeśli chcesz użyć innej metody przekazywania hasła do użytkownika.

   Możesz użyć suwaka, aby określić liczbę znaków w haśle do odszyfrowywania certyfikatów.

Opcja wyświetlania hasła jest wymagana, na przykład, w celu ochrony certyfikatu współdzielonego w autonomicznym pakiecie instalacyjnym Kaspersky Endpoint Security for Android. Ochrona hasłem uniemożliwia intruzowi uzyskanie dostępu do certyfikatu współdzielonego poprzez kradzież autonomicznego pakietu instalacyjnego z Kaspersky Security Center Web Server.

Jeśli to pole jest wyłączone, certyfikat zostanie automatycznie odszyfrowany podczas instalacji, a użytkownik nie będzie pytany o hasło. Domyślnie opcja ta jest wyłączona.

5. Kliknij **OK**, aby zapisać zmiany i powrócić do okna kreatora wstępnej konfiguracji.

   Kliknij przycisk **Anuluj**, aby powrócić do kreatora wstępnej konfiguracji bez zapisywania jakichkolwiek zmian.

W celu włączenia funkcji przenoszenia urządzeń mobilnych do grupy administracyjnej, którą wybierzesz,

W polu **Automatyczne przenoszenie urządzeń mobilnych** wybierz opcję **Utwórz regułę przenoszenia dla urządzeń mobilnych**.

Jeśli opcja **Utwórz regułę przenoszenia dla urządzeń mobilnych** jest wybrana, aplikacja automatycznie tworzy regułę przenoszenia, która przenosi urządzenia działające pod systemem Android i iOS do grupy **Zarządzane urządzenia**:

- Z systemami operacyjnymi Android, na których zainstalowany jest Kaspersky Endpoint Security for Android oraz certyfikat dla urządzeń mobilnych
- Z systemami operacyjnymi iOS, na których zainstalowany jest profil iOS MDM oraz certyfikat współdzielony

Jeśli taka reguła już istnieje, aplikacja nie tworzy jej ponownie.

Domyślnie opcja ta jest wyłączona.

Kaspersky nie wspiera już Kaspersky Safe Browser.

Krok 11. Pobieranie aktualizacji

Aktualizacje antywirusowych baz danych dla Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky są pobierane automatycznie. Aktualizacje są pobierane z serwerów Kaspersky.

Aby pobierać aktualizacje niezależnie od kreatora wstępnej konfiguracji, utwórz i skonfiguruj zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

Krok 12. Wykrywanie urządzeń

Okno **Przeszukiwanie sieci** wyświetla informacje o stanie przeszukiwania sieci wykonywanym przez Serwer administracyjny.

Możesz wyświetlić urządzenia sieciowe wykryte przez Serwer administracyjny i uzyskać pomoc na temat pracy z oknem **Wykrywanie urządzeń**, klikając odnośniki w dolnej części okna.

Możesz wykonać przeszukiwanie sieci później, niezależnie od kreatora wstępnej konfiguracji. Użyj Konsoli administracyjnej, aby skonfigurować przeszukiwanie domen Windows, Active Directory, zakresów IP i sieci IPv6.

Krok 13. Zamykanie kreatora wstępnej konfiguracji

W oknie zakończenia pracy Kreatora wstępnej konfiguracji wybierz opcję **Tworzenie zadania zdalnej instalacji**, jeśli chcesz uruchomić automatyczną instalację aplikacji antywirusowych i/lub Agenta sieciowego na urządzeniach w sieci.

Aby zakończyć działanie kreatora, kliknij przycisk **Zakończ**.

Konfigurowanie połączenia Konsoli administracyjnej z Serwerem administracyjnym

Konsola administracyjna jest połączona z Serwerem administracyjnym poprzez port SSL TCP 13291. Ten sam port może być używany przez obiekty automatyzacji klakaut.

Port TCP o numerze 14000 może być używany do podłączania Konsoli administracyjnej, punktów dystrybucji, podrzędnych Serwerów administracyjnych i obiektów narzędzia klakaut, a także do pobierania danych z urządzeń klienckich.

Zazwyczaj port TCP o numerze 13000 dla protokołu SSL może być używany tylko przez Agenta sieciowego, podrzędny Serwer administracyjny i główny Serwer administracyjny w DMZ. W niektórych przypadkach konieczne może być podłączenie Konsoli administracyjnej za pośrednictwem portu SSL o numerze 13000:

- Jeśli pojedynczy port SSL będzie używany dla Konsoli administracyjnej i do innych działań (pobierania danych z urządzeń klienckich, podłączania punktów dystrybucji lub podłączania podrzędnych Serwerów administracyjnych).
- Jeśli obiekt narzędzia klakaut nie jest podłączany bezpośrednio do Serwera administracyjnego, ale za pośrednictwem punktu dystrybucji w DMZ.

W celu zezwolenia na łączenie Konsoli administracyjnej za pośrednictwem portu 13000:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).
2. Przejdź do gałęzi:
   - W systemach 32-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - W systemach 64-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Dla klucza LP_ConsoleMustUsePort13291 (DWORD) ustaw wartość 00000000.

   1 jest domyślną wartością określoną dla tego klucza.
4. Uruchom ponownie usługę Serwera administracyjnego.

Teraz możliwe będzie połączenie Konsoli administracyjnej z Serwerem administracyjnym za pośrednictwem portu 13000.

Konfigurowanie ustawień dostępu do Internetu dla Serwera administracyjnego

Należy skonfigurować dostęp do Internetu w taki sposób, aby korzystać z Kaspersky Security Network i pobierać aktualizacje antywirusowych baz danych dla Kaspersky Security Center i zarządzanych aplikacji Kaspersky.

Aby określić ustawienia dostępu do Internetu dla Serwera administracyjnego:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego przejdź do **Zaawansowane** → **Konfiguracja dostępu do internetu**.
4. Wybierz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest wybrana, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

   - **Adres**

     Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

   - **Numer portu**

     Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

   - **Pomiń serwer proxy dla adresów lokalnych**

     Żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

   - **Uwierzytelnianie na serwerze proxy**

     Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

     To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

   - **Nazwa użytkownika**

     Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

   - **Hasło**

     Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

     Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

Dostęp do Internetu można również skonfigurować za pomocą kreatora wstępnej konfiguracji.

Podłączanie urządzeń mobilnych

Ta sekcja opisuje sposób podłączania zarządzanych urządzeń mobilnych (czyli zarządzanych urządzeń znajdujących się poza siecią główną) z Serwerem administracyjnym.

Scenariusz: Podłączanie urządzeń mobilnych przez bramę połączenia

W tym scenariuszu opisano sposób podłączania zarządzanych urządzeń znajdujących się poza siecią główną z Serwerem administracyjnym.

Wymagania wstępne

Scenariusz ma następujące wymagania wstępne:

- Strefa zdemilitaryzowana (DMZ) jest zorganizowana w sieci Twojej organizacji.
- Serwer administracyjny Kaspersky Security Center jest zainstalowany w sieci firmowej.

Etapy

Ten scenariusz przebiega etapami:

1. **Wybieranie urządzenia kliencka w DMZ**

   To urządzenie zostanie użyte jako brama połączenia. Urządzenie, które wybrałeś, musi spełniać wymagania dla bram połączenia.

2. **Instalowanie Agenta sieciowego w roli bramy połączenia**

   Do zainstalowania Agenta sieciowego na wybranym urządzeniu zalecane jest używanie instalacji lokalnej.

   Domyślnie plik instalacyjny znajduje się w następującym miejscu: \\<nazwa serwera>\KLSHARE\PkgInst\NetAgent_<numer wersji>

   W oknie **Brama połączenia** kreatora instalacji Agenta sieciowego wybierz **Użyj Agenta sieciowego jako bramy połączenia w DMZ**. Ten tryb jednocześnie aktywuje rolę bramy połączenia i nakazuje Agentowi sieciowemu czekać na połączenia z Serwera administracyjnego zamiast nawiązywać połączenia z Serwerem administracyjnym.

   Alternatywnie możesz zainstalować Agenta sieciowego na urządzeniu z systemem Linux i skonfigurować Agenta sieciowego do pracy jako brama połączenia, ale zwróć uwagę na listę ograniczeń Agenta sieciowego działającego na urządzeniach z systemem Linux.

3 Zezwalanie na połączenia w zaporach sieciowych w bramie połączenia

Aby upewnić się, że Serwer administracyjny może faktycznie połączyć się z bramą połączenia w strefie DMZ, zezwolić na połączenia z portem TCP o numerze 13000 we wszystkich zaporach ogniowych między Serwerem administracyjnym a bramą połączenia.

Jeśli brama połączenia nie ma rzeczywistego adresu IP w Internecie, ale zamiast tego znajduje się poza NAT (Network Address Translation — translacja adresów sieciowych), skonfiguruj regułę, aby przekazywać połączenia przez NAT.

4 Tworzenie grupy administracyjnej dla urządzeń zewnętrznych

Utwórz nową grupę w grupie **Zarządzane urządzenia**. Ta nowa grupa będzie zawierała zewnętrzne zarządzane urządzenia.

5 Podłączanie bramy połączenia do Serwera administracyjnego

Brama połączenia, którą skonfigurowałeś, oczekuje na połączenie z Serwera administracyjnego. Jednakże Serwer administracyjny nie wyświetla urządzenia z bramą połączenia wśród zarządzanych urządzeń. Dzieje się tak ponieważ brama połączenia nie próbowała nawiązać połączenia z Serwerem administracyjnym. Dlatego też należy przeprowadzić specjalną procedurę w celu zapewnienia, że Serwer administracyjny zainicjuje połączenie z bramą połączenia.

Wykonaj następujące czynności:

1. Dodaj bramę połączenia jako punkt dystrybucji.
2. Przenieś bramę połączenia z grupy **Nieprzypisane urządzenia** do grupy utworzonej dla urządzeń zewnętrznych.

Brama połączenia została podłączona i skonfigurowana.

6 Podłączanie zewnętrznych urządzeń stacjonarnych do Serwera administracyjnego

Zwykle zewnętrzne komputery stacjonarne nie są przenoszone wewnątrz granic. Dlatego musisz skonfigurować je tak, aby łączyły się z Serwerem administracyjnym przez bramę podczas instalowania Agenta sieciowego.

7 Konfigurowanie aktualizacji dla zewnętrznych urządzeń stacjonarnych

Jeśli aktualizacje aplikacji zabezpieczających są skonfigurowane do pobierania z Serwera administracyjnego, urządzenia zewnętrzne pobierają aktualizacje przez bramę połączenia. Ma to dwie wady:

- To niepotrzebny ruch, który zajmuje przepustowość kanału komunikacji internetowej firmy.
- Niekoniecznie jest to najszybszy sposób uzyskiwania aktualizacji. Jest bardzo prawdopodobne, że pobieranie aktualizacji z serwerów aktualizacji Kaspersky byłoby tańsze i szybsze dla urządzeń zewnętrznych.

Wykonaj następujące czynności:

1. Przenieś wszystkie urządzenia zewnętrzne do oddzielnej grupy administracyjnej, którą utworzyłeś wcześniej.
2. Wyklucz grupę z urządzeniami zewnętrznymi z zadania aktualizacji.
3. Utwórz osobne zadanie aktualizacji dla grupy z urządzeniami zewnętrznymi.

8. **Podłączanie przenośnych laptopów do Serwera administracyjnego**

   Przenośne laptopy są czasami w sieci, a czasami poza nią. W celu efektywnego zarządzania należy połączyć je z Serwerem administracyjnym w różny sposób w zależności od ich lokalizacji. Aby efektywnie wykorzystywać ruch sieciowy, muszą również pobierać uaktualnienia z różnych źródeł w zależności od ich lokalizacji.

   Należy skonfigurować reguły dla użytkowników mobilnych: profile połączeń i opisy lokalizacji sieciowych. Każda reguła definiuje instancję Serwera administracyjnego, z którym muszą łączyć się przenośne laptopy w zależności od ich lokalizacji oraz instancji Serwera administracyjnego, z którego muszą pobierać aktualizacje.

Scenariusz: Połączanie urządzeń spoza biura poprzez podrzędny Serwer administracyjny w strefie DMZ

Jeśli chcesz podłączyć urządzenia zarządzane, które znajdują się poza główną siecią, do Serwera administracyjnego, można to zrobić za pomocą podrzędnego Serwera administracyjnego znajdującego się w strefie zdemilitaryzowanej (DMZ).

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- DMZ jest organizowana w sieci Twojej organizacji.
- Serwer administracyjny Kaspersky Security Center jest zlokalizowany w wewnętrznej sieci organizacji.

Etapy

Ten scenariusz przebiega etapami:

1. **Wybieranie urządzenia kliencka w DMZ**

   W DMZ wybierz urządzenie klienckie, które będzie używane jako podrzędny Serwer administracyjny.

2. **Instalowanie Serwera administracyjnego Kaspersky Security Center**

   Zainstaluj Serwer administracyjny Kaspersky Security Center na tym urządzeniu klienckim.

3. **Tworzenie hierarchii Serwerów administracyjnych**

   W przypadku umieszczenia podrzędnego Serwera administracyjnego w strefie DMZ, podrzędny Serwer administracyjny musi uzyskiwać połączenie z głównego Serwera administracyjnego. W tym celu należy dodać nowy Serwer administracyjny jako serwer podrzędny, tak, aby główny Serwer administracyjny łączył się z podrzędnym Serwerem administracyjnym poprzez port 13000. Podczas łączenia dwóch Serwerów administracyjnych w ramach hierarchii upewnij się, że port 13291 jest dostępny na obu Serwerach administracyjnych. Konsola administracyjna nawiązuje połączenie z Serwerem administracyjnym poprzez port 13291.

4. **Połączanie mobilnych urządzeń zarządzanych do podrzędnego Serwera administracyjnego**

   Urządzenia mobilne można połączyć z Serwerem administracyjnym w strefie DMZ w taki sam sposób, w jaki nawiązywane jest połączenie pomiędzy Serwerem administracyjnym i urządzeniami zarządzanymi zlokalizowanymi w sieci głównej. Mobilne urządzenia zarządzane inicjują połączenie poprzez port 13000.

Informacje o podłączaniu urządzeń mobilnych

Niektóre zarządzane urządzenia zawsze znajdują się poza główną siecią (na przykład, urządzenia w oddziałach regionalnych firmy; kioski, bankomaty i terminale zainstalowane w różnych punktach sprzedaży; urządzenia w domowych biurach pracowników). Niektóre urządzenia od czasu do czasu wyjeżdżają poza granicę (na przykład, laptopy użytkowników, którzy odwiedzają oddziały regionalne lub biuro klienta).

Nadal musisz monitorować i zarządzać ochroną urządzeń znajdujących się poza biurem - otrzymywać aktualne informacje o ich stanie ochrony i zapewniać aktualność aplikacji zabezpieczających. Jest to konieczne, ponieważ, na przykład, jeśli do takiego urządzenia ktoś się włamał, gdy znajdowało się poza siecią główną, może stać się platformą do rozprzestrzeniania zagrożeń, gdy tylko połączy się z siecią główną. W celu podłączenia urządzeń mobilnych do Serwera administracyjnego, możesz użyć dwóch metod:

- Brama połączenia w strefie zdemilitaryzowanej (DMZ)

  Zobacz schemat transmisji danych: Serwer administracyjny w sieci LAN, zarządzane urządzenia w internecie, używana brama połączenia

- Serwer administracyjny w strefie DMZ

  Zobacz schemat transmisji danych: Serwer administracyjny w strefie DMZ, zarządzane urządzenia w internecie

Brama połączenia w strefie DMZ

Zalecaną metodą podłączania urządzeń mobilnych do Serwera administracyjnego jest zorganizowanie strefy DMZ w sieci organizacji i zainstalowanie bramy połączenia w strefie DMZ. Urządzenia zewnętrzne nawiążą połączenie z bramą połączenia, a Serwer administracyjny znajdujący się w sieci zainicjuje połączenie z urządzeniami za pośrednictwem bramy połączenia.

W porównaniu z drugą metodą ta jest bezpieczniejsza:

- Nie musisz otwierać dostępu do Serwera administracyjnego spoza sieci.
- Uszkodzona brama połączenia nie stwarza dużego zagrożenia dla bezpieczeństwa urządzeń sieciowych. Brama połączeń w rzeczywistości sama niczym nie zarządza i nie ustanawia żadnych połączeń.

Ponadto brama połączeń nie wymaga wielu zasobów sprzętowych.

Jednakże ta metoda ma bardziej skomplikowany proces konfiguracji:

- Aby urządzenie służyło jako brama połączenia w DMZ, musisz zainstalować Agenta sieciowego i podłączyć go do Serwera administracyjnego w określony sposób.
- Nie będziesz mógł używać tego samego adresu do łączenia się z Serwerem administracyjnym we wszystkich sytuacjach. Poza granicami, będziesz musiał użyć nie tylko innego adresu (adresu bramy połączenia), ale także innego trybu połączenia: przez bramę połączenia.
- Musisz także zdefiniować różne ustawienia połączeń dla laptopów w różnych lokalizacjach.

Aby dodać bramę połączenia do wcześniej skonfigurowanej sieci:

1. Zainstaluj Agenta sieciowego w trybie bramy połączenia.

2. Ponownie zainstaluj Agenta sieciowego na urządzeniach, które chcesz połączyć z nowo dodaną bramą połączenia.

Serwer administracyjny w strefie DMZ

Inną metodą jest zainstalowanie pojedynczego Serwera administracyjnego w strefie DMZ.

Ta konfiguracja jest mniej bezpieczna niż inna metoda. Aby w tym przypadku zarządzać zewnętrznymi laptopami, Serwer administracyjny musi akceptować połączenia z dowolnego adresu w Internecie. Nadal będzie zarządzać wszystkimi urządzeniami w sieci wewnętrznej, ale z DMZ. Dlatego przejęty Serwer może spowodować ogromne szkody, pomimo niskiego prawdopodobieństwa takiego zdarzenia.

Ryzyko jest znacznie niższe, jeśli Serwer administracyjny w DMZ nie zarządza urządzeniami w sieci wewnętrznej. Taka konfiguracja może być wykorzystana, na przykład, przez usługodawcę do zarządzania urządzeniami klientów.

Możesz chcieć użyć tej metody w następujących przypadkach:

- Jeśli jesteś zaznajomiony z instalacją i konfiguracją Serwera administracyjnego i nie chcesz wykonywać innej procedury instalacji i konfiguracji bramy połączenia.

- Jeśli potrzebujesz zarządzać większą liczbą urządzeń. Maksymalna pojemność Serwera administracyjnego to 100 000 urządzeń, podczas gdy brama połączenia może obsługiwać do 10 000 urządzeń.

To rozwiązanie ma również możliwe trudności:

- Serwer administracyjny wymaga większej ilości zasobów sprzętowych i jeszcze jednej bazy danych.

- Informacje o urządzeniach będą przechowywane w dwóch niepowiązanych bazach danych (dla Serwera administracyjnego w sieci i jednej w DMZ), co komplikuje monitorowanie.

- Aby zarządzać wszystkimi urządzeniami, Serwer administracyjny musi być połączony w hierarchię, co komplikuje nie tylko monitorowanie, ale także zarządzanie. Instancja podrzędnego Serwera administracyjnego nakłada ograniczenia na możliwe struktury grup administracyjnych. Musisz zdecydować, w jaki sposób i które zadania i zasady mają być dystrybuowane do instancji podrzędnego Serwera administracyjnego.

- Skonfigurowanie urządzeń zewnętrznych do używania Serwera administracyjnego w DMZ z zewnątrz oraz do używania głównego Serwera administracyjnego od wewnątrz nie jest prostsze niż zwykłe skonfigurowanie ich tak, aby używały warunkowego połączenia przez bramę.

- Wysokie zagrożenia bezpieczeństwa. Zagrożona instancja Serwera administracyjnego ułatwia włamanie się do zarządzanych laptopów. Jeśli tak się stanie, hakerzy muszą tylko poczekać, aż jeden z laptopów wróci do sieci firmowej, aby mogli kontynuować atak na sieć lokalną.

Podłączanie zewnętrznych urządzeń stacjonarnych do Serwera administracyjnego

Urządzenia stacjonarne, które zawsze znajdują się poza główną siecią (na przykład, urządzenia w oddziałach regionalnych firmy; kioski, bankomaty i terminale zainstalowane w różnych punktach sprzedaży; urządzenia w domowych biurach pracowników) nie mogą być podłączane bezpośrednio do Serwera administracyjnego. Muszą być podłączeni do Serwera administracyjnego przez bramę połączenia zainstalowaną w strefie zdemilitaryzowanej (DMZ). Ta konfiguracja jest wykonywana podczas instalacji Agenta sieciowego na tych urządzeniach.

W celu podłączenia zewnętrznych urządzeń stacjonarnych do Serwera administracyjnego:

1. Utwórz nowy pakiet instalacyjny dla Agenta sieciowego.
2. Otwórz właściwości utworzonego pakietu instalacyjnego i przejdź do sekcji **Zaawansowane**, a następnie wybierz opcję **Połącz z Serwerem administracyjnym korzystając z bramy połączenia**.

   Ustawienie **Połącz z Serwerem administracyjnym korzystając z bramy połączenia** jest niekompatybilne z ustawieniem **Użyj Agenta sieciowego jako bramy połączenia w DMZ**. Nie możesz włączyć obu tych ustawień jednocześnie.

3. W sekcji **Adres bramy połączenia** określ publiczny adres bramy połączenia.

   Jeśli brama połączenia znajduje się za translacją adresów sieciowych (NAT) i nie ma własnego adresu publicznego, skonfiguruj regułę bramy NAT w celu przekazywania połączeń z adresu publicznego na adres wewnętrzny bramy połączenia.

4. Utwórz autonomiczny pakiet instalacyjny w oparciu o utworzony pakiet instalacyjny.
5. Dostarcz autonomiczny pakiet instalacyjny na docelowe urządzenia, elektronicznie lub na dysku wymiennym.
6. Zainstaluj Agenta sieciowego z pakietu autonomicznego.

Zewnętrzne urządzenia stacjonarne są połączone z Serwerem administracyjnym.

Informacje o profilach połączenia dla użytkowników mobilnych

Mobilni użytkownicy laptopów (zwanych dalej również "urządzeniami") mogą potrzebować zmiany metody łączenia się z Serwerem administracyjnym lub przełączania pomiędzy Serwerami administracyjnymi w zależności od aktualnej lokalizacji urządzenia w sieci firmowej.

Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows i macOS.

Używanie różnych adresów jednego Serwera administracyjnego

Urządzenia z zainstalowanym Agentem sieciowym mogą łączyć się z Serwerem administracyjnym z poziomu wewnętrznej sieci organizacji lub internetu. W tej sytuacji wymagane może być, aby Agent sieciowy używał innych adresów do łączenia się z Serwerem administracyjnym: zewnętrznego adresu Serwera administracyjnego dla połączenia internetowego oraz wewnętrznego adresu Serwera administracyjnego dla wewnętrznego połączenia sieciowego.

W tym celu musisz dodać profil (dla połączenia z Serwerem administracyjnym z poziomu internetu) do zasady Agenta sieciowego. Dodaj profil we właściwościach zasady (sekcja **Łączność**, podsekcja **Profile połączenia**). W oknie tworzenia profilu należy wyłączyć opcję **Użyj tylko do pobierania uaktualnień** oraz wybrać opcję **Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu**. Jeśli do łączenia się z Serwerem administracyjnym używasz bramy połączenia (na przykład, w konfiguracji Kaspersky Security Center, opisanej w sekcji Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej), w odpowiednim polu profilu połączenia musisz określić adres bramy połączenia.

Przełączanie pomiędzy Serwerami administracyjnymi w zależności od aktualnej sieci

Jeśli organizacja posiada kilka biur z różnymi Serwerami administracyjnymi, a niektóre urządzenia z zainstalowanym Agentem sieciowym są przenoszone pomiędzy nimi, Agent sieciowy musi łączyć się z Serwerem administracyjnym sieci lokalnej w biurze, w którym znajduje się urządzenie.

W tej sytuacji konieczne jest utworzenie profilu dla połączenia z Serwerem administracyjnym we właściwościach zasady Agenta sieciowego dla każdego z biur, za wyjątkiem głównego biura, w którym znajduje się oryginalny macierzysty Serwer administracyjny. W profilach połączenia należy określić adresy Serwerów administracyjnych i włączyć lub wyłączyć opcję **Użyj tylko do pobierania uaktualnień**:

- Wybierz tę opcję, jeśli chcesz, aby Agent sieciowy zsynchronizował się z macierzystym Serwerem administracyjnym, a Serwer lokalny był używany tylko do pobierania uaktualnień.
- Wyłącz tę opcję, jeśli Agent sieciowy ma być całkowicie zarządzany przez lokalny Serwer administracyjny.

Następnie powinieneś ustalić warunki przełączania do nowo utworzonych profili: przynajmniej jeden warunek dla każdego z biur, za wyjątkiem głównego biura. Celem każdego warunku jest wykrycie elementów, które są specyficzne dla środowiska sieciowego w biurze. Jeśli warunek jest prawdziwy, odpowiedni profil zostaje aktywowany. Jeśli żaden z warunków nie jest prawdziwy, Agent sieciowy przełączy się do macierzystego Serwera administracyjnego.

Tworzenie profilu połączenia dla użytkowników mobilnych

Profil połączenia serwera administracyjnego jest dostępny tylko na urządzeniach działających pod kontrolą systemu Windows i macOS.

W celu utworzenia profilu połączenia Agenta sieciowego z Serwerem administracyjnym dla użytkowników mobilnych:

1. W drzewie konsoli wybierz grupę administracyjną zawierającą urządzenia klienckie, dla których chcesz utworzyć profil połączenia Agenta sieciowego z Serwerem administracyjnym.

2. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz utworzyć profil połączenia dla wszystkich urządzeń w grupie, w obszarze roboczym grupy, na zakładce **Zasady** wybierz zasadę Agenta sieciowego. Otwórz okno właściwości wybranej zasadę.

   - Jeśli chcesz utworzyć profil dla urządzenia w grupie, w obszarze roboczym grupy, na zakładce **Urządzenia** wybierz urządzenie i wykonaj następujące czynności:

     a. Otwórz okno właściwości wybranego urządzenia.

     b. W sekcji **Aplikacje** okna właściwości urządzenia wybierz Agenta sieciowego.

     c. Otwórz okno właściwości Agenta sieciowego.

3. W oknie właściwości, w sekcji **Łączność** wybierz podsekcję **Profile połączenia**.

4. W grupie ustawień **Profile połączeń Serwera administracyjnego** kliknij przycisk **Dodaj**.

   Domyślnie, lista profili połączeń zawiera profile <Tryb offline> i <Macierzysty serwer administracyjny>. Profili nie można modyfikować ani usunąć.

   Profil <Tryb offline> nie określa żadnego Serwera do nawiązania połączenia. Dlatego też, agent sieciowy, gdy zostaje przełączony do tego profilu, nie próbuje nawiązać połączenia z żadnym serwerem administracyjnym, gdy aplikacje zainstalowane na urządzeniach klienckich działają pod kontrolą zasad użytkownika mobilnego. Profil <Tryb offline> może być używany, jeśli urządzenia są odłączone od sieci.

   Profil <Macierzysty serwer administracyjny> dotyczy połączenia z serwerem administracyjnym, który został wybrany podczas instalacji agenta sieciowego. Profil <Macierzysty serwer administracyjny> jest stosowany, gdy urządzenie jest ponownie podłączane do macierzystego Serwera administracyjnego po tym, jak przez jakiś czas działało w sieci zewnętrznej.

5. W otwartym oknie **Nowy profil** skonfiguruj profil połączenia:

   - **Nazwa profilu**

     W tym polu możesz przejrzeć lub zmienić nazwę profilu połączenia.

   - **Serwer administracyjny**

     Adres Serwera administracyjnego, z którym urządzenie klienckie musi łączyć się podczas aktywacji profilu.

   - **Port**

     Numer portu używanego do nawiązywania połączenia.

   - **Port SSL**

     Numer portu połączenia podczas używania portu SSL.

   - **Użyj SSL**

     Jeśli ta opcja jest włączona, połączenie jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

Domyślnie opcja ta jest włączona. Zalecamy, aby nie wyłączać tej opcji, aby Twoje połączenie pozostało bezpieczne.

- Kliknij odnośnik **Konfiguruj połączenie poprzez serwer proxy**, aby skonfigurować połączenie poprzez serwer proxy. Wybierz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest wybrana, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

  - **Adres serwera proxy**

    Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

  - **Numer portu**

    Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

  - **Uwierzytelnianie na serwerze proxy**

    Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

    To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

  - **Nazwa użytkownika** (to pole jest dostępne, jeśli opcja **Uwierzytelnianie na serwerze proxy** jest zaznaczona)

    Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

  - **Hasło** (to pole jest dostępne, jeśli została wybrana opcja **Uwierzytelnianie na serwerze proxy**)

    Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

    Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

- **Ustawienia bramy połączenia**

  Adres bramy, poprzez którą urządzenia klienckie łączą się z Serwerem administracyjnym.

- **Włącz tryb użytkownika mobilnego**

  Jeśli ta opcja jest włączona, w przypadku połączenia przez ten profil, aplikacje zainstalowane na urządzeniu klienckim będą używać profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

  Jeżeli ta opcja jest wyłączona, aplikacje będą używać zasad aktywnych.

  Domyślnie opcja ta jest wyłączona.

- **Użyj tylko do pobierania uaktualnień**

  Jeżeli ta opcja jest włączona, profil będzie używany tylko do pobierania aktualizacji przez aplikacje zainstalowane na urządzeniu klienckim. Dla innych działań połączenie z Serwerem administracyjnym będzie nawiązywane z użyciem wstępnych ustawień określonych podczas instalacji Agenta sieciowego.

  Domyślnie opcja ta jest włączona.

- **Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu**

  Jeśli ta opcja jest włączona, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym przy użyciu ustawień określonych we właściwościach profilu.

  Jeśli ta opcja jest wyłączona, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym przy użyciu oryginalnych ustawień określonych podczas instalacji.

  Ta opcja jest dostępna, jeśli opcja **Użyj tylko do pobierania aktualizacji** jest wyłączona.

  Domyślnie opcja ta jest wyłączona.

6. Zaznacz opcję **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny**, aby zezwolić aplikacjom zainstalowanym na urządzeniu klienckim na korzystanie z profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego, za każdym razem, gdy Serwer administracyjny nie jest dostępny. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

Profil połączenia Agenta sieciowego z Serwerem administracyjnym zostanie utworzony dla użytkowników mobilnych. Jeśli agent sieciowy łączy się z serwerem administracyjnym przy użyciu tego profilu, aplikacje zainstalowane na urządzeniu klienckim będą używać zasad dla urządzeń w trybie użytkownika mobilnego lub zasad użytkownika mobilnego.

Informacje o przełączaniu Agenta sieciowego na inne Serwery administracyjne

Początkowe ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym są definiowane podczas instalacji Agenta sieciowego. Aby przełączać Agenta sieciowego na inne Serwery administracyjne, można skorzystać z reguł przełączania. Ta funkcja jest obsługiwana tylko w przypadku agentów sieciowych zainstalowanych na urządzeniach z systemem Windows lub macOS.

Reguły przełączania mogą być uruchamiane przy zmianie następujących parametrów sieci:

- Domyślny adres bramy.
- Adres IP serwera protokołu dynamicznej konfiguracji hosta (DHCP).
- Sufiks DNS podsieci.
- Adres IP sieciowego serwera DNS.
- Dostępność domeny Windows. Ten parametr jest dostępny tylko dla urządzeń z systemem Windows.
- Adres i maska podsieci.
- Adres IP sieciowego serwera WINS. Ten parametr jest dostępny tylko dla urządzeń z systemem Windows.
- Nazwa DNS lub NetBIOS urządzenia klienckiego.
- Dostępność adresu połączenia SSL.

Jeśli reguły przełączania Agenta sieciowego na inne Serwery administracyjne zostały zmienione, Agent sieciowy odpowiada na zmiany w parametrach sieci w następujący sposób:

- Jeśli ustawienia sieci pokrywają się z ustawieniami jednej z utworzonych reguł, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym określonym w tej regule. Aplikacje zainstalowane na urządzeniach klienckich przełączają się do zasady użytkownika mobilnego pod warunkiem, że takie zachowanie jest dozwolone przez regułę.
- Jeśli nie jest stosowana żadna z reguł, Agent sieciowy przywróci ustawienia domyślne połączenia z Serwerem administracyjnym określone podczas instalacji. Aplikacje zainstalowane na urządzeniach klienckich przywracają aktywne zasady.
- Jeśli Serwer administracyjny jest niedostępny, Agent sieciowy używa zasad użytkownika mobilnego.

Agent sieciowy przełącza się do zasady użytkownika mobilnego tylko wtedy, gdy opcja **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny** jest włączona w ustawieniach zasady Agenta sieciowego.

Ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym są zapisywane w profilu połączenia. W profilu połączenia możesz utworzyć reguły przełączania urządzeń klienckich do zasad użytkownika mobilnego, a także skonfigurować profil tak, aby mógł być używany tylko do pobierania uaktualnień.

Tworzenie reguły przełączania Agenta sieciowego według lokalizacji sieciowej

Przełączanie agenta sieciowego według lokalizacji sieciowej jest dostępne tylko na urządzeniach działających pod kontrolą systemu Windows i macOS.

W celu utworzenia reguły przełączania Agenta sieciowego z jednego z Serwera administracyjnego na inny w przypadkui zmiany ustawień sieciowych:

1. W drzewie konsoli należy wybrać grupę administracyjną zawierającą urządzenia, dla których ma zostać utworzona reguła przełączania Agenta sieciowego według opisu lokalizacji sieciowej.
2. Wykonaj jedną z poniższych czynności:
   - Jeśli chcesz utworzyć regułę dla wszystkich urządzeń w grupie, w obszarze roboczym grupy, na zakładce **Zasady** wybierz zasadę Agenta sieciowego. Otwórz okno właściwości wybranej zasadę.
   - Jeśli chcesz utworzyć regułę dla urządzenia wybranego w grupie, w obszarze roboczym grupy, na zakładce **Urządzenia** wybierz urządzenie i wykonaj następujące czynności:
     a. Otwórz okno właściwości wybranego urządzenia.
     b. W sekcji **Aplikacje** okna właściwości urządzenia wybierz Agenta sieciowego.
     c. Otwórz okno właściwości Agenta sieciowego.
3. W otwartym oknie **Właściwości**, w sekcji **Łączność** wybierz podsekcję **Profile połączenia**.
4. W sekcji **Ustawienia lokalizacji sieciowej** kliknij przycisk **Dodaj**.

5. W otwartym oknie **Nowy opis** skonfiguruj opis lokalizacji sieciowej i regułę przełączania. Określ następujące ustawienia opisu lokalizacji sieciowej:

   - **Nazwa opisu lokalizacji sieciowej**

     Nazwa opisu lokalizacji sieciowej nie może być dłuższa niż 255 znaków i nie może zawierać znaków specjalnych, takich jak ("*<>?\/:|).

   - **Użyj profilu połączenia**

     Na liście rozwijalnej możesz określić profil połączenia, którego Agent sieciowy używa do nawiązania połączenia z Serwerem administracyjnym. Ten profil będzie używany, jeśli spełnione są warunki opisu lokalizacji sieciowej. Profil połączenia zawiera ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym i definiuje, kiedy urządzenia klienckie muszą przełączyć się do zasad użytkownika mobilnego. Profil jest używany tylko do pobierania uaktualnień.

6. W sekcji **Warunki przełączenia** kliknij przycisk **Dodaj**, aby utworzyć listę warunków opisu lokalizacji sieciowej.

   Warunki w regule są połączone przy użyciu operatora logicznego I. Aby wyzwolić regułę przełączania według opisu lokalizacji sieciowej, muszą być spełnione wszystkie warunki przełączania reguły.

7. Z listy rozwijalnej wybierz wartość odpowiadającą zmianie charakterystyki sieci, do której podłączone jest urządzenie klienckie:

   - **Adres domyślnej bramy połączenia** — zmiana adresu głównej bramy sieci.
   - **Adres serwera DHCP** — zmiana adresu IP serwera sieciowego (DHCP).
   - **Domena DNS** — zmiana sufiksu DNS podsieci.
   - **Adres serwera DNS** — zmiana adresu IP serwera DNS.
   - **Dostępność domeny Windows (tylko w systemie Windows)** – zmiana stanu domeny Windows, do której podłączone jest urządzenie klienckie. Użyj tego ustawienia tylko w przypadku urządzeń z systemem Windows.
   - **Podsieć** – zmiana adresu i maski podsieci.
   - **Adres serwera WINS (tylko w systemie Windows)** — adres IP sieciowego serwera WINS został zmieniony. Użyj tego ustawienia tylko w przypadku urządzeń z systemem Windows.
   - **Możliwość rozwiązywania nazw** — nazwa DNS lub NetBIOS urządzenia klienckiego uległa zmianie.
   - **Dostępność adresu połączenia SSL** — urządzenie klienckie może lub nie może (w zależności od wybranej opcji) nawiązać połączenie SSL z określonym serwerem (nazwa:port). Dla każdego serwera możesz dodatkowo określić certyfikat SSL. W takim przypadku Agent sieciowy weryfikuje certyfikat serwera, oprócz sprawdzenia możliwości połączenia SSL. Jeśli certyfikat nie pasuje, połączenie nie powiedzie się. Częstotliwość połączenia wynosi raz na minutę.

8. W otwartym oknie możesz określić warunek do przełączenia Agenta sieciowego do innego Serwera administracyjnego. Nazwa okna zależy od wartości wybranej w poprzednim kroku. Określ następujące ustawienia warunku przełączania:

   - **Wartość**

     W tym polu możesz dodać jeden lub kilka wartości dla tworzonego warunku.

- **Zgodny z przynajmniej jedną wartością z listy**

  Jeśli ta opcja jest zaznaczona, warunek zostanie spełniony bez względu na wartość określoną na liście **Wartość**.

  Domyślnie opcja ta jest zaznaczona.

- **Niezgodny z żadną wartością z listy**

  Jeśli ta opcja jest zaznaczona, warunek zostanie spełniony, jeśli jego wartość nie znajduje się na liście **Wartość**.

9. W oknie **Nowy opis** zaznacz opcję **Opis włączony**, aby włączyć korzystanie z nowego opisu lokalizacji sieciowej.

Zostanie utworzona nowa reguła przełączania według opisu lokalizacji sieciowej. Za każdym razem, gdy zostaną spełnione warunki reguły, Agent sieciowy będzie używał profilu połączenia, określonego w regule, do łączenia się z Serwerem administracyjnym.

Opisy lokalizacji sieciowej są sprawdzane, czy pasują do układu sieci, zgodnie z ich kolejnością na liście. Jeżeli do sieci pasuje kilka opisów, użyty będzie pierwszy z nich. Możesz zmienić kolejność wyświetlania reguł na liście przy pomocy przycisków **W górę** (⬆) i **W dół** (⬇).

Powiadomienia o zdarzeniach

Ta sekcja opisuje sposób wybrania metody dostarczenia administratorowi powiadomień o zdarzeniach, które wystąpiły na urządzeniach klienckich, a także sposób skonfigurowania ustawień powiadomień o zdarzeniach.

Znaleźć tu można także opis sposobu przetestowania dostarczania powiadomień o zdarzeniach przy użyciu wirusa testowego Eicar.

Konfigurowanie powiadomień o zdarzeniach

Kaspersky Security Center umożliwia wybranie metody powiadamiania administratora o zdarzeniach występujących na urządzeniach klienckich oraz skonfigurowanie powiadomień:

- Poprzez e-mail. Po wystąpieniu zdarzenia, aplikacja wyśle powiadomienie na określone adresy e-mail. Możesz zmodyfikować treść powiadomienia.
- Za pośrednictwem wiadomości SMS. Po wystąpieniu zdarzenia, aplikacja wyśle powiadomienie na określone numery telefonu. Możesz skonfigurować wysyłanie powiadomień SMS poprzez bramkę pocztową.
- Poprzez uruchomienie pliku wykonywalnego. Po wystąpieniu zdarzenia na urządzeniu, na stacji roboczej administratora zostanie uruchomiony plik wykonywalny. Korzystając z pliku wykonywalnego, administrator może pobrać parametry dowolnego zdarzenia, które wystąpiło.

W celu skonfigurowania wysyłania powiadomień o zdarzeniach występujących na urządzeniach klienckich:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.

3. Kliknij odnośnik **Konfiguruj powiadomienia i eksportowanie zdarzeń** i z listy rozwijalnej wybierz wartość **Konfiguruj powiadomienia**.

   Spowoduje to otwarcie okna **Właściwości: Zdarzenia**.

4. W sekcji **Powiadamianie** wybierz metodę powiadamiania (poprzez e-mail, za pośrednictwem wiadomości SMS lub przez uruchomienie pliku wykonywalnego) i zdefiniuj ustawienia powiadomień:

   - **E-mail**

     Zakładka **E-mail** umożliwia skonfigurowanie wysyłania powiadomień o zdarzeniach za pośrednictwem poczty elektronicznej.

     W polu **Adresaci (adresy e-mail)** określ adresy e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami.

     W polu **Serwer SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

     - Adres IPv4 lub IPv6
     - Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
     - Nazwa DNS serwera SMTP

     W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

     Jeśli włączysz opcję **Użyj przeszukiwania DNS MX**, możesz użyć kilku wpisów MX adresów IP dla tej samej nazwy DNS serwera SMTP. Ta sama nazwa DNS może posiadać kilka wpisów MX z różnymi wartościami priorytetu odbierania wiadomości e-mail. Serwer administracyjny spróbuje wysłać powiadomienia e-mail do serwera SMTP w kolejności rosnącej priorytetów wpisów MX. Domyślnie opcja ta jest wyłączona.

     > Jeśli włączysz opcję **Użyj przeszukiwania DNS MX** i nie włączysz korzystania z ustawień TLS, zalecane jest użycie ustawień DNSSEC na urządzeniu serwerowym jako dodatkowego środka ochrony wysyłania powiadomień e-mail.

     Kliknij odnośnik **Ustawienia**, aby zdefiniować dodatkowe ustawienia powiadomień:

     - Nazwa podmiotu (nazwa podmiotu wiadomości e-mail)
     - Adres e-mail nadawcy
     - Ustawienia uwierzytelniania ESMTP

     Jeśli dla serwera SMTP włączono uwierzytelnianie ESMTP, do autoryzacji na serwerze SMTP należy określić konto.

     - Ustawienia TLS dla serwera SMTP:
       - **Nie korzystaj z TLS**

         Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.

       - **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

         Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.

       - **Zawsze używaj TLS, sprawdź certyfikat serwera pod kątem ważności**

Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź certyfikat serwera pod kątem ważności**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

Możesz określić ustawienia TLS dla serwera SMTP:

- Odszukaj plik certyfikatu serwera SMTP:

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

- Odszukaj plik certyfikatu klienta:

Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

- Certyfikat X-509:

Musisz określić plik z certyfikatem oraz plik z kluczem prywatnym. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po załadowaniu obu plików należy określić hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

- Kontener pkcs12:

Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

Pole **Treść powiadomienia** zawiera standardowy tekst z informacjami dotyczącymi zdarzenia, który aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera dodatkowe parametry, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny. Istnieje możliwość zmodyfikowania treści wiadomości poprzez dodanie innych parametrów zastępczych z bardziej szczegółowymi danymi dotyczącymi zdarzenia. Lista dodatkowych parametrów jest dostępna po kliknięciu przycisku, znajdującego się z prawej strony pola.

Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%".

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy poprawnie skonfigurowałeś powiadomienia. Aplikacja powinna wysłać powiadomienie testowe na adresy e-mail, które określiłeś.

- **SMS**

Na zakładce **SMS** możesz skonfigurować wysyłanie powiadomień SMS o różnych zdarzeniach na telefon komórkowy. Wiadomości SMS są wysyłane poprzez bramkę pocztową.

W polu **Odbiorcy (adresy e-mail)** określ adres e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami. Powiadomienia będą dostarczane na numery telefonów skojarzone z określonymi adresami e-mail.

W polu **Serwery SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
- Nazwa DNS serwera SMTP

W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

Kliknij odnośnik **Ustawienia**, aby zdefiniować dodatkowe ustawienia powiadomień:

- Nazwa podmiotu (nazwa podmiotu wiadomości e-mail)
- Adres e-mail nadawcy
- Ustawienia uwierzytelniania ESMTP

Jeśli to konieczne, jeśli dla serwera SMTP włączono uwierzytelnianie ESMTP, do autoryzacji na serwerze SMTP możesz określić konto.

- Ustawienia TLS dla serwera SMTP

Możesz wyłączyć korzystanie z TLS, użyć TLS, jeśli serwer SMTP obsługuje ten protokół lub możesz wymusić użycie tylko TLS. Jeśli zdecydujesz się używać tylko TLS, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Dodatkowo, jeśli wybierzesz używanie tylko TLS, możesz określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

- Odszukaj plik certyfikatu serwera SMTP

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Kaspersky Security Center. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może zawierać pustą wartość, jeśli klucz prywatny nie zostanie zakodowane. Pole **Treść powiadomienia** zawiera standardowy tekst z informacjami o zdarzeniu, które aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera dodatkowe parametry, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny. Istnieje możliwość zmodyfikowania treści wiadomości poprzez dodanie innych parametrów zastępczych z bardziej szczegółowymi danymi dotyczącymi zdarzenia. Lista dodatkowych parametrów jest dostępna po kliknięciu przycisku, znajdującego się z prawej strony pola.

Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%”.

Kliknij odnośnik **Ustaw limit liczby powiadomień**, aby określić maksymalną liczbę powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy powiadomienia zostały skonfigurowane poprawnie. Aplikacja powinna wysłać powiadomienie testowe do określonych odbiorców.

- **Plik wykonywalny do uruchomienia**

  Jeśli wybrana jest ta metoda powiadamiania, w polu wejściowym określ aplikację, która zostanie uruchomiona, gdy wystąpi zdarzenie.

  Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

  Przycisk **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie na wskazany adres e-mail.

5. W polu **Treść powiadomienia** wprowadź tekst, który aplikacja wyśle po wystąpieniu zdarzenia.

   Możesz użyć listy rozwijanej znajdującej się na prawo od pola tekstowego, aby dodać dodatkowe ustawienia ze szczegółami zdarzenia (na przykład: opis zdarzenia lub czas wystąpienia).

   > Jeżeli tekst powiadomienia zawiera znak %, należy go określić dwukrotnie, aby umożliwić wysłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%".

6. Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy powiadomienia zostały skonfigurowane poprawnie.

   Aplikacja wysyła powiadomienie testowe do określonego użytkownika.

7. Kliknij **OK**, aby zachować zmiany.

Skonfigurowane ustawienia powiadamiania zostaną zastosowane do wszystkich zdarzeń występujących na urządzeniach klienckich.

Możesz zastąpić ustawienia powiadamiania dla pewnych zdarzeń w sekcji **Konfiguracja zdarzenia** ustawień Serwera administracyjnego, ustawień zasady lub ustawień aplikacji.

Sprawdzanie opcji wysyłania powiadomień

Aby sprawdzić, czy powiadomienia o zdarzeniach są dostarczane, aplikacja używa powiadomień o wykryciu na urządzeniach klienckich „wirusa" testowego EICAR.

W celu sprawdzenia opcji wysyłania powiadomień o zdarzeniach:

1. Zatrzymaj zadanie ochrony systemu plików w czasie rzeczywistym na urządzeniu klienckim, a następnie skopiuj na nie „wirusa" testowego EICAR. Włącz ponownie ochronę w czasie rzeczywistym systemu plików.

2. Uruchom zadanie skanowania dla urządzeń klienckich w grupie administracyjnej lub dla wskazanych urządzeń, uwzględniając urządzenie zawierające „wirusa" testowego EICAR.

   Jeżeli zadanie skanowania jest skonfigurowane poprawnie, "wirus" testowy zostanie wykryty. Jeżeli powiadomienia są skonfigurowane poprawnie, zostaniesz powiadomiony o wykryciu wirusa.

   W obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Zdarzenia** wybór **Ostatnie zdarzenia** będzie wyświetlał wpis dotyczący wykrycia "wirusa".

> EICAR nie zawiera kodu, który mógłby wyrządzić szkody na urządzeniu. Jednak większość aplikacji zabezpieczających wykrywa ten plik jako wirusa. „Wirusa" testowego możesz pobrać z oficjalnej strony EICAR.

Wyświetlanie powiadomień o zdarzeniach po uruchomieniu pliku wykonywalnego

Kaspersky Security Center może powiadamiać administratora o zdarzeniach na urządzeniach klienckich poprzez uruchomienie pliku wykonywalnego. Plik wykonywalny musi zawierać inny plik wykonywalny z symbolami zastępczymi zdarzenia przekazywanymi administratorowi (patrz poniższa tabela).

Symbole zastępcze opisujące zdarzenie

Symbol zastępczy	Opis symbolu zastępczego
%SEVERITY%	Priorytet zdarzenia. Możliwe wartości: • **Informacja** • **Ostrzeżenie** • **Błąd** • **Krytyczny**
%COMPUTER%	Nazwa urządzenia, na którym wystąpiło zdarzenie. Maksymalna długość nazwy urządzenia wynosi 256 znaków.
%DOMAIN%	Nazwa domeny urządzenia, na którym wystąpiło zdarzenie.
%EVENT%	Nazwa typu zdarzenia. Maksymalna długość nazwy typu zdarzenia wynosi 50 znaków.
%DESCR%	Opis zdarzenia. Maksymalna długość opisu wynosi 1000 znaków.
%RISE_TIME%	Czas utworzenia zdarzenia.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nazwa zadania. Maksymalna długość nazwy zadania wynosi 100 znaków.
%KL_PRODUCT%	Nazwa aplikacji.
%KL_VERSION%	Numer wersji aplikacji.
%KLCSAK_EVENT_SEVERITY_NUM%	Numer priorytetu zdarzenia. Możliwe wartości: • 1—**Informacja** • 2—**Ostrzeżenie** • 3—**Błąd** • 4—**Krytyczny**
%HOST_IP%	Adres IP urządzenia, na którym wystąpiło zdarzenie.
%HOST_CONN_IP%	Adres IP połączenia urządzenia, na którym wystąpiło zdarzenie.

Na przykład:
Powiadomienia o zdarzeniach są wysyłane przez plik wykonywalny (na przykład script1.bat), w którym uruchomiony jest inny plik wykonywalny (na przykład script2.bat) z symbolem zastępczym %COMPUTER%. Po wystąpieniu zdarzenia, plik script1.bat jest uruchamiany na urządzeniu administratora, który uruchamia plik script2.bat z symbolem zastępczym %COMPUTER%. Administrator uzyska nazwę urządzenia, na którym wystąpiło zdarzenie.

Szyfrowanie komunikacji z TLS

Aby usunąć luki w sieci korporacyjnej organizacji, możesz włączyć szyfrowanie ruchu sieciowego przy użyciu protokołu TLS. Możesz włączyć protokoły szyfrowania TLS i obsługiwane zestawy szyfrów na serwerze administracyjnym i serwerze iOS MDM. Kaspersky Security Center obsługuje wersje protokołu TLS 1.0, 1.1, 1.2 i 1.3. Możesz wybrać wymagany protokół szyfrowania i zestawy szyfrowania.

Kaspersky Security Center używa certyfikatów z podpisem własnym. Dodatkowa konfiguracja urządzeń iOS nie jest wymagana. Możesz także użyć swoich własnych certyfikatów. Specjaliści z Kaspersky zalecają używanie certyfikatów wydanych przez zaufane urzędy certyfikacji.

Serwer administracyjny

W celu skonfigurowania dozwolonych protokołów szyfrowania i zestawów szyfrowania na Serwerze administracyjnym:

1. Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Użyj flagi SrvUseStrictSslSettings w celu skonfigurowania dozwolonych protokołów szyfrowania i zestawów szyfrowania na Serwerze administracyjnym. Wpisz następujące polecenie:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <wartość> -t d
   ```

   Określ parametr <wartość> flagi SrvUseStrictSslSettings:

   - `4` — Włączone są tylko protokoły TLS 1.2 i TLS 1.3. Włączone są także zestawy szyfrów z TLS_RSA_WITH_AES_256_GCM_SHA384 (te zestawy szyfrów są potrzebne do zapewnienia kompatybilności z wcześniejszymi wersjami z Kaspersky Security Center). To jest wartość domyślna.

     Zestawy szyfrów obsługiwane dla protokołu TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (zestaw szyfrów z TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Zestawy szyfrów obsługiwane dla protokołu TLS 1.3:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - `5` — Włączone są tylko protokoły TLS 1.2 i TLS 1.3. W przypadku protokołów TLS 1.2 i TLS 1.3 obsługiwane są określone zestawy szyfrów wymienione poniżej.

     Zestawy szyfrów obsługiwane dla protokołu TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Zestawy szyfrów obsługiwane dla protokołu TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

Nie zalecamy używania wartości 0, 1, 2 lub 3 jako wartości parametru flagi SrvUseStrictSslSettings. Te wartości parametrów odpowiadają niezabezpieczonym wersjom protokołu TLS (protokoły TLS 1.0 i TLS 1.1) oraz niezabezpieczonym zestawom szyfrów i są używane wyłącznie w celu zapewnienia kompatybilności wstecznej z wcześniejszymi wersjami Kaspersky Security Center.

3. Uruchom ponownie następujące usługi Kaspersky Security Center 15.1:
   - Serwer administracyjny
   - Serwer sieciowy
   - Activation Proxy

Włączone jest szyfrowanie ruchu sieciowego przy użyciu protokołu TLS.

Możesz użyć flag KLTR_TLS12_ENABLED i KLTR_TLS13_ENABLED, aby włączyć obsługę odpowiednio protokołów TLS 1.2 i TLS 1.3. Te flagi są domyślnie włączone.

Aby włączyć lub wyłączyć obsługę protokołów TLS 1.2 i TLS 1.3:

1. Uruchom narzędzie klscflag.

   Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Wpisz następujące polecenia w wierszu polecenia systemu Windows, korzystając z uprawnień administratora:
   - Użyj tego polecenia, aby włączyć lub wyłączyć obsługę protokołu TLS 1.2:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <wartość> -t d
     ```

   - Użyj tego polecenia, aby włączyć lub wyłączyć obsługę protokołu TLS 1.3:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <wartość> -t d
     ```

Określ parametr < `wartość` > flagi:

- `1` — Aby włączyć obsługę protokołu TLS.
- `0` — Aby wyłączyć obsługę protokołu TLS.

Serwer iOS MDM

Połączenie między urządzeniami iOS a serwerem iOS MDM jest szyfrowane domyślnie.

W celu skonfigurowania dozwolonych protokołów szyfrowania i zestawów szyfrowania na serwerze iOS MDM:

1. Otwórz rejestr systemu urządzenia klienckiego, na którym jest zainstalowany serwer iOS MDM (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).
2. Przejdź do gałęzi:
   - W systemach 32-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
   - W systemach 64-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI
3. Utwórz klucz o nazwie `StrictSslSettings`.
4. Jako typ klucza określ `DWORD`.
5. Określ wartość klucza:
   - `2` — Włączone są protokoły TLS 1.0, TLS 1.1 i TLS 1.2.
   - `3` — Włączony jest tylko protokół TLS 1.2 (wartość domyślna).
6. Uruchom ponownie usługę serwera iOS MDM Kaspersky Security Center.

Konfigurowanie interfejsu

Możesz skonfigurować interfejs Kaspersky Security Center:

- Wyświetlić i ukryć obiekty w drzewie konsoli, w obszarze roboczym i w oknach właściwości obiektów (folderach, sekcjach) w zależności od funkcji, z której korzystasz.
- Wyświetlić i ukryć elementy okna głównego (na przykład drzewo konsoli lub standardowe menu, takie jak **Akcje** i **Widok**).

W celu skonfigurowania interfejsu Kaspersky Security Center zgodnie z aktualnie używanym zestawem funkcji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Na pasku menu okna głównego aplikacji wybierz **Widok** → **Konfiguruj interfejs**.

3. W oknie **Konfiguracja interfejsu**, które zostanie otwarte, skonfiguruj wyświetlanie elementów interfejsu, korzystając z następujących pól:

- **Wyświetl Zarządzanie lukami i poprawkami**

  Jeśli ta opcja jest włączona, w folderze **Zdalna instalacja** wyświetlany jest podfolder **Rozsyłanie obrazów urządzenia**, a w folderze **Repozytoria** wyświetlany jest podfolder **Sprzęt**.

  Ta opcja jest domyślnie wyłączona, jeśli działanie kreatora wstępnej konfiguracji nie zostało zakończone. Ta opcja jest domyślnie włączona, jeśli działanie kreatora wstępnej konfiguracji zostało zakończone.

  > Jeśli ta opcja jest wyłączona, pozycje menu **Utwórz sesję Pulpitu zdalnego** i **Udostępnianie pulpitu Windows** nie będą dostępne, nawet jeśli posiadasz licencję na zarządzanie systemami.

- **Wyświetl szyfrowanie i ochronę danych**

  Jeśli ta opcja jest włączona, drzewo konsoli wyświetla folder **Szyfrowanie i ochrona danych**.

  Domyślnie opcja ta jest włączona.

- **Wyświetl ustawienia kontroli węzła końcowego**

  Jeśli ta opcja jest włączona, w sekcji **Kontrola zabezpieczeń** okna właściwości zasady Kaspersky Endpoint Security for Windows wyświetlane są następujące podsekcje:

  - **Kontrola aplikacji**
  - **Kontrola urządzeń**
  - **Kontrola sieci**
  - **Adaptacyjna kontrola anomalii**

  Jeśli ta opcja jest wyłączona, wyżej wymienione podsekcje nie są wyświetlane w sekcji **Kontrola zabezpieczeń**.

  Domyślnie opcja ta jest włączona.

- **Wyświetl Zarządzanie urządzeniami mobilnymi**

  Jeśli ta opcja jest włączona, funkcja **Zarządzanie urządzeniami mobilnymi** jest dostępna. Po ponownym uruchomieniu aplikacji, drzewo konsoli wyświetla folder **Urządzenia mobilne**.

  Domyślnie opcja ta jest włączona.

- **Wyświetl podrzędne Serwery administracyjne**

  Jeśli to pole jest zaznaczone, drzewo konsoli będzie wyświetlać węzły podrzędnych i wirtualnych Serwerów administracyjnych wchodzących w skład grup administracyjnych. Funkcje związane z podrzędnymi i wirtualnymi Serwerami administracyjnymi—na przykład, tworzenie zadań zdalnej instalacji aplikacji na podrzędnych Serwerach administracyjnych—będą dostępne.

  Domyślnie pole to nie jest zaznaczone.

- **Wyświetl sekcje ustawień zabezpieczeń**

  Jeśli ta opcja jest włączona, sekcja **Zabezpieczenia** jest wyświetlana w oknie właściwości Serwera administracyjnego, grup administracyjnych i innych obiektów. Ta opcja umożliwia nadanie użytkownikom i grupom użytkowników niestandardowych uprawnień do pracy z obiektami.

Domyślnie opcja ta jest wyłączona.

4. Kliknij **OK**.

Aby zastosować niektóre zmiany, musisz zamknąć okno główne aplikacji, a następnie otworzyć je ponownie.

W celu skonfigurowania wyświetlania elementów w oknie głównym aplikacji:

1. Na pasku menu okna głównego aplikacji wybierz **Widok** → **Konfiguruj**.
2. W oknie **Konfiguracja widoku**, które zostanie otwarte, skonfiguruj wyświetlanie elementów okna głównego, korzystając z dostępnych pól.
3. Kliknij **OK**.

Wykrywanie urządzeń w sieci

Ta sekcja opisuje kroki, jakie musisz podjąć po zainstalowaniu Kaspersky Security Center.

Scenariusz: Wykrywanie urządzeń w sieci

Przed zainstalowaniem aplikacji zabezpieczających musisz przeprowadzić wykrywanie urządzeń. Serwer administracyjny otrzymuje informacje o wykrytych urządzeniach i umożliwia zarządzanie urządzeniami za pomocą zasad. Do aktualizacji listy urządzeń dostępnych w sieci potrzebne są regularne ankiety sieciowe.

Przed rozpoczęciem odpytywania sieci upewnij się, że protokół SMB jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Aby włączyć protokół SMB, postępuj zgodnie z instrukcjami dla swojego systemu operacyjnego.

Wykrywanie urządzeń sieciowych przebiega w następujących etapach:

1. **Odkryj urządzenia**

   Kreator wstępnej konfiguracji poprowadzi Cię przez wstępne wyszukiwanie urządzeń i pomoże w odnalezieniu urządzeń w sieci, takich jak komputery, tablety i telefony komórkowe. Możesz także ręcznie przeprowadzić wykrywanie urządzeń.

2. **Skonfiguruj zaplanowane ankiety**

   Zdecyduj, których typów przeszukiwania chcesz używać regularnie. Włącz żądane typy i skonfiguruj harmonogram ankiety. Możesz zapoznać się z zaleceniami dotyczącymi częstotliwości odpytywania sieci.

3. **Konfiguracja reguł dodawania wykrytych urządzeń do grup administracyjnych (opcjonalne)**

   Jeśli nowe urządzenia pojawią się w Twojej sieci, zostaną wykryte podczas regularnych przeszukiwań i zostaną automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**. Możesz skonfigurować reguły przenoszenia urządzeń, aby zautomatyzować przydzielanie urządzeń do grupy **Zarządzane urządzenia**. Możesz także skonfigurować reguły zatrzymania.

   Jeśli pominiesz krok 3, nowo wykryte urządzenia zostaną przydzielone do grupy **Urządzenia nieprzypisane**. Jeśli chcesz, możesz ręcznie przenieść te urządzenia do grupy **Zarządzane urządzenia**. Jeśli ręcznie przeniesiesz te urządzenia do grupy **Zarządzane urządzenia**, możesz przeanalizować informacje o każdym urządzeniu i zdecydować, czy chcesz przenieść je do grupy administracyjnej i do jakiej grupy.

Wyniki

Zakończenie scenariusza powoduje, że:

- Serwer administracyjny Kaspersky Security Center wykrywa urządzenia, które znajdują się w sieci, i zapewnia informacje o nich.
- Przyszłe przeszukiwania zostają skonfigurowane i przeprowadzone zgodnie z określonym terminarzem.
- Nowo wykryte urządzenia zostaną rozmieszczone zgodnie ze skonfigurowanymi regułami (lub jeśli nie ma skonfigurowanych reguł, urządzenia pozostają w grupie **Urządzenia nieprzypisane**).

Urządzenia nieprzypisane

Sekcja ta zawiera informacje o sposobie zarządzania urządzeniami w sieci firmowej, gdy nie należą do grupy administracyjnej.

Wykrywanie urządzeń

Ta sekcja opisuje typy wykrywania urządzeń dostępne w Kaspersky Security Center i oferuje informacje dotyczące korzystania z każdego typu.

Serwer administracyjny otrzymuje informacje o strukturze sieci i urządzeń w tej sieci poprzez regularne przeszukiwanie. Informacje są zapisywane w bazie danych Serwera administracyjnego. Serwer administracyjny może wykorzystywać następujące typy przeszukiwania:

- **Przeszukiwanie sieci Windows**. Serwer administracyjny może wykonywać dwa rodzaje przeszukiwań sieci Windows: szybkie i pełne. Podczas szybkiego przeszukiwania Serwer administracyjny pobiera wyłącznie informacje o urządzeniach znajdujących się na liście nazw NetBIOS wszystkich domen sieci i grup roboczych. Podczas pełnego przeszukiwania wymaganych jest więcej informacji z urządzenia klienckiego, takich jak: nazwa systemu operacyjnego, adres IP, nazwa DNS, nazwa NetBIOS. Domyślnie włączone są oba przeszukiwania: szybkie i pełne. Przeszukiwanie sieci Windows może nie wykryć urządzeń, na przykład, jeśli porty UDP 137, UDP 138, TCP 139 są zamknięte na routerze lub przez zaporę sieciową.

- **Przeszukiwanie Active Directory**. Serwer administracyjny pobiera informacje na temat struktury jednostki Active Directory i nazw DNS urządzeń z grup Active Directory. Domyślnie ten typ przeszukiwania jest włączony. Zalecane jest użycie przeszukiwania Active Directory, jeśli używasz Active directory; w przeciwnym razie Serwer administracyjny nie wykryje żadnych urządzeń. Jeśli używasz Active Directory, ale niektóre z urządzeń w sieci nie są wymienione jako członkowie, te urządzenia nie mogą być wykrywane przez przeszukiwanie Active Directory.

- **Przeszukiwanie zakresu IP**. Serwer administracyjny przeszukuje określone zakresy IP przy użyciu pakietów ICMP lub protokołu NBNS i sporządza pełen zestaw danych na temat urządzeń znajdujących się w tych zakresach IP. Domyślnie ten typ przeszukiwania jest wyłączony. Nie jest zalecane korzystanie z tego typu przeszukiwania, jeśli korzystasz z przeszukiwania sieci Windows i/lub przeszukiwania Active Directory.

- **Przeszukiwanie Zeroconf**. Punkt dystrybucji, który odpytuje sieć IPv6 za pomocą zero-configuration networking (zwany również *Zeroconf*). Domyślnie ten typ przeszukiwania jest wyłączony. Możesz użyć przeszukiwania Zeroconf, jeśli na punkcie dystrybucji działa system Linux.

Jeśli skonfigurowałeś i włączyłeś reguły przenoszenia urządzeń, nowo wykryte urządzenia są automatycznie umieszczane w grupie **Zarządzane urządzenia**. Jeśli nie włączono żadnych reguł przenoszenia, nowo wykryte urządzenia zostają automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**.

Możesz zmodyfikować ustawienia wykrywania urządzeń dla każdego typu. Na przykład, możesz chcieć zmodyfikować terminarz przeszukiwania lub ustawić, czy przeszukiwany ma być cały las domeny lub tylko określona domena.

Przed rozpoczęciem przeszukiwania sieci upewnij się, że protokół SMB jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Aby włączyć protokół SMB, postępuj zgodnie z instrukcjami dla swojego systemu operacyjnego.

Przeszukiwanie sieci Windows

Informacje o przeszukiwaniu sieci Windows

Podczas szybkiego przeszukiwania Serwer administracyjny pobiera wyłącznie informacje o urządzeniach znajdujących się na liście nazw NetBIOS wszystkich domen sieci i grup roboczych. Podczas pełnego przeszukiwania wymagane są następujące informacje o każdym urządzeniu klienckim:

- Nazwa systemu operacyjnego

- Adres IP

- Nazwa DNS
- Nazwa NetBIOS

Szybkie przeszukiwanie i pełne przeszukiwanie wymagają:

- Porty UDP 137/138, TCP 139, UDP 445, TCP 445 muszą być dostępne w sieci.
- Protokół SMB jest włączony.
- Usługa Przeglądarka komputera Microsoft musi być używana, a główna przeglądarka komputera musi być włączona na Serwerze administracyjnym.
- Usługa Przeglądarka komputera Microsoft musi być używana, a główna przeglądarka komputera musi być włączona na urządzeniach klienckich:
  - Przynajmniej na jednym urządzeniu, jeśli liczba urządzeń w sieci nie przekracza 32.
  - Przynajmniej na jednym urządzeniu dla każdego z 32 urządzeń w sieci.

Pełne przeszukiwanie może być uruchomione tylko wtedy, gdy szybkie przeszukiwanie było uruchomione przynajmniej raz.

Przeglądanie i modyfikowanie ustawień przeszukiwania sieci Windows

W celu zmodyfikowania ustawień dla przeszukiwania sieci Windows:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Domeny**.

   Do folderu **Urządzenia nieprzypisane** możesz przejść z folderu **Wykrywanie urządzeń**, klikając przycisk **Przeszukaj teraz**.

   W obszarze roboczym podfolderu **Domeny** zostanie wyświetlona lista urządzeń.

2. Kliknij **Przeszukaj teraz**.

   Zostanie otwarte okno właściwości domeny. Jeśli chcesz, zmodyfikuj ustawienia przeszukiwania sieci Windows:

   - **Włącz przeszukiwanie sieci Windows**

     Opcja ta jest wybrana domyślnie. Jeśli nie chcesz przeprowadzić przeszukiwania sieci Windows (na przykład, jeśli myślisz, że przeszukiwanie Active Directory wystarczy), możesz odznaczyć tę opcję.

   - **Ustaw terminarz szybkiego przeszukiwania**

     Domyślny czas to 15 minut.

     Podczas szybkiego przeszukiwania Serwer administracyjny pobiera wyłącznie informacje o urządzeniach znajdujących się na liście nazw NetBIOS wszystkich domen sieci i grup roboczych.

     Dane otrzymane przy kolejnym przeszukiwaniu całkowicie zastępują starsze dane.

     Dostępne są następujące opcje terminarza przeszukiwania:

     - **Co N dni**

       Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

       Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N minut**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

  Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

- **Według dni tygodnia**

  Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc, w określone dni wybranych tygodni**

  Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Uruchom pominięte zadania**

  Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

  Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

  Domyślnie opcja ta jest włączona.

- **Ustaw terminarz pełnego przeszukiwania**

  Domyślny przedział czasu wynosi jedną godzinę. Dane otrzymane przy kolejnym przeszukiwaniu całkowicie zastępują starsze dane.

  Dostępne są następujące opcje terminarza przeszukiwania:

  - **Co N dni**

    Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Co N minut**

    Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

    Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

  - **Według dni tygodnia**

    Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

    Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

  - **Co miesiąc, w określone dni wybranych tygodni**

    Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Uruchom pominięte zadania**

  Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

  Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

  Domyślnie opcja ta jest włączona.

Jeśli chcesz przeprowadzić przeszukiwanie natychmiast, kliknij **Przeszukaj teraz**. Zostaną uruchomione oba typy przeszukiwań.

Na wirtualnym Serwerze administracyjnym ustawienia przeszukiwania sieci Windows można przeglądać i modyfikować w oknie ustawień punktu dystrybucji, w sekcji **Wykrywanie urządzeń**.

Przeszukiwanie Active Directory

Użyj przeszukiwania Active Directory, jeśli używasz Active Directory; w innym przypadku zalecane jest użycie innych typów przeszukiwania. Jeśli używasz Active Directory, ale niektóre z urządzeń w sieci nie są wymienione jako członkowie, te urządzenia nie mogą być wykrywane przez przeszukiwanie Active Directory.

Wyniki przeszukiwania Active Directory są przechowywane na Serwerze administracyjnym przez 30 dni niezależnie od wyników kolejnego przeszukiwania.

Przed rozpoczęciem przeszukiwania sieci upewnij się, że protokół SMB jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Aby włączyć protokół SMB, postępuj zgodnie z instrukcjami dla swojego systemu operacyjnego.

Przeglądanie i modyfikowanie ustawień przeszukiwania Active Directory

W celu zmodyfikowania ustawień przeszukiwania grup Active Directory:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Active Directory**.

   Alternatywnie, z folderu **Urządzenia nieprzypisane** możesz przejść do folderu **Wykrywanie urządzeń**, klikając przycisk **Przeszukaj teraz**.

2. Kliknij **Konfiguruj przeszukiwanie**.

   Zostanie otwarte okno właściwości Active Directory. Jeśli chcesz, zmodyfikuj ustawienia przeszukiwania grupy Active Directory:

   - **Włącz przeszukiwanie Active Directory**

     Opcja ta jest wybrana domyślnie. Jednakże, jeśli nie używasz Active Directory, przeszukiwanie nie pobierze żadnych wyników. W tym przypadku możesz odznaczyć tę opcję.

- **Ustaw terminarz przeszukiwania**

  Domyślny przedział czasu wynosi jedną godzinę.

  Dostępne są następujące opcje terminarza przeszukiwania:

  - **Co N dni**

    Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Co N minut**

    Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

    Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

  - **Według dni tygodnia**

    Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

    Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

  - **Co miesiąc, w określone dni wybranych tygodni**

    Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

    Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

  - **Uruchom pominięte zadania**

    Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

    Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

    Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

    Domyślnie opcja ta jest włączona.

- **Zaawansowane**

  Możesz wybrać, które domeny Active Directory przeszukiwać:

  - Domena Active Directory, do której należy Kaspersky Security Center.
  - Las domeny, do którego należy Kaspersky Security Center.
  - Określona lista domen Active Directory.

Jeśli wybierzesz tę opcję, możesz dodać domeny do obszaru przeszukiwania:

- Kliknij przycisk **Dodaj**.
- W odpowiednich polach określ adres kontrolera domeny, nazwę i hasło konta, aby uzyskać do niego dostęp.
- Kliknij **OK**, aby zachować zmiany.

Możesz wybrać adres kontrolera domeny na liście i kliknąć przyciski **Modyfikuj** lub **Usuń**, aby go zmodyfikować lub usunąć.

- Kliknij **OK**, aby zachować zmiany.

Jeśli chcesz przeprowadzić przeszukiwanie natychmiast, kliknij przycisk **Przeszukaj teraz**.

Na wirtualnym Serwerze administracyjnym ustawienia przeszukiwania grup Active Directory można przeglądać i modyfikować w oknie właściwości punktu dystrybucji, w sekcji **Wykrywanie urządzeń**.

Przeszukiwanie zakresu IP

Serwer administracyjny przeszukuje określone zakresy IP przy użyciu pakietów ICMP lub protokołu NBNS i sporządza pełen zestaw danych na temat urządzeń znajdujących się w tych zakresach IP. Domyślnie ten typ przeszukiwania jest wyłączony.

Dla hostów z systemem Linux w ramach kontrolera domeny Microsoft Active Directory lub Samba, określ parametry `netbios name` i `workgroup` w pliku `/etc/samba/smb.conf`. W przeciwnym razie wyniki przeszukiwania mogą zawierać zduplikowane hosty.

Przed rozpoczęciem przeszukiwania sieci upewnij się, że protokół SMB jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Aby włączyć protokół SMB, postępuj zgodnie z instrukcjami dla swojego systemu operacyjnego.

Przeglądanie i modyfikowanie ustawień przeszukiwania zakresu IP

W celu przejrzenia i zmodyfikowania ustawień przeszukiwania grup Zakres IP:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Zakresy IP**.

   Możesz przejść z folderu **Urządzenia nieprzypisane** do folderu **Wykrywanie urządzeń** poprzez kliknięcie **Przeszukaj teraz**.

2. Jeśli chcesz, w podfolderze **Zakresy IP** kliknij **Dodaj podsieć**, aby dodać zakres IP dla przeszukiwania, a następnie kliknij **OK**.

3. Kliknij **Konfiguruj przeszukiwanie**.

Zostanie otwarte okno właściwości zakresów IP. Jeśli chcesz, możesz zmodyfikować ustawienia przeszukiwania zakresu IP:

- **Włącz przeszukiwanie zakresu IP**

  Opcja ta nie jest wybrana domyślnie. Nie jest zalecane korzystanie z tego typu przeszukiwania, jeśli korzystasz z przeszukiwania sieci Windows i/lub przeszukiwania Active Directory.

- **Ustaw terminarz przeszukiwania**

  Domyślny czas to 420 minut. Dane otrzymane przy kolejnym przeszukiwaniu całkowicie zastępują starsze dane.

  Dostępne są następujące opcje terminarza przeszukiwania:

  - **Co N dni**

    Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Co N minut**

    Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

    Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

  - **Według dni tygodnia**

    Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

    Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

  - **Co miesiąc, w określone dni wybranych tygodni**

    Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

    Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

  - **Uruchom pominięte zadania**

    Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

    Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

    Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

    Domyślnie opcja ta jest włączona.

Jeśli chcesz przeprowadzić przeszukiwanie natychmiast, kliknij **Przeszukaj teraz**. Ten przycisk jest dostępny tylko wtedy, gdy wybrałeś **Włącz przeszukiwanie zakresu IP**.

Na wirtualnym Serwerze administracyjnym ustawienia przeszukiwania zakresu IP można przeglądać i modyfikować w oknie właściwości punktu dystrybucji, w sekcji **Wykrywanie urządzeń**. Urządzenia klienckie wykryte podczas przeszukiwania zakresów IP są wyświetlane w folderze **Domeny** wirtualnego Serwera administracyjnego.

Przeszukiwanie Zeroconf

Ten typ przeszukiwania jest obsługiwany tylko w przypadku punktów dystrybucji opartych na systemie Linux.

Punkt dystrybucji może przeszukiwać sieci, które mają urządzenia z adresami IPv6. W takim przypadku zakresy adresów IP nie są określone, a punkt dystrybucji przeszukuje całą sieć za pomocą zero-configuration networking (zwany również *Zeroconf*). Aby rozpocząć korzystanie z Zeroconf, musisz zainstalować narzędzie avahi-browse w punkcie dystrybucji.

W celu włączenia przeszukiwania Zeroconf:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Zakresy IP**.

   Możesz przejść z folderu **Urządzenia nieprzypisane** do folderu **Wykrywanie urządzeń** poprzez kliknięcie **Przeszukaj teraz**.

2. Kliknij **Konfiguruj przeszukiwanie**.

3. W otwartym oknie właściwości zakresów adresów IP wybierz **Włącz przeszukiwanie za pomocą technologii Zeroconf**.

Następnie punkt dystrybucji zaczyna przeszukiwać sieć. W takim przypadku określone zakresy adresów IP są ignorowane.

Praca z domenami Windows. Przeglądanie i modyfikowanie ustawień domeny

W celu zmodyfikowania ustawień domeny:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Domeny**.

2. Wybierz domenę i otwórz okno jej właściwości w jeden z następujących sposobów:

   - z menu kontekstowego domeny wybierz polecenie **Właściwości**.
   - kliknij odnośnik **Pokaż właściwości grupy**.

Zostanie otwarte okno **Właściwości: <Nazwa domeny>**, w którym możesz skonfigurować wybraną domenę.

Konfigurowanie reguły zatrzymania dla urządzeń nieprzypisanych

Po zakończeniu przeszukiwania sieci Windows, wykryte urządzenia zostały umieszczone w podgrupach grupy administracyjnej Urządzenia nieprzypisane. T grupę administracyjną można znaleźć w **Zaawansowane** → **Wykrywanie urządzeń** → **Domeny**. Folder **Domeny** to grupa nadrzędna. Zawiera grupy potomne, które zostały nazwane po odpowiednich domenach i grupach roboczych, które zostały wykryte podczas przeszukiwania sieci. Grupa nadrzędna może także zawierać grupę administracyjną urządzeń mobilnych. Możesz skonfigurować reguły zatrzymania urządzeń nieprzypisanych dla grupy nadrzędnej i dla każdej grupy potomnej. Reguły zatrzymania nie zależą od ustawień przeszukiwania sieci i działają nawet wtedy, gdy przeszukiwanie sieci jest wyłączone.

W celu skonfigurowania reguł zatrzymania dla urządzeń nieprzypisanych:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wykonaj jedną z następujących czynności:

   - Aby skonfigurować ustawienia grupy nadrzędnej, kliknij prawym klawiszem myszy podfolder **Domeny** i wybierz **Właściwości**.

     Zostanie otwarte okno właściwości grupy nadrzędnej.

   - Aby skonfigurować ustawienia grupy potomnej, kliknij jej nazwę prawym klawiszem myszy i z otwartego menu wybierz **Właściwości**.

     Zostanie otwarte okno właściwości grupy potomnej.

2. W sekcji **Urządzenia** określ następujące ustawienia:

   - **Usuń urządzenie z grupy, jeżeli było nieaktywne dłużej niż (dni)**

     Jeśli ta opcja jest włączona, możesz określić przedział czasu, po upływie którego urządzenie zostanie automatycznie usunięte z grupy. Domyślnie, ta opcja jest także rozsyłana do grup potomnych. Domyślny przedział czasu wynosi 7 dni.

     Domyślnie opcja ta jest włączona.

   - **Dziedzicz z grupy nadrzędnej**

     Jeśli ta opcja jest włączona, okres zatrzymania dla urządzeń w bieżącej grupie jest dziedziczony z grupy nadrzędnej nie może zostać zmieniony.

     Ta opcja jest dostępna tylko dla grup potomnych.

     Domyślnie opcja ta jest włączona.

   - **Wymuś dziedziczenie w grupach podrzędnych**

     Wartości ustawień zostaną rozesłane do grup podrzędnych ale we właściwościach grup podrzędnych te ustawienia są zablokowane.

     Domyślnie opcja ta jest wyłączona.

Twoje zmiany zostaną zapisane i zastosowane.

Praca z zakresami IP

Możesz dostosować istniejące zakresy IP oraz utworzyć nowe.

Tworzenie zakresu IP

W celu utworzenia zakresu IP:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Zakresy IP**.
2. Z menu kontekstowego folderu wybierz **Nowy → Zakres IP**.
3. W oknie **Nowy zakres IP**, które zostanie otwarte, dostosuj ustawienia nowego zakresu IP.

Nowy zakres IP pojawi się w folderze **Zakresy IP**.

Przeglądanie i modyfikowanie ustawień zakresu IP

W celu zmodyfikowania ustawień zakresu IP:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Zakresy IP**.
2. Wybierz zakres IP i otwórz okno jego właściwości w jeden z następujących sposobów:
   - Z menu kontekstowego zakresu IP wybierz polecenie **Właściwości**.
   - kliknij odnośnik **Pokaż właściwości grupy**.

Zostanie otwarte okno **Właściwości: <Nazwa zakresu IP>**, w którym możesz skonfigurować właściwości wybranego zakresu IP.

Praca z grupami Active Directory. Przeglądanie i modyfikowanie ustawień grupy

W celu zmodyfikowania ustawień grupy Active Directory:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Active Directory**.
2. Wybierz grupę Active Directory i otwórz okno jej właściwości w jeden z następujących sposobów:
   - Z menu kontekstowego zakresu IP wybierz polecenie **Właściwości**.
   - kliknij odnośnik **Pokaż właściwości grupy**.

Zostanie otwarte okno **Właściwości: <Nazwa grupy Active Directory>**, w którym można skonfigurować ustawienia wybranej grupy Active Directory.

Tworzenie reguł automatycznego przenoszenia urządzeń do grup administracyjnych

Możesz skonfigurować automatyczne przenoszenie urządzeń do grup administracyjnych po ich wykryciu podczas przeszukiwania sieci firmowej.

W celu skonfigurowania reguł automatycznego przenoszenia urządzeń do grup administracyjnych:

1. Z drzewa konsoli wybierz folder **Urządzenia nieprzypisane**.
2. W obszarze roboczym folderu kliknij **Konfiguruj reguły**.

   Spowoduje to otwarcie okna **Właściwości: Urządzenia nieprzypisane**. W sekcji **Przenieś urządzenia** skonfiguruj reguły automatycznego przenoszenia urządzeń do grup administracyjnych.

Do urządzenia zostanie zastosowana pierwsza odpowiednia reguła na liście (od góry do dołu listy).

Używanie dynamicznego trybu VDI na urządzeniach klienckich

Wirtualna infrastruktura może zostać wdrożona w sieci firmowej z użyciem tymczasowych maszyn wirtualnych. Kaspersky Security Center wykrywa tymczasowe maszyny wirtualne i dodaje o nich informacje do bazy danych Serwera administracyjnego. Gdy użytkownik zakończy korzystanie z tymczasowej maszyny wirtualnej, maszyna ta jest usuwana z wirtualnej infrastruktury. Wpis dotyczący usuniętej maszyny wirtualnej może być zapisany w bazie danych Serwera administracyjnego. Dodatkowo, w Konsoli administracyjnej mogą być wyświetlane nieistniejące maszyny wirtualne.

Aby informacje o nieistniejących maszynach wirtualnych nie były zapisywane, Kaspersky Security Center obsługuje tryb dynamiczny obsługi Virtual Desktop Infrastructure (VDI). Administrator może włączyć obsługę trybu dynamicznego dla VDI we właściwościach pakietu instalacyjnego Agenta sieciowego instalowanego na tymczasowej maszynie wirtualnej.

Jeśli tymczasowa maszyna wirtualna jest wyłączona, Agent sieciowy informuje Serwer administracyjny o jej wyłączeniu. Po pomyślnym wyłączeniu maszyny wirtualnej jest ona usuwana z listy urządzeń podłączonych do Serwera administracyjnego. Jeśli wyłączenie maszyny wirtualnej zakończyło się błędami, a Agent sieciowy nie wysłał do Serwera administracyjnego powiadomienia o wyłączonej maszynie wirtualnej, wdrażany jest scenariusz kopii zapasowej. W tym scenariuszu maszyna wirtualna jest usuwana z listy urządzeń podłączonych do Serwera administracyjnego po trzech niepomyślnych próbach synchronizacji z Serwerem administracyjnym.

Włączanie dynamicznego trybu VDI we właściwościach pakietu instalacyjnego Agenta sieciowego

W celu włączenia dynamicznego trybu VDI:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
2. Z menu kontekstowego pakietu instalacyjnego Agenta sieciowego wybierz **Właściwości**.

   Zostanie otwarte okno **Właściwości: Agent sieciowy Kaspersky Security Center**.

3. W oknie **Właściwości: Agent sieciowy Kaspersky Security Center** wybierz sekcję **Zaawansowane**.
4. W sekcji **Zaawansowane** wybierz opcję **Włącz tryb dynamiczny VDI**.

Urządzenie, na którym jest instalowany Agent sieciowy, stanie się częścią VDI.

Wyszukiwanie urządzeń będących częścią VDI

W celu wyszukania nieprzypisanych urządzeń będących częścią VDI:

1. Wybierz **Szukaj** z menu kontekstowego folderu **Urządzenia nieprzypisane**.

   Aby wyświetlić listę wszystkich urządzeń będących częścią Virtual Desktop Infrastructure, wybierz opcję **Szukaj** z menu kontekstowego folderu **Serwer administracyjny**.
2. W oknie **Szukaj**, na karcie **Maszyny wirtualne**, w grupie ustawień **Tak** wybierz opcję **Część Virtual Desktop Infrastructure**.
3. Kliknij przycisk **Znajdź teraz**.

Wyświetlana jest lista nieprzypisanych urządzeń, które są częścią Virtual Desktop Infrastructure.

Przenoszenie urządzeń z VDI do grupy administracyjnej

W celu przeniesienia urządzeń będących częścią VDI do grupy administracyjnej:

1. W obszarze roboczym folderu **Urządzenia nieprzypisane** kliknij **Konfiguruj reguły**.

   Zostanie otwarte okno właściwości folderu **Urządzenia nieprzypisane**.
2. W oknie właściwości folderu **Urządzenia nieprzypisane**, w sekcji **Przenieś urządzenia** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Nowa reguła**.
3. W oknie **Nowa reguła** wybierz sekcję **Maszyny wirtualne**.
4. Z listy rozwijalnej **Jest maszyną wirtualną** wybierz **Tak**.

Zostanie utworzona reguła przeniesienia urządzenia do grupy administracyjnej.

Inwentaryzacja sprzętu

Lista sprzętu (**Repozytoria** → **Sprzęt**), której używasz do przeprowadzenia inwentaryzacji sprzętu, jest uzupełniana na dwa sposoby: automatycznie i ręcznie. Po każdym przeszukaniu sieci, wszystkie wykryte urządzenia zostają dodane do listy automatycznie; jednakże możesz także ręcznie dodać urządzenia, jeśli nie chcesz przeszukiwać sieci. Możesz ręcznie dodać inne urządzenia do listy, na przykład, routery, drukarki lub sprzęt komputerowy.

We właściwościach urządzenia możesz wyświetlić i zmodyfikować szczegółowe informacje o tym urządzeniu.

Lista sprzętu może zawierać następujące typy urządzeń:

- Komputery
- Urządzenia mobilne
- Urządzenia sieciowe
- Urządzenia wirtualne
- Składniki OEM
- Peryferia komputerowe
- Podłączone urządzenia
- Telefony VoIP
- Repozytoria sieciowe

Administrator może przypisać atrybut *Sprzęt firmowy* do wykrytych urządzeń. Ten atrybut jest przypisywany ręcznie we właściwościach urządzenia, administrator może również określić kryteria automatycznego przypisywania dla tego atrybutu. W takim przypadku atrybut *Sprzęt firmowy* jest przypisywany zgodnie z typem urządzenia.

Kaspersky Security Center pozwala na wyrejestrowywanie sprzętu. W tym celu wybierz opcję **Urządzenie wyrejestrowane** we właściwościach urządzenia. Takie urządzenie nie jest wyświetlane na liście sprzętu.

Administrator może zarządzać listą programowalnych sterowników logicznych (PLC) w folderze **Sprzęt**. Szczegółowe informacje na temat zarządzania listą PLC można znaleźć w *podręczniku użytkownika dla Kaspersky Industrial CyberSecurity for Nodes*.

Dodawanie informacji o nowych urządzeniach

W celu dodania informacji o nowych urządzeniach w sieci:

1. W folderze **Repozytoria** drzewa konsoli wybierz podfolder **Sprzęt**.
2. W obszarze roboczym folderu **Sprzęt** kliknij przycisk **Dodaj urządzenie**, aby otworzyć okno **Nowe urządzenie**.
   Zostanie otwarte okno **Nowe urządzenie**.
3. W oknie **Nowe urządzenie**, na liście rozwijalnej **Typ** wybierz typ urządzenia, które chcesz dodać.
4. Kliknij **OK**.
   Okno właściwości urządzenia zostanie otwarte na sekcji **Ogólne**.

5. W sekcji **Ogólne** wypełnij pola wejściowe danymi urządzenia. Sekcja **Ogólne** wyświetla następujące ustawienia:

   - **Urządzenie firmowe**. Zaznacz to pole, jeśli chcesz przypisać atrybut *Firmowy* do urządzenia. Przy użyciu tego atrybutu można wyszukiwać urządzenia w folderze **Sprzęt**.
   - **Urządzenie wyrejestrowane**. Zaznacz pole, jeśli nie chcesz, aby urządzenie było wyświetlane na liście urządzeń w folderze **Sprzęt**.

6. Kliknij **Zastosuj**.

Nowe urządzenie będzie wyświetlane w obszarze roboczym foldera **Sprzęt**.

Konfigurowanie kryteriów wykorzystywanych do określania urządzeń firmowych

W celu skonfigurowania kryteriów wykrywania dla urządzeń firmowych:

1. W folderze **Repozytoria** drzewa konsoli wybierz podfolder **Sprzęt**.
2. W obszarze roboczym folderu **Sprzęt** kliknij przycisk **Akcje dodatkowe** i z listy rozwijalnej wybierz **Ustaw regułę dla urządzeń firmowych**.

   Zostanie otwarte okno właściwości sprzętu.
3. W oknie właściwości sprzętu, w sekcji **Urządzenia firmowe** wybierz metodę przydzielania atrybutu *Firmowy* do urządzenia:

   - **Ustaw dla urządzenia atrybut urządzenie firmowe ręcznie**. Atrybut *Sprzęt firmowy* jest przypisywany do urządzenia ręcznie w oknie właściwości urządzenia, w sekcji **Ogólne**.
   - **Ustaw dla urządzenia atrybut urządzenie firmowego automatycznie**. W sekcji ustawień **Według typu urządzenia** określ typy urządzeń, dla których aplikacja będzie automatycznie przydzielać atrybut *Firmowy*.

     > Ta opcja dotyczy tylko urządzeń, które zostały dodane przez przeszukiwanie sieci. W przypadku urządzeń dodanych ręcznie ustaw atrybut *Firmowy* ręcznie.

4. Kliknij **OK**.

Skonfigurowano kryteria wykrywania dla urządzeń firmowych.

Konfiguracja pól niestandardowych

W celu skonfigurowania niestandardowych pól urządzeń:

1. W folderze **Repozytoria** drzewa konsoli wybierz podfolder **Sprzęt**.
2. W obszarze roboczym folderu **Sprzęt** kliknij przycisk **Akcje dodatkowe** i z listy rozwijalnej wybierz **Konfiguruj niestandardowe pola danych**.

   Zostanie otwarte okno właściwości sprzętu.

3. W oknie właściwości sprzętu wybierz sekcję **Pola niestandardowe** i kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Dodaj pole**.

4. W oknie **Dodaj pole** określ nazwę pola niestandardowego, które będzie wyświetlane we właściwościach sprzętu.

   Możesz utworzyć kilka pól niestandardowych z unikatowymi nazwami.

5. Kliknij **OK**.

Dodane pola niestandardowe są wyświetlane w sekcji **Pola niestandardowe** właściwości sprzętu. Możesz użyć pół niestandardowych do dostarczenia określonych informacji o urządzeniach. Na przykład, to może być wewnętrzny numer zamówienia dla zakupu sprzętu.

Licencjonowanie

Ta sekcja zawiera informacje dotyczące ogólnych zasad związanych z licencjonowaniem Kaspersky Security Center 15.1.

Zdarzenia przekroczenia limitu licencji

Kaspersky Security Center pozwala uzyskać informacje o zdarzeniach, gdy pewne limity licencji zostaną przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich.

Istotność takich zdarzeń, gdy limity licencji zostaną przekroczone, jest definiowana zgodnie z następującymi regułami:

- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją mieści się w 90% do 100% całkowitej liczby jednostek objętych licencją, istotność publikowanego zdarzenia to **Informacja**.
- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją mieści się w 100% do 110% całkowitej liczby jednostek objętych licencją, publikowane zdarzenie posiada istotność: **Ostrzeżenie**.
- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją przekracza 110% całkowitej liczby jednostek objętych licencją, istotność publikowanego zdarzenia to **Zdarzenie krytyczne**.

Informacje o licencjonowaniu

Ta sekcja zawiera informacje o licencjonowaniu aplikacji firmy Kaspersky zarządzanej za pośrednictwem Kaspersky Security Center.

Informacje o licencji

Licencja to czasowo ograniczone prawo do korzystania z Kaspersky Security Center nadane zgodnie z warunkami Umowy licencyjnej (Umowa licencyjna użytkownika końcowego).

Zakres świadczonych usług oraz okres ważności zależą od licencji do korzystania z aplikacji.

Dostępne są następujące typy licencji:

- *Wersja próbna*

  Darmowa licencja udostępniana w celu zapoznania się z aplikacją. Licencja testowa ma zazwyczaj krótki okres ważności.

  Jeśli licencja testowa wygaśnie, wszystkie funkcje Kaspersky Security Center zostają wyłączone. Aby kontynuować korzystanie z aplikacji, należy zakupić licencję komercyjną.

  Z aplikacji można korzystać w ramach licencji próbnej tylko przez jeden okres próbny.

- *Wersja komercyjna*

  Płatna licencja.

  Po wygaśnięciu licencji komercyjnej kluczowe funkcje aplikacji zostają wyłączone. Aby kontynuować korzystanie z Kaspersky Security Center, musisz odnowić swoją licencję komercyjną. Po wygaśnięciu licencji komercyjnej nie można kontynuować korzystania z aplikacji i należy ją usunąć z urządzenia.

  Zalecamy odnowienie licencji przed jej wygaśnięciem, aby zapewnić stałą ochronę przed wszystkimi zagrożeniami.

Informacje o Umowie licencyjnej użytkownika końcowego

Umowa licencyjna użytkownika końcowego to wiążąca umowa prawna zawierana pomiędzy Tobą a firmą AO Kaspersky Lab, która określa zasady korzystania z zakupionej aplikacji.

Przed rozpoczęciem korzystania z aplikacji uważnie przeczytaj Umowę licencyjną.

Program Kaspersky Security Center i jego komponenty, na przykład, Agent sieciowy, ma swoją własną Umowę licencyjną.

Z warunkami Umowy licencyjnej dla Kaspersky Security Center można zapoznać się, korzystając z następujących metod:

- Podczas instalacji Kaspersky Security Center.
- W dokumencie license.txt, znajdującym się w pakiecie dystrybucyjnym Kaspersky Security Center.
- W dokumencie license.txt, znajdującym się w folderze instalacyjnym Kaspersky Security Center.
- Pobierając plik license.txt ze strony Kaspersky.

Warunki Umowy licencyjnej dla Agenta sieciowego dla systemu Windows, Agenta sieciowego dla systemu Mac, Agenta sieciowego dla systemu Linux można przejrzeć przy użyciu następujących metod:

- Podczas pobierania pakietu dystrybucyjnego Agenta sieciowego z serwerów sieciowych Kaspersky.
- Podczas instalacji Agenta sieciowego dla systemu Windows, Agenta sieciowego dla systemu Mac, Agenta sieciowego dla systemu Linux.
- Otwierając dokument license.txt znajdujący się w pakiecie dystrybucyjnym Agenta sieciowego dla systemu Windows, Agenta sieciowego dla systemu Mac, Agenta sieciowego dla systemu Linux.

- Otwierając dokument license.txt znajdujący się w folderze instalacyjnym Agenta sieciowego dla systemu Windows, Agenta sieciowego dla systemu Mac, Agenta sieciowego dla systemu Linux.
- Pobierając plik license.txt ze strony Kaspersky.

Akceptujesz warunki Umowy licencyjnej użytkownika końcowego, zaznaczając odpowiednią opcję podczas instalacji aplikacji. Jeśli nie akceptujesz warunków Umowy licencyjnej, anuluj instalację aplikacji i nie używaj aplikacji.

Informacje o certyfikacie licencji

Certyfikat licencyjny to dokument, który otrzymujesz wraz z plikiem klucza lub kodem aktywacyjnym.

Certyfikat licencji zawiera następujące informacje o dostarczonej licencji:

- ID licencji lub numer zamówienia
- Informacje o użytkowniku, który otrzymał licencję
- Informacje o aplikacji, która może być aktywowana za pomocą zakupionej licencji
- Ograniczenie liczby jednostek licencyjnych (np. urządzeń, na których może być używana aplikacja na podstawie dostarczonej licencji)
- Data rozpoczęcia okresu ważności licencji
- Data wygaśnięcia licencji lub okres licencji
- Typ licencji

Informacje o kluczu licencyjnym

Klucz licencyjny jest to sekwencja bitów, które możesz zastosować w celu aktywacji, a następnie użyć aplikacji zgodnie z warunkami Umowy licencyjnej. Klucze licencyjne są generowane przez specjalistów z Kaspersky.

Możesz dodać klucz licencyjny do aplikacji, korzystając z następujących metod: stosując *plik klucza* lub wprowadzając *kod aktywacyjny*. Po dodaniu klucza licencyjnego do aplikacji jest on wyświetlany w interfejsie aplikacji jako unikatowa sekwencja alfanumeryczna.

Klucz licencyjny może zostać zablokowany przez Kaspersky w przypadku naruszenia warunków Umowy licencyjnej. Jeśli klucz licencyjny został zablokowany, aby móc korzystać z aplikacji, musisz dodać inny klucz.

Klucz licencyjny musi być aktywny lub dodatkowy (lub zapasowy).

Aktywny klucz licencyjny to klucz licencyjny, który jest aktualnie używany przez aplikację. Aktywny klucz licencyjny może zostać dodany dla licencji testowej lub komercyjnej. Aplikacja nie może posiadać więcej niż jednego aktywnego klucza licencyjnego.

Dodatkowy (lub zapasowy) klucz licencyjny to klucz licencyjny, który upoważnia użytkownika do korzystania z aplikacji, ale nie jest aktualnie w użyciu. Dodatkowy klucz licencyjny staje się aktywny automatycznie po wygaśnięciu licencji skojarzonej z bieżącym aktywnym kluczem licencyjnym. Dodatkowy klucz licencyjny może zostać dodany tylko wtedy, gdy aktywny klucz licencyjny został już dodany.

Klucz licencyjny dla licencji testowej można dodać tylko jako aktywny klucz licencyjny. Klucz licencyjny dla licencji testowej nie może zostać dodany jako dodatkowy klucz licencyjny.

Informacje o pliku klucza

Plik klucza to plik z rozszerzeniem .key, dostarczony przez firmę Kaspersky. Pliki kluczy zostały zaprojektowane do aktywowania aplikacji poprzez dodanie klucza licencyjnego.

Plik klucza otrzymasz na adres e-mail, który określiłeś podczas zakupu Kaspersky Security Center lub po zamówieniu wersji testowej Kaspersky Security Center.

Aby aktywować aplikację przy użyciu pliku klucza, nie ma konieczności nawiązywania połączenia z serwerami aktywacji Kaspersky.

W sytuacji przypadkowego usunięcia pliku klucza istnieje możliwość jego odzyskania. Plik klucza może być niezbędny, na przykład, do zarejestrowania konta Kaspersky CompanyAccount.

W celu odzyskania pliku klucza, należy wykonać jedną z poniższych czynności:

- Skontaktuj się ze sprzedawcą licencji.
- Uzyskaj plik klucza poprzez stronę internetową Kaspersky, korzystając z dostępnego kodu aktywacyjnego.
- Eksportuj plik klucza licencyjnego z innego Serwera administracyjnego.

Informacje o subskrypcji

Subskrypcja na Kaspersky Security Center jest to zamówienie aplikacji z wybranymi ustawieniami (data wygaśnięcia subskrypcji, liczba chronionych urządzeń). Możesz zarejestrować swoją subskrypcję na Kaspersky Security Center u swojego dostawcy usługi (na przykład, dostawcy internetu). Subskrypcja może być odnawiana ręcznie lub automatycznie. Istnieje również możliwość jej anulowania.

Subskrypcja może być ograniczona (na przykład, na jeden rok) lub nieograniczona (bez daty wygaśnięcia). Aby możliwe było kontynuowanie korzystania z Kaspersky Security Center po wygaśnięciu ograniczonej subskrypcji, należy ją odnowić. Nieograniczona subskrypcja jest odnawiana automatycznie, jeśli została opłacona u dostawcy usług w odpowiednim terminie.

Po wygaśnięciu ograniczonej subskrypcji, może zostać zaoferowany okres karencji na odnowienie subskrypcji, w trakcie którego aplikacja będzie dalej działała. Dostępność i czas trwania okresu karencji są definiowane przez dostawcę usługi.

Aby używać Kaspersky Security Center z subskrypcją, należy wprowadzić kod aktywacyjny otrzymany od dostawcy usługi.

Możesz zastosować dla Kaspersky Security Center inny kod aktywacyjny dopiero wtedy, gdy Twoja subskrypcja wygaśnie lub gdy ją anulujesz.

W zależności od dostawcy usługi, zestaw możliwych działań do zarządzania subskrypcją może się różnić. Dostawca usługi może nie zaoferować okresu karencji na odnowienie subskrypcji i wówczas aplikacja przestanie działać.

Kody aktywacyjne zakupione dla subskrypcji nie mogą zostać użyte do aktywowania wcześniejszych wersji Kaspersky Security Center.

Jeśli korzystasz z aplikacji z subskrypcją, Kaspersky Security Center automatycznie próbuje uzyskać dostęp do serwera aktywacji w określonych przedziałach czasu, aż do wygaśnięcia subskrypcji. Zapewnia to synchronizację informacji o subskrypcji z serwerem aktywacji. Jeżeli dostęp do serwera za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Możesz odnowić swoją subskrypcję na stronie dostawcy usługi.

Możesz zaktualizować informacje o subskrypcji ręcznie, bez czekania, aż Kaspersky Security Center uzyska dostęp do serwera aktywacji. Może to być na przykład przydatne przy zmianie ustawień subskrypcji.

Ręczna aktualizacja informacji o subskrypcji:

1. Z drzewa konsoli wybierz folder **Licencje Kaspersky**.
2. Kliknij opcję **Dodatkowe działania** i z listy rozwijanej wybierz opcję **Synchronizuj ustawienia subskrypcji z serwerem licencjonowania**.

Informacje o subskrypcji są aktualizowane na serwerze aktywacyjnym.

Informacje o kodzie aktywacyjnym

Kod aktywacyjny to unikatowa sekwencja 20 znaków alfanumerycznych. Możesz wprowadzić kod aktywacyjny w celu dodania klucza licencyjnego aktywującego Kaspersky Security Center. Kod aktywacyjny otrzymasz na adres e-mail, który określiłeś podczas składania zamówienia, po zakupieniu Kaspersky Security Center lub po zamówieniu wersji testowej Kaspersky Security Center.

Aby aktywować aplikację za pomocą kodu aktywacyjnego, potrzebny jest dostęp do internetu w celu nawiązania połączenia z serwerami aktywacji Kaspersky. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS.

Jeśli aplikacja była aktywowana przy użyciu kodu aktywacyjnego, w niektórych przypadkach aplikacja wysyła regularne żądania do serwerów aktywacji Kaspersky w celu sprawdzenia bieżącego stanu klucza licencyjnego. Aby możliwe było wysyłanie żądań, należy zapewnić aplikacji dostęp do internetu.

Jeśli zgubiłeś kod aktywacyjny po zainstalowaniu aplikacji, skontaktuj się z partnerem Kaspersky, od którego zakupiłeś licencję.

Nie można używać plików kluczy do aktywacji zarządzanych aplikacji; akceptowane są tylko kody aktywacyjne.

Wycofanie zgody z Umową Licencyjną Użytkownika Końcowego

Jeśli decydujesz się zatrzymać ochronę swoich urządzeń klienckich, możesz odinstalować zarządzane aplikacje firmy Kaspersky i anulować swoją Umowę licencyjną użytkownika końcowego dla tych aplikacji.

W celu anulowania Umowy licencyjnej użytkownika końcowego dla zarządzanych aplikacji Kaspersky:

1. W drzewie konsoli wybierz **Serwer administracyjny → Zaawansowane → Zaakceptowane Umowy licencyjne**.

   Wyświetlana jest lista Umów licencyjnych użytkownika końcowego, zaakceptowanych po utworzeniu pakietów instalacyjnych, w momencie bezproblemowej instalacji aktualizacji lub po wdrożeniu Kaspersky Security for Mobile.

2. Z listy wybierz Umowę licencyjną użytkownika końcowego, którą chcesz anulować.

   Możesz sprawdzić następujące właściwości Umowy licencyjnej użytkownika końcowego:

   - Datę zaakceptowania Umowy licencyjnej użytkownika końcowego.
   - Nazwę użytkownika, który zaakceptował Umowę licencyjną użytkownika końcowego.
   - Odnośnik do warunków Umowy licencyjnej użytkownika końcowego.
   - Listy obiektów, które są powiązane z Umową licencyjną użytkownika końcowego: nazwy pakietów instalacyjnych, nazwy aktualizacji typu seamless, nazwy aplikacji mobilnych.

3. Kliknij przycisk **Wycofaj Umowę licencyjną użytkownika końcowego**.

   W otwartym oknie zostanie wyświetlona informacja, że musisz odinstalować aplikację firmy Kaspersky odpowiadającą Umowie licencyjnej użytkownika końcowego.

4. Kliknij przycisk, aby potwierdzić wycofanie.

   Kaspersky Security Center sprawdzi, czy pakiety instalacyjne (odpowiadające zarządzanej aplikacji firmy Kaspersky, której Umowę licencyjną użytkownika końcowego chcesz anulować) są odinstalowane.

   Możesz anulować tylko Umowę licencyjną użytkownika końcowego dla zarządzanej aplikacji firmy Kaspersky, której pakiety instalacyjne są usuwane.

Umowa licencyjna użytkownika końcowego zostanie wycofana. Nie jest wyświetlana na liście Umów licencyjnych w sekcji **Serwer administracyjny → Zaawansowane → Zaakceptowane Umowy licencyjne**. Nie możesz chronić urządzeń klienckich przy pomocy aplikacji firmy Kaspersky, której Umowę licencyjną użytkownika końcowego wycofałeś.

Informacje o przekazywaniu danych

Dane przesyłane do firm trzecich

Jeśli korzystasz z funkcji Zarządzania urządzeniami mobilnymi Oprogramowania, do czasowego dostarczenia poleceń na urządzenia działające pod kontrolą systemu operacyjnego Android poprzez mechanizm powiadomień push używana jest usługa Google Firebase Cloud Messaging. Jeśli Użytkownik skonfigurował użycie usługi Google Firebase Cloud Messaging, Użytkownik akceptuje dostarczenie następujących informacji do usługi Google Firebase Cloud Messaging w trybie automatycznym: identyfikator instalacji aplikacji Kaspersky Endpoint Security for Android, do której musi zostać wysłane powiadomienie push.

Aby zapobiec wymianie informacji z usługą Google Firebase Cloud Messaging, Użytkownik musi wycofać ustawienia korzystania z usługi Google Firebase Cloud Messaging do wartości fabrycznych.

Jeśli korzystasz z funkcji Zarządzania urządzeniami mobilnymi Oprogramowania, do czasowego dostarczenia poleceń na urządzenia działające pod kontrolą systemu operacyjnego iOS poprzez mechanizm powiadomień push używana jest usługa Apple Push Notification Service (APNs). Jeśli Użytkownik zainstalował certyfikat APNs na serwerze iOS MDM, utworzył profil iOS MDM ze zbiorem ustawień do podłączenia urządzeń mobilnych iOS z Oprogramowaniem i zainstalował ten profil na urządzeniach mobilnych, Użytkownik wyraża zgodę na dostarczenie następujących informacji do APNs w trybie automatycznym:

- Token—push token urządzenia. Serwer używa tego tokena podczas wysyłania powiadomień push do urządzenia.
- PushMagic—ciąg znaków, który musi zostać zawarty w powiadomieniu push. Ta wartość ciągu znaków jest generowana przez urządzenie.

Dane przetwarzane lokalnie

Kaspersky Security Center służy do scentralizowanego wykonywania podstawowych zadań dotyczących administracji i zarządzania w sieci firmy. Kaspersky Security Center zapewnia administratorowi dostęp do szczegółowych informacji dotyczących poziomu ochrony sieci organizacji; Kaspersky Security Center umożliwia administratorowi skonfigurowanie wszystkich składników ochrony opartych o aplikacje Kaspersky. Kaspersky Security Center wykonuje następujące główne funkcje:

- Wykrywanie urządzeń i ich użytkowników w sieci organizacji
- Tworzenie hierarchii grup administracyjnych dla zarządzania urządzeniem
- Instalowanie aplikacji firmy Kaspersky na urządzeniach
- Zarządzanie ustawieniami i zadaniami zainstalowanych aplikacji
- Zarządzanie aktualizacjami dla aplikacji firmy Kaspersky oraz aplikacji firm trzecich, a także wyszukiwanie i eliminowanie luk
- Aktywowanie aplikacji firmy Kaspersky na urządzeniach
- Zarządzanie kontami użytkowników
- Przeglądanie informacji o działaniu aplikacji firmy Kaspersky na urządzeniach
- Przeglądanie raportów

Aby program Kaspersky Security Center mógł wykonywać główne funkcje, może otrzymywać, przechowywać i przetwarzać następujące informacje:

- Informacje o urządzeniach w sieci organizacji uzyskane poprzez przeszukiwanie domeny Windows, kontrolerów domeny Active Directory lub Samba lub poprzez skanowanie przedziałów IP. Serwer administracyjny pobiera dane samodzielnie lub otrzymuje dane od Agenta sieciowego działającego jako punkt dystrybucji.
- Informacje z Active Directory i Samby o jednostkach organizacyjnych, domenach, użytkownikach i grupach. Serwer administracyjny pobiera dane samodzielnie lub otrzymuje dane od Agenta sieciowego działającego jako punkt dystrybucji.

- Szczegóły dotyczące zarządzanych urządzeń. Agent sieciowy przesyła dane wymienione poniżej z urządzenia na Serwer administracyjny. Użytkownik wprowadza wyświetlaną nazwę oraz opis urządzenia w interfejsie Konsoli administracyjnej lub w interfejsie Kaspersky Security Center Web Console:

    - Specyfikacje techniczne zarządzanego urządzenia i jego komponenty wymagane do identyfikacji urządzenia: wyświetlana nazwa i opis urządzenia, typ i nazwa domeny Windows, nazwa urządzenia w środowisku Windows, domena DNS i nazwa DNS, adres IPv4, adres IPv6, lokalizacja sieci, adres MAC, numer seryjny, typ systemu operacyjnego, czy urządzenie to maszyna wirtualna wraz z typem hipernadzorcy oraz czy urządzenie jest dynamiczną maszyną wirtualną jako część VDI.

    - Inne specyfikacje zarządzanych urządzeń i ich komponenty wymagane do audytu zarządzanych urządzeń oraz do podejmowania decyzji odnośnie tego, czy określone poprawki i aktualizacje są stosowane: stan Agenta Windows Update (WUA), architektura systemu operacyjnego, producent systemu operacyjnego, numer kompilacji systemu operacyjnego, identyfikator publikacji systemu operacyjnego, folder lokalizacyjny, jeśli urządzenie jest maszyną wirtualną—typ maszyny wirtualnej; nazwa wirtualnego Serwera administracyjnego, który zarządza urządzeniem; dane urządzenia w chmurze (region w chmurze, VPC, strefa dostępności w chmurze, podsieć w chmurze, strefa umieszczenia w chmurze).

    - Szczegóły dotyczące działań na zarządzanych urządzeniach: data i godzina ostatniej aktualizacji, czas, gdy urządzenie było ostatnio widoczne w sieci, stan oczekiwania na ponowne uruchomienie oraz czas, gdy urządzenie było włączone.

    - Szczegóły kont użytkownika na urządzeniu i sesji ich pracy.

- Dane uzyskane podczas zdalnej diagnostyki na zarządzanym urządzeniu: pliki śledzenia, informacje o systemie, szczegóły aplikacji Kaspersky zainstalowanych na urządzeniu, pliki zrzutów, dzienniki zdarzeń, wyniki uruchomienia skryptów diagnostycznych otrzymane od pomocy technicznej Kaspersky.

- Statystyki działania punktu dystrybucji, jeśli urządzenie jest punktem dystrybucji. Agent sieciowy przesyła dane z urządzenia na Serwer administracyjny.

- Ustawienia punktu dystrybucji wprowadzone przez Użytkownika w Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console.

- Dane niezbędne do nawiązania połączenia między urządzeniami mobilnymi a Serwerem administracyjnym: certyfikat, port połączenia urządzenia mobilnego, adres połączenia Serwera administracyjnego. Użytkownik wprowadza dane w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.

- Szczegóły urządzeń mobilnych przesyłane przy użyciu protokołu iOS MDM. Dane wymienione poniżej są przesyłane z urządzenia mobilnego na Serwer administracyjny:

    - Specyfikacje techniczne urządzenia mobilnego i jego składników wymagane do identyfikacji urządzenia: nazwa urządzenia, model, nazwa systemu operacyjnego, numer kompilacji systemu operacyjnego, numer modelu urządzenia, numer IMEI, UDID, MEID, numer seryjny, ilość pamięci, wersja oprogramowania firmware modemu, adres MAC Bluetooth, adres MAC Wi-Fi i szczegóły karty SIM (identyfikator ICCID jako część identyfikatora karty SIM).

    - Szczegóły dotyczące sieci komórkowej używanej przez zarządzane urządzenie: typ sieci komórkowej, nazwa aktualnie używanej sieci komórkowej, nazwa domowej sieci komórkowej, wersja ustawień operatora sieci mobilnej, stan roamingu połączeń głosowych i stan roamingu danych, kod kraju sieci domowej, kod kraju zamieszkania, kod kraju aktualnie używanej sieci i poziom szyfrowania.

    - Ustawienia zabezpieczeń urządzenia mobilnego: użycie hasła i jego zgodność z ustawieniami zasady, lista profili konfiguracyjnych i profili informacyjnych używanych do zainstalowania aplikacji firm trzecich.

    - Data ostatniej synchronizacji z Serwerem administracyjnym i stan zarządzania urządzeniem.

- Szczegóły aplikacji Kaspersky zainstalowanych na urządzeniu. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego:
  - Ustawienia aplikacji firmy Kaspersky zainstalowanych na zarządzanym urządzeniu: nazwa i wersja aplikacji firmy Kaspersky, stan ochrony w czasie rzeczywistym, data i godzina ostatniego skanowania, liczba wykrytych zagrożeń, liczba obiektów, których wyleczenie się nie powiodło, dostępność i stan komponentów aplikacji, godzina ostatniej aktualizacji i wersja antywirusowych baz danych, szczegóły dotyczące zadań i ustawień aplikacji Kaspersky, informacje o aktywnym i zapasowym kluczu licencyjnym, data i identyfikator instalacji aplikacji.
  - Statystyki działania aplikacji: zdarzenia dotyczące zmian w stanie komponentów aplikacji Kaspersky na zarządzanym urządzeniu i wykonywanie zadań zainicjowanych przez komponenty aplikacji.
  - Stan urządzenia zdefiniowany przez aplikację Kaspersky.
  - Znaczniki przypisane przez aplikację Kaspersky.
  - Zestaw zainstalowanych i stosowanych aktualizacji dla aplikacji firmy Kaspersky.
- Dane znajdujące się w zdarzeniach z komponentów Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky. Agent sieciowy przesyła dane z urządzenia na Serwer administracyjny.
- Dane niezbędne do integracji Kaspersky Security Center z systemem SIEM w celu eksportowania zdarzeń. Użytkownik wprowadza dane w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
- Ustawienia komponentów Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky, przedstawionych w zasadach i profilach zasad. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.
- Ustawienia zadania komponentów Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.
- Dane przetwarzane przez funkcję Zarządzanie lukami i poprawkami. Agent sieciowy przesyła dane wymienione poniżej z urządzenia na Serwer administracyjny:
  - Szczegóły dotyczące aplikacji i poprawek zainstalowanych na zarządzanych urządzeniach (Rejestr aplikacji).
  - Informacje o sprzęcie wykrytym na zarządzanych urządzeniach (Rejestr sprzętu).

    Jeżeli Agent sieciowy jest zainstalowany na urządzeniu z systemem Windows, wysyła on do Serwera administracyjnego następujące informacje o sprzęcie urządzenia:
    - Pamięć RAM
    - Urządzenia pamięci masowej
    - Płyta główna
    - Procesor
    - Karty sieciowe
    - Monitory

- Karta graficzna
- Karta dźwiękowa

Jeżeli Agent sieciowy jest zainstalowany na urządzeniu z systemem Linux lub macOS, wysyła on do Serwera administracyjnego następujące informacje o sprzęcie urządzenia, jeżeli informacje te są dostarczane przez system operacyjny:

- Całkowita ilość pamięci RAM
- Całkowita pojemność urządzeń pamięci masowej
- Płyta główna
- Procesor
- Karty sieciowe

- Szczegóły dotyczące luk w oprogramowaniu innej firmy wykrytych na zarządzanych urządzeniach.
- Szczegóły dotyczące aktualizacji dostępnych dla aplikacji innych firm, zainstalowanych na zarządzanych urządzeniach.
- Szczegóły dotyczące aktualizacji firmy Microsoft, wykrytych przez funkcję WSUS.
- Lista aktualizacji firmy Microsoft, wykrytych przez funkcję WSUS, która musi zostać zainstalowana na urządzeniu.

- Dane wymagane do pobrania aktualizacji na izolowanym serwerze administracyjnym w celu naprawienia luk w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach. Użytkownik wprowadza i przesyła dane za pomocą narzędzia klscflag serwera administracyjnego.
- Dane niezbędne do pracy Kaspersky Security Center ze środowiskami chmury (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud). Użytkownik wprowadza dane w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
- Kategorie użytkownika dla aplikacji. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.
- Szczegóły plików wykonywalnych wykrytych na zarządzanych urządzeniach przez funkcję Kontroli aplikacji. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.
- Szczegóły dotyczące plików w Kopii zapasowej. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.
- Szczegóły dotyczące plików w Kwarantannie. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.
- Szczegóły dotyczące plików, o które poprosili specjaliści z Kaspersky, w celu przeprowadzenia szczegółowej analizy. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Szczegóły dotyczące stanu i wyzwolenia reguł Adaptacyjnej kontroli anomalii. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Szczegóły dotyczące urządzeń zewnętrznych (jednostki pamięci, informacje o narzędziach do przenoszenia danych, informacje o narzędziach do drukowania oraz magistrale połączeń), zainstalowane lub podłączone do zarządzanego urządzenia i wykryte przez funkcję Kontroli urządzeń. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Informacje o zaszyfrowanych urządzeniach i stanie szyfrowania. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego.

- Szczegóły dotyczące błędów szyfrowania danych na urządzeniach, wykonane przy użyciu funkcji Szyfrowanie danych z aplikacji firmy Kaspersky. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Lista zarządzanych programowalnych sterowników logicznych (PLC). Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Dane wymagane do utworzenia łańcucha rozprzestrzeniania się zagrożeń. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Informacje o próbach uzyskania przez pracowników organizacji dostępu do usług w chmurze. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Dane wymagane do integracji Kaspersky Security Center z usługą Kaspersky Managed Detection and Response (dedykowana wtyczka musi być zainstalowana dla Kaspersky Security Center Web Console): token inicjujący integrację, token integracji i token sesji użytkownika. Użytkownik wprowadza token inicjujący integrację w interfejsie konsoli Kaspersky Security Center Web Console. Usługa Kaspersky MDR przesyła token integracji i token sesji użytkownika za pośrednictwem dedykowanej wtyczki.

- Szczegóły wprowadzonych kodów aktywacyjnych lub określonych plików kluczy. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Konta użytkowników: nazwa, opis, imię i nazwisko, adres e-mail, główny numer telefonu, hasło, tajny klucz wygenerowany przez Serwer administracyjny oraz hasło jednorazowe do weryfikacji dwuetapowej. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Dane, których Identity and Access Manager potrzebuje do scentralizowanego uwierzytelniania i dostarczania technologii Single Sign-on (SSO) między aplikacjami Kaspersky zintegrowanymi z Kaspersky Security Center: ustawienia instalacji i konfiguracji Identity and Access Manager, sesja użytkownika Identity and Access Manager, tokeny Identity and Access Manager, stany programu klienckiego i stany serwera zasobu. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Historia rewizji zarządzanych obiektów. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Adres IP urządzenia, na którym użytkownik utworzył rewizję. Adres IP jest definiowany automatycznie przez Serwer administracyjny.

- Rejestr usuniętych zarządzanych obiektów. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Pakiety instalacyjne utworzone z pliku, a także ustawienia instalacji. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.
- Dane wymagane do wyświetlania ogłoszeń z Kaspersky w Kaspersky Security Center Web Console. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.
- Dane wymagane do działania wtyczek zarządzanych aplikacji w konsoli Kaspersky Security Center Web Console i zapisywane przez wtyczki w bazie danych Serwera administracyjnego podczas ich rutynowego działania. Opis i sposoby podawania danych znajdują się w plikach pomocy odpowiedniej aplikacji.
- Ustawienia użytkownika Kaspersky Security Center Web Console: wersja językowa oraz temat interfejsu, ustawienia wyświetlania panelu Monitorowanie, informacje o stanie powiadomień (Przeczytane / Nieprzeczytane), stan kolumn w arkuszach kalkulacyjnych (Pokaż / Ukryj), postęp trybu Uczenie. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.
- Dziennik zdarzeń aplikacji Kaspersky dla komponentów Kaspersky Security Center i zarządzanej aplikacji firmy Kaspersky. Dziennik zdarzeń aplikacji Kaspersky jest przechowywany na każdym urządzeniu i nie jest nigdy przesyłany na Serwer administracyjny.
- Certyfikaty dla bezpiecznego podłączania zarządzanych urządzeń do komponentów Kaspersky Security Center. Użytkownik wprowadza i przesyła dane za pomocą narzędzia klsetsrvcert serwera administracyjnego.
- Certyfikaty potwierdzające zaufanie do wewnętrznych zasobów sieciowych organizacji. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.
- Dane wymagane do działania Kaspersky Security Center w środowiskach chmury, takich jak Amazon Web Services (AWS), Microsoft Azure, Google Cloud i Yandex.Cloud. Serwer administracyjny otrzymuje dane z maszyny wirtualnej, na której działa.
- Informacja o akceptacji przez Użytkownika warunków umów prawnych z Kaspersky.
- Dane serwera administracyjnego, które użytkownik wprowadza w następujących składnikach:
  - Konsola administracyjna
  - Kaspersky Security Center Web Console
  - Terminal wiersza polecenia podczas korzystania z narzędzia klscflag
  - Składniki współpracujące z serwerem administracyjnym za pośrednictwem obiektów automatyzacji klakaut i Kaspersky Security Center OpenAPI
- Wszelkie dane, jakie Użytkownik wprowadza w Konsoli administracyjnej lub interfejsie konsoli Kaspersky Security Center Web Console.

Dane wymienione powyżej mogą zostać przedstawione w Kaspersky Security Center, jeśli stosowana jest jedna z następujących metod:

- Użytkownik wprowadza dane w interfejsie następujących składników:
  - Konsola administracyjna
  - Kaspersky Security Center Web Console

- Terminal wiersza polecenia podczas korzystania z narzędzia klscflag
- Składniki współpracujące z serwerem administracyjnym za pośrednictwem obiektów automatyzacji klakaut i Kaspersky Security Center OpenAPI

- Agent sieciowy automatycznie pobiera dane z urządzenia i przesyła je na Serwer administracyjny.
- Agent sieciowy pobiera dane otrzymane przez zarządzaną aplikację firmy Kaspersky i przesyła je na Serwer administracyjny. Listy danych przetwarzanych przez zarządzane aplikacje firmy Kaspersky są dostarczane w plikach pomocy dla odpowiednich aplikacji.
- Serwer administracyjny samodzielnie pobiera informacje o urządzeniach sieciowych lub otrzymuje informacje od Agenta sieciowego działającego jako punkt dystrybucji.
- Dane są przesyłane z urządzenia mobilnego do Serwera administracyjnego przy użyciu protokołu iOS MDM.

Wymienione dane są przechowywane w bazie danych Serwera administracyjnego. Nazwy użytkowników i hasła są przechowywane w postaci zaszyfrowanej.

Wszystkie wymienione dane mogą być przesyłane do Kaspersky tylko poprzez pliki zrzutów, pliki śledzenia lub pliki raportów komponentów Kaspersky Security Center, w tym pliki raportów utworzone przez instalatory i narzędzia.

Pliki zrzutów, pliki śledzenia i pliki raportów komponentów Kaspersky Security Center zawierają losowe dane Serwera administracyjnego, Agenta sieciowego, Konsoli administracyjnej, serwera iOS MDM oraz Kaspersky Security Center Web Console. Te pliki mogą zawierać szczegóły osobiste oraz dane wrażliwe. Pliki zrzutów, pliki śledzenia oraz pliki raportów na urządzeniu w postaci niezaszyfrowanej. Pliki zrzutów, pliki śledzenia i pliki raportów nie są przesyłane do Kaspersky automatycznie; jednakże administrator może przesyłać dane do Kaspersky ręcznie na prośbę pomocy technicznej, aby rozwiązać problemy związane z działaniem Kaspersky Security Center.

Klikając odnośniki w Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console, Użytkownik wyraża zgodę na automatyczne przesyłanie następujących danych:

- Kod Kaspersky Security Center
- Wersja Kaspersky Security Center
- Lokalizacja Kaspersky Security Center
- Identyfikator licencji
- Typ licencji
- Czy licencja została zakupiona u partnera

Lista danych dostarczonych za pośrednictwem odnośników zależy od celu i lokalizacji odnośnika.

Firma Kaspersky wykorzystuje uzyskane dane tylko jako ogólne statystyki. Ogólne statystyki są generowane automatycznie z otrzymanych informacji i nie zawierają żadnych danych osobowych ani poufnych informacji. Jak tylko nowe dane zostaną zebrane, poprzednie dane zostaną usunięte (raz na rok). Statystyki podsumowujące są przechowywane cały czas.

Firma Kaspersky chroni wszelkie zebrane informacje zgodnie z prawem oraz obowiązującymi przepisami stosowanymi w firmie Kaspersky. Dane są przesyłane za pośrednictwem bezpiecznego kanału.

Opcje licencjonowania Kaspersky Security Center

Kaspersky Security Center może pracować w następujących trybach:

- **Brak licencji (podstawowa funkcjonalność)**

  Kaspersky Security Center działa w tym trybie przed aktywacją aplikacji lub po wygaśnięciu licencji komercyjnej. Kaspersky Security Center z obsługą podstawowej funkcjonalności Konsoli administracyjnej jest dostarczany jako część aplikacji Kaspersky do ochrony sieci firmowych. Można ją również pobrać ze strony firmy Kaspersky.

- **Licencja komercyjna**

  Jeśli potrzebujesz dodatkowej funkcjonalności, która nie jest zawarta w podstawowych funkcjach Konsoli administracyjnej, musisz zakupić licencję komercyjną.

  Podczas dodawania klucza licencyjnego w oknie właściwości Serwera administracyjnego upewnij się, że dodasz klucz licencyjny, który umożliwia użycie Kaspersky Security Center. Możesz odszukać te informacje na stronie internetowej firmy Kaspersky. Każda strona internetowa rozwiązania zawiera listę aplikacji znajdujących się w rozwiązaniu. Serwer administracyjny może akceptować nieobsługiwane klucze licencyjne, na przykład klucz licencyjny dla Kaspersky Endpoint Security Cloud, ale takie klucze licencyjne nie udostępniają żadnych nowych funkcji poza podstawową funkcjonalnością Konsoli administracyjnej.

Funkcja lub właściwość	Tryb pracy Kaspersky Security Center	
	Brak licencji	Licencja komercyjna
Podstawowe funkcje Konsoli administracyjnej Dostępne są następujące funkcje: • Tworzenie wirtualnych Serwerów administracyjnych, które są używane do zarządzania siecią zdalnych biur lub organizacji klientów. • Tworzenie hierarchii grup administracyjnych w celu zarządzania określonymi urządzeniami jako pojedynczą jednostką. • Zdalna instalacja aplikacji. • Scentralizowana konfiguracja aplikacji zainstalowanych na urządzeniach klienckich. • Kontrola stanu ochrony antywirusowej firmy. • Zarządzanie rolami użytkownika. • Statystyki i raporty z działania aplikacji, a także powiadomienia o zdarzeniach krytycznych. • Scentralizowana praca z plikami przeniesionymi do Kwarantanny lub Kopii zapasowej i plikami, których przetwarzanie zostało odroczone. • Zarządzanie szyfrowaniem i ochroną danych. • Przeglądanie i modyfikowanie istniejących grup licencjonowanych aplikacji. • Wyświetlanie i ręczne modyfikowanie listy komponentów sprzętu wykrytych poprzez przeszukiwanie sieci. • Wyświetlanie listy obrazów systemów operacyjnych dostępnych do zdalnej instalacji.	✓	✓

Funkcja lub właściwość	Tryb pracy Kaspersky Security Center	
	Brak licencji	Licencja komercyjna
Zarządzanie lukami i poprawkami: podstawowa funkcjonalność Następujące zadania nie wymagają licencji komercyjnej: • Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* Za pośrednictwem tego zadania Kaspersky Security Center otrzymuje listy wykrytych luk w zabezpieczeniach i wymaganych aktualizacji dla oprogramowania firm trzecich zainstalowanego na zarządzanych urządzeniach. • Zadanie *Zainstaluj aktualizacje Windows Update* To zadanie może służyć tylko do instalowania aktualizacji usługi Windows Update. Aby skorzystać z tego zadania, musisz ręcznie określić wymagane aktualizacje w ustawieniach zadania. • Tworzenie zadania *Napraw luki* Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla programów innych firm. Aby użyć tego zadania, należy ręcznie określić poprawki użytkownika dla luk wymienionych w ustawieniach zadania.	✓	✓
Zarządzanie lukami i poprawkami: zaawansowana funkcjonalność Dostępne są następujące funkcje: • Zdalna instalacja aktualizacji oprogramowania i automatyczne naprawianie luk, zgodnie z ustalonymi przez Ciebie zasadami. • Wykorzystanie Serwera administracyjnego jako serwera Windows Server Update Services (WSUS) do dostarczania aktualizacji usług Windows Update na urządzeniach w trybie scentralizowanym i z ustaloną częstotliwością.	—	✓
Funkcja zarządzania urządzeniami mobilnymi w konsoli administracyjnej opartej na konsoli MMC Funkcja zarządzania urządzeniami mobilnymi służy do zarządzania urządzeniami mobilnymi z systemem iOS MDM i Android. Dla urządzeń iOS MDM dostępne są następujące funkcje: • Dodawanie nowych urządzeń pod zarządzaniem Kaspersky Security Center. • Tworzenie i modyfikowanie profili konfiguracyjnych oraz instalowanie profili konfiguracyjnych na urządzeniach mobilnych. • Instalowanie aplikacji na urządzeniach mobilnych za pośrednictwem App Store®, plików manifestu (.plist) lub pakietów instalacyjnych dla urządzeń mobilnych (.ipa). • Wykonywanie poleceń na urządzeniach iOS MDM, w tym blokowanie urządzeń mobilnych, resetowanie hasła urządzenia mobilnego i usuwanie wszystkich danych z urządzenia mobilnego. Dla urządzeń Android dostępne są następujące funkcje: • Dodawanie nowych urządzeń pod zarządzaniem Kaspersky Security Center. • Zarządzanie Kaspersky Endpoint Security for Android za pomocą profilu zasad. • Wykonywanie poleceń na urządzeniach. Jednostką zarządzającą funkcji Zarządzanie urządzeniami mobilnymi jest urządzenie mobilne. Urządzenie mobilne jest zarządzane po jego podłączeniu do serwera urządzeń mobilnych.	—	✓ (Klucz licencyjny musi zostać dodany do właściwości Serwera administracyjnego.)
Ochrona urządzenia mobilnego w Kaspersky Security Center Web Console Kaspersky Security Center Web Console udostępnia następujące funkcje do zarządzania urządzeniami mobilnymi z systemami Android i iOS: • Dodawanie nowych urządzeń pod zarządzaniem Kaspersky Security Center. • Zarządzanie Kaspersky Endpoint Security for Android i Kaspersky Security for iOS za pomocą profili zasad. • Wysyłanie poleceń do urządzeń mobilnych za pomocą odpowiednich protokołów i wykonywanie poleceń.	—	✓ (Klucz licencyjny musi być dodany do każdego urządzenia mobilnego.)

Funkcja lub właściwość	Tryb pracy Kaspersky Security Center	
	Brak licencji	Licencja komercyjna
Zarządzanie systemami Dostępne są następujące funkcje: • Instalacja systemów operacyjnych i aplikacji. Kaspersky Security Center umożliwia tworzenie obrazów systemów operacyjnych i instalowanie ich na urządzeniach klienckich w sieci, a także wykonywanie zdalnej instalacji aplikacji firmy Kaspersky lub innych producentów. Możesz przechwytywać obrazy systemów operacyjnych z urządzeń i przesyłać je do Serwera administracyjnego. Takie obrazy systemów operacyjnych są przechowywane na Serwerze administracyjnym w dedykowanym folderze. Obraz systemu operacyjnego odpowiedniego urządzenia może zostać przechwycony i utworzony przy użyciu zadania tworzenia pakietu instalacyjnego. Możesz użyć przechwyconych obrazów do zainstalowania ich na nowych urządzeniach w sieci, na których nie zainstalowano jeszcze systemu operacyjnego. W tym przypadku wykorzystywana jest technologia Preboot eXecution Environment (PXE). • Zarządzanie grupą licencjonowanych aplikacji. • Możliwość zdalnego połączenia z urządzeniami klienckimi poprzez komponent systemu Microsoft® Windows® o nazwie Podłączanie pulpitu zdalnego. • Nawiązywanie zdalnego połączenia z urządzeniami klienckimi poprzez udostępnianie pulpitu Windows. • Zdalne połączenie poprzez **Kaspersky Remote Desktop Session Viewer**.	—	✓
Integracja ze środowiskami chmury Kaspersky Security Center pracuje nie tylko z urządzeniami lokalnymi, ale także oferuje specjalne funkcje do pracy w środowisku chmury, takie jak Kreator konfiguracji środowiska chmury. Kaspersky Security Center działa z następującymi maszynami wirtualnymi: • Instancje Amazon EC2 • Maszyny wirtualne Microsoft Azure • Instancje maszyn wirtualnych Google Cloud • Maszyny wirtualne w chmurze Yandex.Cloud	—	✓
Eksport zdarzeń do systemów SIEM: z wykorzystaniem protokołu Syslog Korzystając z protokołu Syslog, możesz przekazywać dowolne zdarzenia, które wystąpiły na Serwerze administracyjnym Kaspersky Security Center i w aplikacjach firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Możesz go użyć do eksportowania zdarzeń do systemu SIEM.	✓	✓

Funkcje licencjonowania Kaspersky Security Center i zarządzanych aplikacji

Licencjonowanie Serwera administracyjnego i zarządzanych aplikacji posiada następujące specjalne funkcje:

- Możesz dodać klucz licencyjny lub ważny kod aktywacyjny do Serwera administracyjnego, aby aktywować Zarządzanie lukami i poprawkami, Zarządzanie urządzeniami mobilnymi lub Integracja z systemami SIEM. Niektóre funkcje Kaspersky Security Center są dostępne tylko w zależności od aktywnych plików kluczy lub ważnych kodów aktywacyjnych dodanych do Serwera administracyjnego.

- Do repozytorium Serwera administracyjnego można dodać kilka kodów aktywacyjnych i plików kluczy dla zarządzanych aplikacji.

Informacje o licencjonowaniu Kaspersky Security Center

Jeśli aktywowano jedną z licencjonowanych funkcji (na przykład, Zarządzanie urządzeniami mobilnymi) przy użyciu pliku klucza, ale chcesz też korzystać z innej licencjonowanej funkcji (na przykład, Zarządzania lukami i poprawkami), musisz kupić u swojego dostawcy usługi plik klucza, który aktywuje obie te funkcje, i musisz aktywować Serwer administracyjny przy użyciu tego pliku klucza.

Funkcje licencjonowania zarządzanych aplikacji

Licencjonowanie zarządzanych aplikacji obejmuje wdrożenie kodu aktywacyjnego lub pliku klucza automatycznie lub w inny dogodny sposób. W celu wdrożenia kodu aktywacyjnego lub pliku klucza można zastosować następujące metody:

- Automatyczne wdrażanie

  > Jeśli używasz różnych zarządzanych aplikacji i musisz rozesłać określony plik klucza lub kod aktywacyjny na urządzenia, zdecyduj się na inne sposoby wdrożenia tego kodu aktywacyjnego lub pliku klucza.

  Kaspersky Security Center umożliwia automatyczne rozesłanie dostępnych kluczy licencyjnych na urządzenia. Na przykład, trzy klucze licencyjne są przechowywane w repozytorium Serwera administracyjnego. Zaznaczyłeś pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia** dla wszystkich trzech kluczy licencyjnych. Aplikacja zabezpieczająca Kaspersky—na przykład Kaspersky Endpoint Security for Windows—jest zainstalowana na urządzeniach w organizacji. Zostanie wykryte nowe urządzenie, do którego musi być rozesłany klucz licencyjny. Aplikacja określi, na przykład, że na urządzeniu mogą zostać zastosowane dwa klucze licencyjne z repozytorium: klucz licencyjny o nazwie *Key_1* oraz klucz licencyjny o nazwie *Key_2*. Jeden z tych kluczy licencyjnych zostanie zastosowany na urządzeniu. W tym przypadku nie można przewidzieć, który z dwóch kluczy licencyjnych zostanie wdrożony na urządzeniu, ponieważ automatyczne wdrażanie kluczy licencyjnych nie oferuje administratorowi podejmowania żadnych działań.

  Podczas rozsyłania klucza licencyjnego urządzenia są zliczane dla tego klucza licencyjnego. Musisz upewnić się, że liczba urządzeń, na których klucz licencyjny został zastosowany, nie przekracza limitu określonego przez licencję. Jeśli liczba urządzeń przekracza limit określony przez licencję, wszystkie urządzenia, które nie zostały objęte licencją, otrzymają stan *Krytyczny*.

- Dodawanie pliku klucza lub kodu aktywacyjnego do pakietu instalacyjnego zarządzanej aplikacji

  Jeśli instalujesz zarządzaną aplikację przy użyciu pakietu instalacyjnego, możesz określić kod aktywacyjny lub plik klucza w tym pakiecie instalacyjnym lub w zasadzie aplikacji. Klucz licencyjny zostanie rozesłany na zarządzane urządzenia podczas kolejnej synchronizacji urządzenia z Serwerem administracyjnym.

- Wdrażanie poprzez zadanie dodaj klucz licencyjny dla zarządzanej aplikacji

  Jeśli zdecydujesz się na użycie zadania dodaj klucz licencyjny dla zarządzanej aplikacji, możesz wybrać klucz licencyjny, który musi zostać rozesłany na urządzenia, oraz wybrać urządzenia w dowolny sposób—na przykład, wybierając grupę administracyjną lub wybór urządzeń.

- Ręczne dodawanie kodu aktywacyjnego lub pliku klucza do urządzeń

Aplikacje Kaspersky. Scentralizowane wdrażanie

Ta sekcja opisuje metody zdalnej instalacji aplikacji firmy Kaspersky i ich usuwanie z urządzeń w sieci.

Przed zainstalowaniem aplikacji na urządzeniach klienckich należy upewnić się, że sprzęt i oprogramowanie tych urządzeń klienckich spełniają stosowne wymagania.

Agent sieciowy jest składnikiem umożliwiającym łączenie się Serwera administracyjnego z urządzeniami klienckimi. Dlatego też Agent sieciowy musi być zainstalowany na każdym urządzeniu klienckim, które będzie połączone ze zdalnym scentralizowanym systemem kontroli. Urządzenie, na którym jest zainstalowany Serwer administracyjny, może użyć tylko wersji serwerowej Agenta sieciowego. Ta wersja jest częścią Serwera administracyjnego, która jest z nim instalowana i usuwana. Nie ma konieczności instalowania Agenta sieciowego na tym urządzeniu.

Agent sieciowy może być instalowany lokalnie lub zdalnie podobnie jak każda inna aplikacja. Podczas scentralizowanego wdrażania aplikacji zabezpieczających poprzez Konsolę administracyjną możesz zainstalować Agenta sieciowego wraz z tymi aplikacjami zabezpieczającymi.

Agenty sieciowe mogą się różnić w zależności od aplikacji Kaspersky, z którymi pracują. W niektórych przypadkach Agent sieciowy może być instalowany tylko lokalnie (w celu uzyskania szczegółowych informacji przeczytaj dokumentację dla konkretnej aplikacji). Wystarczy tylko raz zainstalować Agenta sieciowego na urządzeniu klienckim.

Aplikacje firmy Kaspersky są zarządzane poprzez Konsolę administracyjną przy użyciu wtyczek zarządzających. Dlatego, aby mieć dostęp do interfejsu do zarządzania aplikacjami poprzez Kaspersky Security Center, na stacji roboczej administratora należy zainstalować odpowiednią wtyczkę administracyjną.

Możesz przeprowadzić zdalną instalację aplikacji ze stacji roboczej administratora w oknie głównym Kaspersky Security Center.

Aby zdalnie zainstalować oprogramowanie, musisz utworzyć zadanie zdalnej instalacji.

Utworzone zadanie zdalnej instalacji zostanie uruchomione zgodnie z jego terminarzem. Możesz przerwać instalację, ręcznie zatrzymując wykonywanie zadania.

Jeżeli zdalna instalacja aplikacji zwróci błąd, upewnij się, że spełnione są wymagania dotyczące przygotowania urządzenia.

Możesz monitorować proces zdalnej instalacji aplikacji firmy Kaspersky w sieci, korzystając z raportu ze zdalnej instalacji.

W celu uzyskania bardziej szczegółowych informacji o zarządzaniu wymienionymi aplikacjami za pośrednictwem Kaspersky Security Center zajrzyj do dokumentacji dla konkretnej aplikacji.

Zastępowanie aplikacji zabezpieczających firm trzecich

Instalacja aplikacji zabezpieczających firmy Kaspersky poprzez Kaspersky Security Center może wymagać usunięcia oprogramowania firmy trzeciej niekompatybilnego z instalowaną aplikacją. Kaspersky Security Center oferuje kilka sposobów usunięcia aplikacji firm trzecich.

Usuwanie niekompatybilnych aplikacji przy użyciu instalatora

Ta opcja jest dostępna tylko w Konsoli administracyjnej opartej na konsoli Microsoft Management Console.

Metoda instalatora dotycząca usuwania niekompatybilnych aplikacji jest obsługiwana przez różne typy instalacji. Przed zainstalowaniem aplikacji zabezpieczającej wszystkie niekompatybilne aplikacje są usuwane automatycznie, jeśli w oknie właściwości pakietu instalacyjnego tej aplikacji zabezpieczającej (sekcja **Niekompatybilne aplikacje**) wybrano opcję **Automatycznie odinstaluj niekompatybilne aplikacje**.

Usuwanie niekompatybilnych aplikacji podczas konfigurowania zdalnej instalacji aplikacji

Możesz włączyć opcję **Automatycznie odinstaluj niekompatybilne aplikacje**, gdy konfigurujesz zdalną instalację aplikacji zabezpieczającej. W Konsoli administracyjnej opartej na Microsoft Management Console (MMC) ta opcja jest dostępna w kreatorze zdalnej instalacji. W Kaspersky Security Center Web Console tę opcję można znaleźć w kreatorze wdrażania ochrony. Jeśli ta opcja jest włączona, Kaspersky Security Center usunie niekompatybilne aplikacje przed zainstalowaniem aplikacji zabezpieczającej na zarządzanym urządzeniu.

Dostępne instrukcje:

- Konsola administracyjna: Usuwanie niekompatybilnych aplikacji przy pomocy Kreatora zdalnej instalacji
- Kaspersky Security Center Web Console: Usuwanie niekompatybilnych aplikacji przed instalacją

Dezinstalowanie niekompatybilnych aplikacji przy użyciu dedykowanego zadania

Aby usunąć niekompatybilne aplikacje, użyj zadania **Zdalna dezinstalacja aplikacji**. Zadanie to powinno być uruchomione na urządzeniach przed zadaniem instalacji aplikacji zabezpieczającej. Na przykład, w zadaniu instalacji możesz wybrać opcję terminarza **Po zakończeniu wykonywania innego zadania**, gdzie inne zadanie to **Zdalna dezinstalacja aplikacji**.

Ta metoda dezinstalacji jest przydatna, jeśli instalator aplikacji zabezpieczającej nie może skutecznie usunąć niekompatybilnej aplikacji.

Instrukcje dotyczące Konsoli administracyjnej: Tworzenie zadania.

Instalowanie aplikacji przy pomocy zadania zdalnej instalacji

Kaspersky Security Center umożliwia zdalne instalowanie aplikacji na urządzeniach przy użyciu zadań zdalnej instalacji. Te zadania są tworzone i przydzielane do urządzeń za pośrednictwem dedykowanego kreatora. W celu szybkiego i łatwego przypisywania zadań do urządzeń, możesz wskazać urządzenia (maksymalnie do 1000 urządzeń) w oknie kreatora w jeden z następujących sposobów:

- **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**. W tym przypadku zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**. Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.
- **Przypisz zadanie do wyboru urządzeń**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonym wyborze. Możesz określić predefiniowany lub niestandardowy wybór, który utworzyłeś.
- **Przypisz zadanie do grupy administracyjnej**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonej grupie administracyjnej.

Aby uniknąć problemów, które mogą wystąpić podczas instalacji aplikacji na urządzeniu klienckim bez zainstalowanego Agenta sieciowego, należy postępować zgodnie z opisem procedury wymuszonego wdrożenie przy użyciu zadania zdalnej instalacji z Kaspersky Security Center.

Instalowanie aplikacji na wybranych urządzeniach

W celu zainstalowania aplikacji na wybranych urządzeniach:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania, klikając przycisk **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w węźle **Serwer administracyjny Kaspersky Security Center** wybierz **Zdalna instalacja aplikacji** jako typ zadania.

   Kreator tworzenia nowego zadania tworzy Zadanie zdalnej instalacji wybranej aplikacji dla określonych urządzeń. Nowo utworzone zadanie będzie wyświetlane w obszarze roboczym folderu **Zadania**.
3. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji, wybrana aplikacja zostanie zainstalowana na wybranych urządzeniach.

Instalowanie aplikacji na urządzeniach klienckich z grupy administracyjnej

W celu zainstalowania aplikacji na urządzeniach klienckich z grupy administracyjnej:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednią grupę administracyjną.
2. Z drzewa konsoli wybierz grupę administracyjną.
3. W obszarze roboczym grupy wybierz zakładkę **Zadania**.
4. Uruchom tworzenie zadania, klikając przycisk **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w węźle **Serwer administracyjny Kaspersky Security Center** wybierz **Zdalna instalacja aplikacji** jako typ zadania.

   Kreator tworzenia nowego zadania tworzy grupowe Zadanie zdalnej instalacji wybranej aplikacji. Nowe zadanie pojawi się w obszarze roboczym grupy administracyjnej na zakładce **Zadania**.
5. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji, wybrana aplikacja zostanie zainstalowana na urządzeniach klienckich w grupie administracyjnej.

Instalowanie aplikacji przy użyciu zasad grupy Active Directory

Kaspersky Security Center pozwala na instalowanie aplikacji Kaspersky na zarządzanych urządzeniach przy użyciu zasad grupy Active Directory. Urządzenie Serwera administracyjnego musi znajdować się w tej samej domenie co zarządzane urządzenia.

Możesz zainstalować aplikacje, korzystając z zasad grupy Active Directory jedynie przy pomocy pakietów instalacyjnych, które zawierają Agenta sieciowego.

W celu zainstalowania aplikacji przy użyciu zasad grupy Active Directory:

1. Uruchom konfigurowanie instalacji aplikacji przy użyciu kreatora zdalnej instalacji.
2. W oknie **Określanie ustawień** zadania zdalnej instalacji kreatora zdalnej instalacji wybierz opcję **Przypisz pakiet instalacyjny do zasad grupy Active Directory**.
3. W oknie **Wybierz konta w celu uzyskania dostępu do urządzeń kreatora** zdalnej instalacji wybierz opcję **Konto wymagane (Agent sieciowy nie jest używany)**.
4. Dodaj konto z uprawnieniami administratora na urządzeniu, na którym jest zainstalowany program Kaspersky Security Center, lub konto, które należy do grupy domeny Twórcy-właściciele zasad grupy.

5. Nadaj wybranemu kontu następujące uprawnienia:

    a. Przejdź do **Panel sterowania** → **Narzędzia administracyjne** i otwórz **Zarządzanie zasadami grupy**.

    b. Kliknij węzeł z żądaną domeną.

    c. Kliknij sekcję **Delegowanie**.

    d. Na liście rozwijanej **Uprawnienia** wybierz opcję **Połącz obiekty zasad grupy**.

    e. Kliknij **Dodaj**.

    f. W otwartym oknie **Wybierz Użytkownika, Komputer lub Grupę** wybierz żądane konto.

    g. Kliknij **OK**, aby zamknąć okno **Wybierz Użytkownika, Komputer lub Grupę**.

    h. Na liście **Grupy i użytkownicy** wybierz konto, które zostało dodane, a następnie kliknij **Zaawansowane** → **Zaawansowane**.

    i. Na liście **Wpisy uprawnień** kliknij dwukrotnie konto, które tyle co dodałeś.

    j. Nadaj następujące uprawnienia:

    - **Utwórz obiekty grupy**
    - **Usuń obiekty grupy**
    - **Utwórz obiekty kontenera zasad grupy**
    - **Usuń obiekty kontenera zasad grupy**

    k. Kliknij **OK**, aby zachować zmiany.

6. Określ inne ustawienia, postępując zgodnie z instrukcjami kreatora.

7. Uruchom utworzone zadanie zdalnej instalacji ręcznie lub zaczekaj na jego uruchomienie zgodne z terminarzem.

Rozpocznie się następująca sekwencja zdalnej instalacji:

1. Po uruchomieniu zadania, w każdej domenie, do której należą urządzenia klienckie z określonego zbioru, zostaną utworzone następujące obiekty:

    - Obiekt zasad grupy (GPO) o nazwie **Kaspersky_AK{GUID}**.
    - Grupa bezpieczeństwa, która odpowiada GPO. Ta grupa bezpieczeństwa zawiera urządzenia klienckie objęte zadaniem. Zawartość grupy bezpieczeństwa określa zakres GPO.

2. Kaspersky Security Center instaluje wybrane aplikacje firmy Kaspersky na urządzeniach klienckich bezpośrednio z sieciowego folderu współdzielonego KLSHARE. W folderze instalacyjnym Kaspersky Security Center zostanie utworzony pomocniczy podfolder, zawierający plik .msi potrzebny do zainstalowania aplikacji.

3. Po dodaniu nowych urządzeń do obszaru zadania, są one dodawane do grupy bezpieczeństwa podczas kolejnego uruchomienia zadania. Jeśli w harmonogramie zadań wybrana jest opcja **Uruchom pominięte zadania**, urządzenia są dodawane do grupy zabezpieczeń od razu.

4. Po usunięciu urządzeń z obszaru zadania, są one usuwane z grupy zabezpieczeń podczas kolejnego uruchomienia zadania.

5. Po usunięciu zadania z Active Directory, usuwany jest GPO, odnośnik do GPO oraz odpowiadająca mu grupa zabezpieczeń.

Jeżeli chcesz zastosować inny schemat instalacji przy użyciu Active Directory, możesz ręcznie skonfigurować żądane ustawienia. Na przykład, może to być wymagane w następujących wypadkach:

- Jeśli administrator ochrony antywirusowej nie ma uprawnień do wprowadzania zmian w Active Directory pewnych domen
- Jeśli oryginalny pakiet instalacyjny musi być przechowywany w oddzielnym zasobie sieciowym
- Jeśli konieczne jest połączenie GPO z określonymi jednostkami Active Directory

Dostępne są następujące opcje korzystania z alternatywnego scenariusza instalacji poprzez Active Directory:

- W przypadku, gdy instalacja musi być przeprowadzona bezpośrednio z folderu współdzielonego Kaspersky Security Center, we właściwościach GPO musisz określić plik msi zlokalizowany w podfolderze exec folderu pakietu instalacyjnego żądanej aplikacji.
- Jeżeli pakiet instalacyjny ma znajdować się w innym zasobie sieciowym, skopiuj do niego całą zawartość foldera exec. Jest to konieczne, gdyż oprócz pliku z rozszerzeniem .msi folder zawiera pliki konfiguracyjne wygenerowane podczas tworzenia pakietu. W celu zainstalowania aplikacji wraz z kluczem licencyjnym, skopiuj do tego folderu także plik klucza.

Instalacja zdalna aplikacji na urządzeniach z systemem macOS

Aby zainstalować aplikacje na urządzeniach z systemem macOS za pomocą zadania instalacji zdalnej:

1. Utwórz archiwum składające się z pakietu instalacyjnego i skryptu instalatora .sh.

2. Wyłącz opcję **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem** w Kreatorze tworzenia nowego zadania.

Alternatywnie możesz skorzystać z zadania **Zdalne wykonywanie skryptów**. W poniższym artykule opisano sposób konfiguracji plików dla tego zadania: Zdalna instalacja aplikacji na urządzeniach przy użyciu zadania Zdalne wykonanie skryptu.

Instalowanie aplikacji na podrzędnych Serwerach administracyjnych

W celu zainstalowania aplikacji na podrzędnych Serwerach administracyjnych:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednie podrzędne Serwery administracyjne.

2. Upewnij się, że pakiet instalacyjny dla instalowanej aplikacji znajduje się na każdym z wybranych podrzędnych Serwerów administracyjnych. Jeśli na żadnym podrzędnym Serwerze administracyjnym nie można znaleźć pakietu instalacyjnego, roześlij go przy użyciu zadania rozsyłania pakietu instalacyjnego.

3. Utwórz zadanie instalacji aplikacji na podrzędnych Serwerach administracyjnych w jeden z następujących sposobów:

   - Jeśli chcesz utworzyć zadanie dla podrzędnych Serwerów administracyjnych w wybranej grupie administracyjnej, utwórz grupowe zadanie zdalnej instalacji dla tej grupy.
   - Jeśli chcesz utworzyć zadanie dla określonych podrzędnych Serwerów administracyjnych, utwórz zadanie zdalnej instalacji dla określonych urządzeń.

   Zostanie uruchomiony Kreator tworzenia zadania wdrażania, który poprowadzi Cię przez tworzenie zadania zdalnej instalacji. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w sekcji **Serwer administracyjny Kaspersky Security Center** otwórz folder **Zaawansowane** i wybierz **Zdalna instalacja aplikacji na podrzędnych Serwerach administracyjnych** jako typ zadania.

   Kreator tworzenia nowego zadania utworzy Zadanie zdalnej instalacji wybranej aplikacji na określonych podrzędnych Serwerach administracyjnych.

4. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji, wybrana aplikacja zostanie zainstalowana na podrzędnych Serwerach administracyjnych.

Instalowanie aplikacji przy pomocy kreatora zdalnej instalacji

Do zainstalowania aplikacji firmy Kaspersky można użyć kreatora zdalnej instalacji. Kreator zdalnej instalacji umożliwia przeprowadzenie zdalnej instalacji aplikacji przy pomocy specjalnie utworzonych pakietów instalacyjnych lub bezpośrednio z pakietu dystrybucyjnego.

Aby zadanie Zdalnej instalacji zostało poprawnie wykonane na urządzeniu klienckim, na którym nie został zainstalowany Agent sieciowy, muszą być otwarte następujące porty: TCP 139 i 445; UDP 137 i 138. Domyślnie porty te są otwarte dla wszystkich urządzeń z domeny. W przypadku błędów sieciowych zapoznaj się z bazą wiedzy Kaspersky Security Center.

W celu zainstalowania aplikacji na wybranych urządzeniach przy użyciu kreatora zdalnej instalacji:

1. W drzewie konsoli zlokalizuj folder **Zdalna instalacja**, z którego wybierz podfolder **Pakiety instalacyjne**.
2. W obszarze roboczym folderu wybierz pakiet instalacyjny aplikacji, którą chcesz zainstalować.
3. Z menu kontekstowego pakietu instalacyjnego wybierz **Zainstaluj aplikację**.

   Zostanie uruchomiony Kreator zdalnej instalacji.

4. W oknie **Wybierz urządzenia do instalacji** możesz utworzyć listę urządzeń, na których zostanie zainstalowana aplikacja:

   - **Zainstaluj w grupie zarządzanych urządzeń**

     Jeżeli ta opcja jest zaznaczona, zadanie zdalnej instalacji jest tworzone dla grupy urządzeń.

- **Wybierz urządzenia do instalacji**

  Jeżeli ta opcja jest zaznaczona, zadanie zdalnej instalacji jest tworzone dla określonych urządzeń. Do tych określonych urządzeń mogą należeć zarządzane urządzenia oraz urządzenia nieprzypisane.

5. W oknie **Określanie ustawień zadania zdalnej instalacji** określ ustawienia zdalnej instalacji aplikacji.

   W grupie ustawień **Wymuś pobranie pakietu instalacyjnego** określ sposób rozsyłania na urządzenia klienckie plików, które są niezbędne do zainstalowania aplikacji:

   - **Przy użyciu Agenta sieciowego**

     Jeśli ta opcja jest włączona, pakiety instalacyjne są dostarczane na urządzenia klienckie przez Agenta sieciowego zainstalowanego na tych urządzeniach klienckich.

     Jeśli ta opcja jest wyłączona, pakiety instalacyjne są dostarczane przy użyciu narzędzi systemu operacyjnego urządzeń klienckich.

     Zalecane jest włączenie tej opcji, jeśli zadanie zostało przypisane do urządzeń z zainstalowanymi Agentami sieciowymi.

     Domyślnie opcja ta jest włączona.

   - **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**

     Jeśli ta opcja jest włączona, pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego urządzeń klienckich za pośrednictwem Serwera administracyjnego. Możesz włączyć tę opcję, jeśli na urządzeniu klienckim nie ma zainstalowanego Agenta sieciowego, ale urządzenie klienckie jest w tej samej sieci co Serwer administracyjny.

     Domyślnie opcja ta jest włączona.

   - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**

     Jeśli ta opcja jest włączona, pakiety instalacyjne są przesyłane na urządzenia klienckie przy użyciu narzędzi systemu operacyjnego za pośrednictwem punktów dystrybucyjnych. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny.

     Jeśli opcja **Przy użyciu Agenta sieciowego** jest włączona, pliki będą dostarczane przy użyciu narzędzi systemu operacyjnego, jeśli narzędzia Agenta sieciowego są niedostępne.

     Domyślnie ta opcja jest włączona dla zadań zdalnej instalacji utworzonych na wirtualnym Serwerze administracyjnym.

     > Jeśli wszystkie punkty dystrybucji przypisane do urządzenia okażą się wadliwe, urządzenie nie będzie otrzymywać aktualizacji (baz wirusów i poprawek) ani pakietów instalacyjnych.

   - **Liczba prób instalacji**

     Jeśli podczas wykonywania zadania Zdalna instalacja programowi Kaspersky Security Center nie uda się zainstalować aplikacji na zarządzanym urządzeniu w obrębie liczby uruchomień instalatora określonych przez parametr, Kaspersky Security Center zatrzyma dostarczanie pakietu instalacyjnego na to zarządzane urządzenie i już nie uruchomi instalatora na urządzeniu.

     Opcja `Liczba prób instalacji` umożliwia zachowanie zasobów zarządzanego urządzenia, a także zmniejszenie ruchu sieciowego (dezinstalacja, uruchomienie pliku MSI i wiadomości o błędach).

Powtarzające się próby uruchomienia zadania mogą wskazywać na problem na urządzeniu, który uniemożliwia przeprowadzenie instalacji. Administrator powinien rozwiązać problem w określonej liczbie prób instalacji (na przykład, przydzielając wystarczającą ilość miejsca, usuwając niekompatybilne aplikacje lub modyfikując ustawienia innych aplikacji, które uniemożliwiają przeprowadzenie instalacji) i uruchomić ponownie zadanie (ręcznie lub zgodnie z terminarzem).

Jeśli instalacja się nie powiedzie, problem jest uznawany za nierozwiązalny i wszelkie dalsze uruchomienia zadania są postrzegane jako niepotrzebne zużywanie zasobów i ruchu sieciowego.

Po utworzeniu zadania, licznik prób jest ustawiony na `0`. Każde uruchomienie instalatora, które zwraca błąd na urządzeniu, zwiększa wartość licznika o jeden.

Jeśli liczba prób określonych w parametrze została przekroczona, a urządzenie jest gotowe do zainstalowania aplikacji, możesz zwiększyć wartość parametru `Number of attempts to install` i uruchomić zadanie do zainstalowania aplikacji. W razie czego możesz utworzyć nowe zadanie Zdalna instalacja.

Określ, co należy robić z urządzeniami klienckimi, zarządzanymi przez inny Serwer administracyjny:

- **Zainstaluj na wszystkich urządzeniach**

  Aplikacja zostanie zainstalowana nawet na urządzeniach zarządzanych przez inne Serwery administracyjne.

  Opcja ta jest wybrana domyślnie. Nie musisz zmieniać tego ustawienia, jeśli masz tylko jeden Serwer administracyjny w swojej sieci.

- **Zainstaluj tylko na urządzeniach zarządzanych przez ten Serwer administracyjny**

  Aplikacja zostanie zainstalowana tylko na urządzeniach zarządzanych przez ten Serwer administracyjny. Wybierz tę opcję, jeśli posiadasz więcej niż jeden Serwer administracyjny w swojej sieci i chcesz uniknąć konfliktów między nimi.

Określ ustawienia dodatkowe:

- **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana**

  Jeśli ta opcja jest włączona, wybrana aplikacja nie zostanie ponownie zainstalowana, jeśli już jest zainstalowana na tym urządzeniu klienckim.

  Jeśli ta opcja jest wyłączona, aplikacja zostanie zainstalowana mimo wszystko.

  Domyślnie opcja ta jest włączona.

- **Przypisz pakiet instalacyjny do zasad grupy Active Directory**

  Jeśli ta opcja jest włączona, pakiet instalacyjny jest instalowany przy użyciu zasad grupy Active Directory.

  Ta opcja jest dostępna, jeśli wybrany jest pakiet instalacyjny Agenta sieciowego.

  Domyślnie opcja ta jest wyłączona.

6. W oknie **Wybierz klucz licencyjny** wybierz klucz licencyjny i metodę jego dystrybucji:

- **Nie umieszczaj klucza licencyjnego w pakiecie instalacyjnym (zalecane)**

  Klucz jest automatycznie rozsyłany na wszystkie urządzenia, z którymi jest kompatybilny:

  - Jeśli we właściwościach klucza jest włączona automatyczna dystrybucja.
  - Jeśli utworzono zadanie **Dodaj klucz**.

- **Umieść klucz licencyjny w pakiecie instalacyjnym**

  Klucz jest rozsyłany na urządzenia wraz z pakietem instalacyjnym.

  > Nie zalecamy rozpowszechniania klucza przy użyciu tej metody, ponieważ współdzielone prawa dostępu do odczytu są włączone do repozytorium pakietów instalacyjnych.

Okno **Wybierz klucz licencyjny** jest wyświetlane, jeśli pakiet instalacyjny nie zawiera klucza licencyjnego.

Jeśli pakiet instalacyjny zawiera klucz licencyjny, zostanie wyświetlone okno **Właściwości klucza licencyjnego** zawierające szczegóły dotyczące klucza licencyjnego.

7. W oknie **Wybieranie sposobu ponownego uruchomienia systemu operacyjnego** określ, czy urządzenia muszą być uruchamiane ponownie, jeśli podczas instalacji aplikacji wymagane jest ponowne uruchomienie systemu operacyjnego:

   - **Nie uruchamiaj ponownie urządzenia**

     Jeśli ta opcja jest zaznaczona, urządzenie nie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

   - **Uruchom urządzenie ponownie**

     Jeśli ta opcja jest zaznaczona, urządzenie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

   - **Pytaj użytkownika o akcję**

     Jeśli ta opcja jest zaznaczona, po zainstalowaniu aplikacji zabezpieczającej wyświetlane jest powiadomienie informujące o konieczności ponownego uruchomienia urządzenia. Po kliknięciu odnośnika **Modyfikuj** możesz zmodyfikować tekst wiadomości, okres wyświetlania wiadomości oraz czas automatycznego ponownego uruchomienia.

     Domyślnie opcja ta jest zaznaczona.

   - **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

     Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie aplikacji na zablokowanych urządzeniach przed ich ponownym uruchomieniem.

     Domyślnie opcja ta jest wyłączona.

8. W oknie **Wybierz konta w celu uzyskania dostępu do urządzeń** możesz dodać konta, które będą używane do uruchamiania zadania Zdalnej instalacji:

   - **Konto nie jest wymagane (Agent sieciowy jest zainstalowany)**

     Jeśli ta opcja jest zaznaczona, nie musisz określić konta, z poziomu którego zostanie uruchomiony instalator aplikacji. Zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

     Jeśli Agent sieciowy nie został zainstalowany na urządzeniach klienckich, ta opcja nie będzie dostępna.

- **Konto wymagane (Agent sieciowy nie jest używany)**

  Wybierz tę opcję, jeśli Agent sieciowy nie jest zainstalowany na urządzeniach, do których przypisano zadanie zdalnej instalacji. W takim przypadku możesz określić konto użytkownika lub certyfikat SSH, aby zainstalować aplikację.

  - **Konto lokalne**. Jeśli ta opcja jest zaznaczona, określ konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji. Kliknij przycisk **Dodaj**, wybierz **Konto lokalne**, a następnie określ poświadczenia konta użytkownika.

    Możesz określić wiele kont użytkowników, jeśli na przykład żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, do których przypisujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

  - **Certyfikat SSH**. Jeśli chcesz zainstalować aplikację na urządzeniu klienckim opartym na systemie Linux, możesz określić certyfikat SSH zamiast konta użytkownika. Kliknij przycisk **Dodaj**, wybierz **Certyfikat SSH**, a następnie określ klucze prywatny i publiczny certyfikatu.

    Aby wygenerować klucz prywatny, możesz użyć narzędzia ssh-keygen. Należy zauważyć, że Kaspersky Security Center obsługuje format PEM kluczy prywatnych, ale narzędzie ssh-keygen domyślnie generuje klucze SSH w formacie OPENSSH. Format OPENSSH nie jest obsługiwany przez Kaspersky Security Center. Aby utworzyć klucz prywatny w obsługiwanym formacie PEM, dodaj opcję -m PEM w poleceniu ssh-keygen. Na przykład:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< adres e-mail użytkownika >"
    ```

9. W oknie **Uruchamianie instalacji** kliknij przycisk **Dalej**, aby utworzyć i uruchomić zadanie Zdalnej instalacji na wybranych urządzeniach.

   Jeśli w oknie **Uruchamianie instalacji** wybrano opcję **Nie uruchamiaj zadania niezwłocznie po zakończeniu działania kreatora zdalnej instalacji**, zadanie zdalnej instalacji nie zostanie uruchomione. Możesz później uruchomić to zadanie ręcznie. Nazwa zadania odpowiada nazwie pakietu instalacyjnego dla aplikacji: **Instalacja <Nazwa pakietu instalacyjnego>**.

W celu zainstalowania aplikacji na urządzeniach w grupie administracyjnej przy użyciu kreatora zdalnej instalacji:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednią grupę administracyjną.
2. Z drzewa konsoli wybierz grupę administracyjną.
3. W obszarze roboczym grupy kliknij przycisk **Wykonaj akcję** i z listy rozwijalnej wybierz **Zainstaluj aplikację**.

   Zostanie uruchomiony Kreator zdalnej instalacji. Postępuj zgodnie z instrukcjami kreatora.
4. W ostatnim kroku kreatora kliknij **Dalej**, aby utworzyć i uruchomić Zadanie zdalnej instalacji na wybranych urządzeniach.

Po zakończeniu działania kreatora zdalnej instalacji, Kaspersky Security Center wykona następujące czynności:

- Tworzenie pakietu instalacyjnego potrzebnego do zainstalowania aplikacji (jeśli nie został utworzony wcześniej). Pakiet instalacyjny znajduje się w folderze **Zdalna instalacja**, w podfolderze **Pakiety instalacyjne** i nosi nazwę odpowiadającą nazwie i wersji aplikacji. Możesz użyć tego pakietu instalacyjnego do przyszłej instalacji aplikacji.
- Tworzy i uruchamia zadanie zdalnej instalacji dla określonych urządzeń lub grupy administracyjnej. Utworzone zadanie zdalnej instalacji jest przechowywane w folderze **Zadania** lub jest dodawane do zadań grupy administracyjnej, dla której zostało utworzone. Możesz później uruchomić to zadanie ręcznie. Nazwa zadania odpowiada nazwie pakietu instalacyjnego dla aplikacji: **Instalacja <Nazwa pakietu instalacyjnego>**.

Praca z wtyczkami zarządzającymi

Aplikacje firmy Kaspersky są zarządzane poprzez Konsolę administracyjną przy użyciu wtyczek administracyjnych. Każda aplikacja firmy Kaspersky, która może zostać zarządzana poprzez Kaspersky Security Center, zawiera wtyczkę zarządzającą. Przy pomocy wtyczki zarządzającej można wykonywać następujące czynności w Konsoli administracyjnej:

- Tworzyć i modyfikować zasady i ustawienia aplikacji, jak również ustawienia zadań aplikacji.
- Uzyskiwać informacje o zadaniach aplikacji, zdarzeniach występujących w trakcie jej pracy oraz statystyki z działania aplikacji odebrane od urządzeń klienckich.

Aby sprawdzić listę zainstalowanych wtyczek i ich wersji:

1. W drzewie Konsoli administracyjnej kliknij prawym przyciskiem myszy **Serwer administracyjny <Nazwa_serwera>** i wybierz **Właściwości**.
2. Kliknij **Zaawansowane → Szczegóły zainstalowanych wtyczek administrujących aplikacją**.

Lista zainstalowanych wtyczek zarządzających i ich wersji pojawi się w prawej części okna.

Wtyczki dla zarządzanych aplikacji możesz zainstalować po uruchomieniu kreatora wstępnej konfiguracji Serwera administracyjnego podczas początkowej konfiguracji Kaspersky Security Center. Można także zainstalować wtyczki zarządzające ręcznie.

Aby ręcznie zainstalować wtyczkę zarządzającą:

1. Pobierz wtyczkę zarządzającą dla aplikacji Kaspersky i wymaganą wersję (na przykład Kaspersky Endpoint Security for Windows 12.6) ze strony internetowej pomocy technicznej Kaspersky.
2. Jeżeli Konsola administracyjna jest uruchomiona, zamknij ją.
3. Rozpakuj pobrany plik wtyczki i uruchom plik klcfginst.msi lub klcfginst.exe. Postępuj zgodnie z instrukcjami kreatora instalacji.
4. Po zakończeniu instalacji uruchom Konsolę administracyjną i upewnij się, że wtyczka znajduje się na liście zainstalowanych wtyczek, zgodnie z opisem w poprzedniej procedurze.

Po uruchomieniu Konsoli administracyjnej po zainstalowaniu wtyczki zarządzającej obsługującej kreatora szybkiego uruchamiania zarządzanych aplikacji, kreator ten zostanie uruchomiony automatycznie. Możesz wykonać kroki kreatora szybkiego uruchamiania zarządzanych aplikacji, aby utworzyć domyślne zasady i zadania aplikacji Kaspersky. Kreator uruchamia się automatycznie tylko wtedy, gdy uruchamiasz Konsolę administracyjną po początkowej instalacji wtyczki lub po zaktualizowaniu wtyczki zarządzającej do wersji zgodnej z inną wersją aplikacji Kaspersky, dla której zadania i zasady nie zostały jeszcze utworzone. Kreator szybkiego uruchamiania zarządzanych aplikacji można również uruchomić ręcznie.

W celu ręcznego uruchomienia kreatora wstępnej konfiguracji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego węzła Serwera administracyjnego, wybierz **Wszystkie zadania → Kreator wstępnej konfiguracji zarządzanych aplikacji**.
3. Zostanie uruchomiony kreator szybkiego uruchamiania zarządzanej aplikacji. Postępuj zgodnie z instrukcjami kreatora, aby utworzyć domyślne zasady i zadania aplikacji Kaspersky.

Aby usunąć wtyczkę zarządzającą:

1. Jeżeli Konsola administracyjna jest uruchomiona, zamknij ją.
2. Otwórz edytor rejestru systemu Windows.
3. Znajdź następujący klucz:
   - `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins` dla systemu 32-bitowego.
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins` dla systemu 64-bitowego.

   Klucz zawiera zainstalowane wtyczki zarządzające. Dla każdej wtyczki wartość `DisplayName` zawiera nazwę wtyczki oraz wartość `UninstallString` zawiera polecenie odinstalowania wtyczki.
4. Znajdź klucz wtyczki, którą chcesz odinstalować, i skopiuj jej wartość `UninstallString` do schowka.
5. Wklej wartość do ciągu poleceń i uruchom go z uprawnieniami administratora systemu.

Wersja wtyczki zarządzającej nie może być wcześniejsza niż wersja aplikacji zarządzanej przez Kaspersky. Jeśli aktualizujesz aplikację Kaspersky na urządzeniach, musisz zainstalować wtyczkę zarządzającą w tej samej wersji.

Po otwarciu zasady utworzonej we wcześniejszej wersji wtyczki zostaniesz poproszony o zaakceptowanie oświadczenia Kaspersky Security Network Statement.

Podczas dezinstalacji konsoli Kaspersky Security Center Web Console odinstalowywane są również wszystkie wtyczki zarządzające.

Jeżeli otworzysz i zapiszesz zasadę w wersji wtyczki późniejszej niż wersja zarządzanej aplikacji, zasada zostanie zaktualizowana i nie będzie można jej otworzyć we wtyczce z wcześniejszej wersji.

Wyświetlanie raportu wdrażania ochrony

Użyj opcji Raport wdrażania ochrony, aby monitorować postęp zdalnej instalacji ochrony sieci.

W celu wyświetlenia raportu wdrażania ochrony:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. W folderze **Raporty** wybierz szablon raportu o nazwie **Raport wdrażania ochrony**.

Obszar roboczy wyświetla raport zawierający informacje o zdalnej instalacji ochrony na wszystkich urządzeniach w sieci.

Możesz wygenerować nowy raport wdrażania ochrony i określić typy danych, które powinien zawierać:

- Dla grupy administracyjnej
- Dla wskazanych urządzeń
- Dla wyboru urządzeń
- Dla wszystkich urządzeń

Kaspersky Security Center zakłada, że na urządzeniu jest wdrożona ochrona, jeśli jest na nim zainstalowana aplikacja zabezpieczająca oraz jest włączona ochrona w czasie rzeczywistym.

Zdalne usuwanie aplikacji

Kaspersky Security Center umożliwia zdalne odinstalowanie aplikacji z urządzeń przy użyciu zadań zdalnej dezinstalacji. Te zadania są tworzone i przydzielane do urządzeń za pośrednictwem dedykowanego kreatora. W celu szybkiego i łatwego przypisywania zadań do urządzeń, należy wskazać urządzenia w oknie kreatora w jeden z następujących sposobów:

- **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**. W tym przypadku zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**. Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.
- **Przypisz zadanie do wyboru urządzeń**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonym wyborze. Możesz określić predefiniowany lub niestandardowy wybór, który utworzyłeś.
- **Przypisz zadanie do grupy administracyjnej**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonej grupie administracyjnej.

Problemy ze zdalnym usuwaniem

Podczas zdalnego usuwania aplikacji innych firm administratorzy mogą napotkać ostrzeżenie: „Zdalna dezinstalacja została zakończona na tym urządzeniu z ostrzeżeniami: Aplikacja do usunięcia nie jest zainstalowana." Problem ten pojawia się zazwyczaj w sytuacji, gdy aplikacja przeznaczona do usunięcia jest zainstalowana wyłącznie dla aktualnie zalogowanego użytkownika. Jeżeli użytkownik nie jest zalogowany, taka aplikacja staje się niewidoczna i nie można jej usunąć zdalnie.

Takie zachowanie kontrastuje z aplikacjami przeznaczonymi do użytku przez wielu użytkowników na tym samym urządzeniu, gdzie aplikacje są widoczne i dostępne globalnie dla wszystkich użytkowników urządzenia.

W ramach Kaspersky Security Center algorytm rejestru aplikacji obsługuje aplikacje dla pojedynczych użytkowników inaczej niż aplikacje dla wielu użytkowników:

- Aplikacje dla wielu użytkowników są aktualizowane na bieżąco na liście zainstalowanych aplikacji.
- Aplikacje dla pojedynczych użytkowników są monitorowane za pomocą mechanizmu buforowania.

  Jeśli w momencie wykrycia aplikacji użytkownik był zalogowany, Kaspersky Security Center buforuje informacje o aplikacjach tego użytkownika. Nawet jeśli użytkownik później się wyloguje, Kaspersky Security Center nadal wyświetla te aplikacje jako zainstalowane na podstawie danych z pamięci podręcznej, chociaż nie są one już widoczne ani dostępne na urządzeniu.

Ta rozbieżność może spowodować sytuacje, w których Kaspersky Security Center zidentyfikuje aplikację jako zainstalowaną na podstawie danych z pamięci podręcznej, ale zadanie usunięcia aplikacji nie powiedzie się, ponieważ aplikacja nie będzie dostępna po wylogowaniu użytkownika.

Domyślnie czas życia danych aplikacji w pamięci podręcznej wynosi 30 dni. Administratorzy mogą zmienić to ustawienie, aby skrócić czas przechowywania danych w pamięci podręcznej, minimalizując w ten sposób rozbieżności między wyświetlanymi danymi a rzeczywistą widocznością aplikacji na urządzeniach.

Aby dostosować czas życia pamięci podręcznej do 1 godziny (3600 sekund), uruchom następujące polecenie na Serwerze administracyjnym:

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

Po uruchomieniu tego polecenia należy ponownie uruchomić Serwer administracyjny, aby zmiany zostały zastosowane.

Źródła informacji o zainstalowanych aplikacjach

Agent sieciowy pobiera informacje o oprogramowaniu zainstalowanym na urządzeniach z systemem Windows z następujących kluczy rejestru:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla wszystkich użytkowników.
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla wszystkich użytkowników.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla bieżącego użytkownika.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla konkretnych użytkowników.

Zdalne usuwanie aplikacji z urządzeń klienckich w grupie administracyjnej

W celu zdalnego usunięcia aplikacji z urządzeń klienckich w grupie administracyjnej:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednią grupę administracyjną.
2. Z drzewa konsoli wybierz grupę administracyjną.
3. W obszarze roboczym grupy wybierz zakładkę **Zadania**.
4. Uruchom tworzenie zadania, klikając przycisk **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w węźle **Serwer administracyjny Kaspersky Security Center**, w folderze **Zaawansowane** wybierz **Zdalna dezinstalacja aplikacji** jako typ zadania.

   Kreator tworzenia nowego zadania tworzy grupowe zadanie zdalnej dezinstalacji wybranej aplikacji. Nowe zadanie pojawi się w obszarze roboczym grupy administracyjnej na zakładce **Zadania**.
5. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej dezinstalacji, wybrana aplikacja zostanie odinstalowana z urządzeń klienckich w grupie administracyjnej.

Zdalne usuwanie aplikacji z wybranych urządzeń

W celu zdalnego usunięcia aplikacji z wybranych urządzeń:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania, klikając **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w węźle **Serwer administracyjny Kaspersky Security Center**, w folderze **Zaawansowane** wybierz **Zdalna dezinstalacja aplikacji** jako typ zadania.

   Kreator tworzenia nowego zadania tworzy zadanie zdalnej dezinstalacji wybranej aplikacji z określonych urządzeń. Nowo utworzone zadanie będzie wyświetlane w obszarze roboczym folderu **Zadania**.
3. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej dezinstalacji, wybrana aplikacja zostanie odinstalowana z wybranych urządzeń.

Praca z pakietami instalacyjnymi

Podczas tworzenia zadań zdalnej instalacji system używa pakietów instalacyjnych zawierających zestawy parametrów potrzebnych do zainstalowania oprogramowania.

Pakiety instalacyjne mogą zawierać plik klucza. Zalecane jest unikanie współdzielenia dostępu do pakietów instalacyjnych zawierających plik klucza.

Możesz użyć jednego pakietu instalacyjnego wiele razy.

Pakiety instalacyjne utworzone dla Serwera administracyjnego zostają przeniesione do drzewa konsoli i znajdują się w folderze **Zdalna instalacja**, w podfolderze **Pakiety instalacyjne**. Pakiety instalacyjne są przechowywane na Serwerze administracyjnym, w podfolderze Pakiety, w obrębie określonego folderu współdzielonego.

W razie potrzeby możesz usunąć pakiet instalacyjny z podfolderu **Pakiety instalacyjne**, postępując zgodnie z instrukcjami zawartymi w artykule Usuwanie obiektu.

Nie zmieniaj ręcznie zawartości pakietów instalacyjnych w folderze współdzielonym. W razie potrzeby możesz utworzyć kopię pakietu instalacyjnego, wprowadzić niezbędne zmiany i utworzyć nowe zadania instalacji.

Tworzenie pakietu instalacyjnego

W tym artykule opisano procedurę tworzenia następujących typów pakietów instalacyjnych:

- Pakiet instalacyjny dla aplikacji Kaspersky
- Pakiet instalacyjny dla określonego pliku wykonywalnego
- Pakiet instalacyjny dla aplikacji z bazy danych Kaspersky

Nie ma konieczności ręcznego utworzenia pakietu instalacyjnego dla zdalnej instalacji Agenta sieciowego. Tworzony jest on automatycznie podczas instalacji programu Kaspersky Security Center w folderze **Pakiety instalacyjne**. Jeśli usunięto pakiet do zdalnej instalacji Agenta sieciowego, wówczas do jego odtworzenia niezbędny będzie plik nagent.kud znajdujący się w folderze NetAgent pakietu dystrybucyjnego programu Kaspersky Security Center.

W celu utworzenia pakietu instalacyjnego:

1. Nawiąż połączenie z żądanym Serwerem administracyjnym.
2. Z drzewa konsoli wybierz **Zaawansowane** → **Zdalna instalacja** → **Pakiety instalacyjne**.

3. Uruchom tworzenie nowego pakietu instalacyjnego w jeden z następujących sposobów:

   - Kliknij prawym przyciskiem myszy folder **Pakiety instalacyjne** i wybierz **Nowy → Pakiet instalacyjny** z menu kontekstowego.
   - Kliknij prawym przyciskiem myszy w pustym obszarze listy pakietów instalacyjnych i wybierz **Utwórz → Pakiet instalacyjny** z menu kontekstowego.
   - Klikając odnośnik **Utwórz pakiet instalacyjny** w sekcji zarządzania listą pakietów instalacyjnych.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu.

4. Wybierz jeden z następujących typów pakietów instalacyjnych, klikając odpowiednią ikonę:

   - Pakiet instalacyjny dla aplikacji Kaspersky.
   - Pakiet instalacyjny dla określonego pliku wykonywalnego.
   - Pakiet instalacyjny dla aplikacji z bazy danych Kaspersky.

5. Podaj nazwę pakietu instalacyjnego, który ma zostać utworzony.

   Możesz podać dowolną nazwę.

6. Wybierz aplikację lub plik wykonywalny, dla którego ma zostać utworzony pakiet instalacyjny, w jeden z następujących sposobów:

   - Kliknij przycisk **Przeglądaj** i w standardowym oknie **Otwórz** systemu Windows wybierz pakiet dystrybucyjny żądanej aplikacji znajdujący się na dostępnych dyskach.

     Opcja ta ma zastosowanie, jeśli zdecydujesz się utworzyć pakiet instalacyjny dla aplikacji Kaspersky lub określonego pliku wykonywalnego.

   - Kliknij przycisk **Przeglądaj** i w oknie **Wybierz aplikację** wybierz pakiet dystrybucyjny żądanej aplikacji.

     Opcja ta ma zastosowanie, jeśli zdecydujesz się utworzyć pakiet instalacyjny aplikacji z bazy danych Kaspersky.

   Jeśli tworzysz pakiet instalacyjny dla Serwera administracyjnego, wybierz plik sc.kud. Plik sc.kud znajduje się w folderze głównym pakietu dystrybucyjnego Kaspersky Security Center.

   W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.

7. Przejrzyj Umowę licencyjną użytkownika końcowego i Politykę prywatności.

   Podczas tworzenia pakietu instalacyjnego dla aplikacji może zostać wyświetlony monit o wyświetlenie i zaakceptowanie Umowy licencyjnej użytkownika końcowego oraz Polityki prywatności dla tej aplikacji.

   Przeczytaj oba dokumenty. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności, zaakceptuj je, zaznaczając odpowiednie pola wyboru.

   Instalacja aplikacji na Twoim urządzeniu będzie kontynuowana, a tworzenie pakietu instalacyjnego zostanie wznowione.

   Podczas tworzenia pakietu instalacyjnego dla Kaspersky Endpoint Security for Mac możesz wybrać język Umowy licencyjnej i Polityki prywatności.

8. W razie potrzeby włącz automatyczną instalację komponentów systemu.

   Jeśli tworzysz pakiet instalacyjny aplikacji z bazy danych Kaspersky, możesz włączyć automatyczną instalację niezbędnych komponentów systemu. Kreator tworzenia nowego pakietu wyświetla listę wszystkich komponentów systemu dostępnych dla wybranej aplikacji. Dostęp do tej listy możesz uzyskać w dowolnym momencie we właściwościach pakietu instalacyjnego.

   Jeśli tworzysz pakiet instalacyjny poprawki, lista zawiera wszystkie wymagania systemowe niezbędne do wdrożenia poprawki.

9. Kliknij przycisk **Zakończ**, aby zakończyć proces tworzenia pakietu.

Po zakończeniu pracy kreatora tworzenia nowego pakietu, nowy pakiet instalacyjny pojawi się w obszarze roboczym folderu **Pakiety instalacyjne**.

Tworzenie autonomicznych pakietów instalacyjnych

Ty oraz użytkownicy urządzeń w Twojej organizacji mogą używać autonomicznych pakietów instalacyjnych, aby ręcznie instalować aplikacje na urządzeniach.

Autonomiczny pakiet instalacyjny jest plikiem wykonywalnym (installer.exe), który można umieścić na serwerze sieciowym lub w folderze sieciowym lub przenieść na urządzenie klienckie w dowolny sposób. Możesz także wysłać odnośnik do autonomicznego pakietu instalacyjnego za pośrednictwem poczty elektronicznej. Na urządzeniu klienckim użytkownik może uruchomić otrzymany plik lokalnie, aby zainstalować aplikację bez udziału Kaspersky Security Center.

Upewnij się, że autonomiczny pakiet instalacyjny nie jest dostępny dla nieupoważnionych osób.

Możesz tworzyć autonomiczne pakiety instalacyjne dla aplikacji Kaspersky i aplikacji innych firm na platformy Windows, macOS i Linux. Aby utworzyć autonomiczny pakiet instalacyjny dla aplikacji firmy trzeciej, w pierwszej kolejności powinieneś utworzyć niestandardowy pakiet instalacyjny.

Źródło utworzenia autonomicznych pakietów instalacyjnych to pakiety instalacyjne na liście utworzonej na Serwerze administracyjnym.

W celu utworzenia autonomicznego pakietu instalacyjnego:

1. W drzewie konsoli wybierz **Serwer administracyjny → Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Na liście pakietów instalacyjnych wybierz pakiet instalacyjny, dla którego chcesz utworzyć pakiet autonomiczny.

3. Z menu kontekstowego wybierz **Utwórz autonomiczny pakiet instalacyjny**.

   Zostanie uruchomiony Kreator tworzenia autonomicznego pakietu instalacyjnego. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

4. Na pierwszej stronie kreatora, jeśli wybrano pakiet instalacyjny dla aplikacji Kaspersky i chcesz zainstalować Agenta sieciowego razem z wybraną aplikacją, upewnij się, że opcja **Zainstaluj Agenta sieciowego wraz z aplikacją** jest włączona.

   Domyślnie opcja ta jest włączona. Zalecane jest włączenie tej opcji, jeśli nie jesteś pewien, czy Agent sieciowy jest zainstalowany na urządzeniu. Jeśli Agent sieciowy jest już zainstalowany na urządzeniu, po zainstalowaniu autonomicznego pakietu instalacyjnego wraz z Agentem sieciowym, Agent sieciowy zostanie zaktualizowany do nowszej wersji.

Jeśli wyłączysz tę opcję, Agent sieciowy nie zostanie zainstalowany na urządzeniu, a urządzenie będzie niezarządzane.

Jeśli autonomiczny pakiet instalacyjny dla wybranej aplikacji już istnieje na Serwerze administracyjnym, kreator poinformuje o tym fakcie. W tym przypadku powinieneś wybrać jedno z następujących działań:

- **Utwórz autonomiczny pakiet instalacyjny**. Wybierz tę opcję, na przykład, jeśli chcesz utworzyć autonomiczny pakiet instalacyjny dla nowej wersji aplikacji oraz chcesz zachować autonomiczny pakiet instalacyjny, który utworzyłeś dla poprzedniej wersji aplikacji. Nowy autonomiczny pakiet instalacyjny zostanie umieszczony w innym folderze.

- **Użyj istniejącego autonomicznego pakietu instalacyjnego**. Wybierz tę opcję, jeśli chcesz użyć istniejącego autonomicznego pakietu instalacyjnego. Proces tworzenia pakietu nie zostanie uruchomiony.

- **Ponownie skompiluj istniejący autonomiczny pakiet instalacyjny**. Wybierz tę opcję, jeśli ponownie chcesz utworzyć autonomiczny pakiet instalacyjny dla tej samej aplikacji. Autonomiczny pakiet instalacyjny znajduje się w tym samym folderze.

5. W kroku kreatora wybierz opcję **Przenieś nieprzypisane urządzenia do tej grupy** i określ grupę administracyjną, do której chcesz przenieść urządzenie klienckie po zainstalowaniu Agenta sieciowego.

   Domyślnie, urządzenie zostanie przeniesione do grupy **Zarządzane urządzenia**.

   Jeśli nie chcesz przenieść urządzenia klienckiego do grupy administracyjnej po zainstalowaniu Agenta sieciowego, wybierz opcję **Nie przenoś urządzeń**.

6. W kolejnym kroku kreatora, po zakończeniu procesu tworzenia autonomicznego pakietu instalacyjnego, zostanie wyświetlony wynik tworzenia autonomicznego pakietu instalacyjnego oraz ścieżka do pakietu autonomicznego.

   Możesz kliknąć odnośniki i wykonać dowolną z następujących czynności:

   - Otwórz folder z autonomicznym pakietem instalacyjnym.

   - Wyślij e-mail zawierający odnośnik do utworzonego autonomicznego pakietu instalacyjnego. Aby wykonać tę akcję, powinieneś mieć uruchomioną aplikację do obsługi wiadomości e-mail.

   - Przykładowy kod HTML do publikacji odnośnika na stronie internetowej. Plik TXT jest tworzony i otwierany w aplikacji, która jest kojarzona z formatem TXT. W pliku wyświetlany jest znacznik HTML <a> z atrybutami.

7. W następnym kroku kreatora, jeśli chcesz otworzyć listę autonomicznych pakietów instalacyjnych, włącz opcję **Otwórz listę pakietów autonomicznych**.

8. Kliknij przycisk **ZAKOŃCZ**.

   Kreator tworzenia autonomicznego pakietu instalacyjnego zostanie zamknięty.

Autonomiczny pakiet instalacyjny jest tworzony i umieszczany w podfolderze Pkglnst folderu współdzielonego Serwera administracyjnego. Możesz przejrzeć listę pakietów autonomicznych, klikając przycisk **Wyświetl listę pakietów autonomicznych** nad listą pakietów instalacyjnych.

Tworzenie niestandardowego pakietu instalacyjnego

W celu wykonania następujących czynności możesz użyć niestandardowych pakietów instalacyjnych:

- Aby zainstalować dowolną aplikację (np. edytor tekstu) na urządzeniu klienckim, na przykład, przy użyciu zadania.

- Aby utworzyć autonomiczny pakiet instalacyjny.

Niestandardowy pakiet instalacyjny to folder z zestawem plików. Źródło utworzenia niestandardowego pakietu instalacyjnego to *plik archiwum*. Plik archiwum zawiera plik lub pliki, które muszą znajdować się w niestandardowym pakiecie instalacyjnym. Tworząc niestandardowy pakiet instalacyjny, możesz określić parametry wiersza poleceń, na przykład, aby zainstalować aplikację w trybie cichym.

W celu utworzenia niestandardowego pakietu instalacyjnego:

1. W drzewie konsoli wybierz **Serwer administracyjny → Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Nad listą pakietów instalacyjnych kliknij przycisk **Utwórz pakiet instalacyjny**.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

3. W pierwszym kroku kreatora wybierz **Utwórz pakiet instalacyjny dla określonego pliku wykonywalnego**.

4. W kolejnym kroku kreatora określ nazwę niestandardowego pakietu instalacyjnego.

5. W kolejnym kroku kreatora kliknij przycisk **Przeglądaj** i w standardowym oknie **Otwórz** systemu Windows wybierz plik archiwum znajdujący się na dostępnych dyskach w celu utworzenia niestandardowego pakietu instalacyjnego.

   Możesz przesłać archiwum ZIP, CAB, TAR lub TAR.GZ. Nie jest możliwe utworzenie pakietu instalacyjnego z pliku SFX (samorozpakowujące się archiwum).

   Pliki są pobierane na Serwer administracyjny Kaspersky Security Center.

6. W kolejnym kroku kreatora określ parametry wiersza poleceń pliku wykonywalnego.

   Możesz określić parametry wiersza poleceń, aby zainstalować aplikację z pakietu instalacyjnego w trybie cichym. Określanie parametrów wiersza poleceń jest opcjonalne.

   Jeśli chcesz, skonfiguruj następujące opcje:

   - **Kopiuj całą zawartość folderu do pakietu instalacyjnego**

     Wybierz tę opcję, jeśli plikowi wykonywalnemu towarzyszą dodatkowe pliki wymagane do zainstalowania aplikacji. Przed włączeniem tej opcji upewnij się, że wszystkie wymagane pliki są przechowywane w tym samym folderze. Jeśli ta opcja jest włączona, aplikacja doda całą zawartość folderu, w tym określony plik wykonywalny, do pakietu instalacyjnego.

   - **Konwertuj ustawienia na zalecane wartości dla aplikacji rozpoznawanych przez Kaspersky Security Center**

     Aplikacja zostanie zainstalowana z zalecanymi ustawieniami, jeśli informacje o określonej aplikacji znajdują się w bazie danych Kaspersky.

     Jeśli wprowadziłeś parametry w polu **Wiersz polecenia pliku wykonywalnego**, zostaną zapisane z zalecanymi ustawieniami.

     Domyślnie opcja ta jest włączona.

     Baza danych Kaspersky jest tworzona i zarządzana przez analityków z Kaspersky. Dla każdej aplikacji dodanej do bazy danych analitycy z Kaspersky definiują optymalne ustawienia instalacji. Ustawienia są definiowane, aby zapewnić pomyślną zdalną instalację aplikacji na urządzeniu klienckim. Baza danych jest automatycznie aktualizowana na Serwerze administracyjnym, gdy uruchamiasz zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego.

   Zostanie uruchomiony proces tworzenia niestandardowego pakietu instalacyjnego.

   Kreator informuje, gdy proces zostanie zakończony.

Jeśli niestandardowy pakiet instalacyjny nie zostanie utworzony, zostanie wyświetlona odpowiednia wiadomość.

7. W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

   Pakiet instalacyjny, który utworzyłeś, zostanie pobrany do podfolderu Packages folderu współdzielonego Serwera administracyjnego. Po pobraniu, niestandardowy pakiet instalacyjny pojawi się na liście pakietów instalacyjnych.

Na liście pakietów instalacyjnych na Serwerze administracyjnym możesz przejrzeć i edytować właściwości niestandardowego pakietu instalacyjnego.

Przeglądanie i edytowanie właściwości niestandardowych pakietów instalacyjnych

Po utworzeniu niestandardowego pakietu instalacyjnego, możesz przejrzeć ogólne informacje o pakiecie instalacyjnym i określić ustawienia instalacyjne w oknie właściwości.

W celu przejrzenia i edytowania właściwości niestandardowego pakietu instalacyjnego:

1. W drzewie konsoli wybierz **Serwer administracyjny → Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Z menu kontekstowego pakietu instalacyjnego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości wybranego pakietu instalacyjnego.

3. Przejrzyj następujące informacje:

   - Nazwa pakietu instalacyjnego
   - Nazwa aplikacji spakowanej w niestandardowy pakiet instalacyjny
   - Wersja aplikacji
   - Data utworzenia pakietu instalacyjnego
   - Ścieżka do niestandardowego pakietu instalacyjnego na Serwerze administracyjnym
   - Parametry wiersza polecenia pliku wykonywalnego

4. Określ następujące ustawienia:

   - Nazwa pakietu instalacyjnego
   - **Zainstaluj wymagane ogólne składniki systemu**

     Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

     Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

     Domyślnie opcja ta jest wyłączona.

Ta opcja jest dostępna tylko, gdy aplikacja dodana do pakietu instalacyjnego zostanie rozpoznana przez Kaspersky Security Center.

- **Wiersz polecenia pliku wykonywalnego**

  Jeśli dla cichej instalacji aplikacja wymaga dodatkowych parametrów, określ je w tym polu. Więcej informacji można znaleźć w dokumentacji producenta.

  Możesz też wprowadzić inne parametry.

  Ta opcja jest dostępna tylko dla pakietów, które nie są tworzone w oparciu o aplikacje Kaspersky.

5. Kliknij przycisk **OK** lub **Zastosuj**, aby zapisać zmiany (jeśli jakiekolwiek są).

Nowe ustawienia zostaną zapisane.

Uzyskiwanie pakietu instalacyjnego Agenta sieciowego z pakietu dystrybucyjnego Kaspersky Security Center

Pakiet instalacyjny Agenta sieciowego można uzyskać z pakietu dystrybucyjnego Kaspersky Security Center bez konieczności instalowania Kaspersky Security Center. Następnie możesz użyć pakietu instalacyjnego do zainstalowania Agenta sieciowego na urządzeniach klienckich.

W celu uzyskania pakietu instalacyjnego Agenta sieciowego z pakietu dystrybucyjnego Kaspersky Security Center:

1. Uruchom plik wykonywalny ksc_<numer wersji>.<numer kompilacji> _full_<język lokalizacji>.exe z pakietu dystrybucyjnego Kaspersky Security Center.
2. W otwartym oknie kliknij odnośnik **Wyodrębnij pakiety instalacyjne**.
3. Na liście pakietów instalacyjnych zaznacz pole obok pakietu instalacyjnego Agenta sieciowego, a następnie kliknij przycisk **Dalej**.
4. W razie potrzeby kliknij przycisk **Przeglądaj**, aby zmienić wyświetlany folder, do którego ma zostać wypakowany pakiet instalacyjny.
5. Kliknij przycisk **Wyodrębnij**.

   Aplikacja rozpakowuje pakiet instalacyjny Agenta sieciowego.
6. Po zakończeniu procesu kliknij przycisk **Zamknij**.

Pakiet instalacyjny Agenta sieciowego zostanie rozpakowany do wybranego folderu.

Możesz użyć pakietu instalacyjnego do zainstalowania Agenta sieciowego na jeden z następujących sposobów:

- Lokalnie, uruchamiając plik setup.exe z wyodrębnionego folderu
- Przez cichą instalację
- Korzystając z zasad grupy Microsoft Windows

Rozsyłanie pakietów instalacyjnych na podrzędne Serwery administracyjne

W celu rozesłania pakietów instalacyjnych na podrzędne Serwery administracyjne:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednie podrzędne Serwery administracyjne.

2. Utwórz zadanie rozsyłania pakietu instalacyjnego na podrzędne Serwery administracyjne w jeden z następujących sposobów:

   - Jeśli chcesz utworzyć zadanie dla podrzędnych Serwerów administracyjnych w wybranej grupie administracyjnej, uruchom tworzenie grupowego zadania dla tej grupy.

   - Jeśli chcesz utworzyć zadanie dla określonych podrzędnych Serwerów administracyjnych, uruchom tworzenie zadania dla określonych urządzeń.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w węźle **Serwer administracyjny Kaspersky Security Center**, w folderze **Zaawansowane** wybierz **Rozsyłanie pakietu instalacyjnego** jako typ zadania.

   Kreator tworzenia nowego zadania utworzy zadanie rozsyłania wybranych pakietów instalacyjnych na określone podrzędne Serwery administracyjne.

3. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Wybrane pakiety instalacyjne zostaną skopiowane na określone podrzędne Serwery administracyjne.

Rozsyłanie pakietów instalacyjnych poprzez punkty dystrybucji

Do rozesłania pakietów instalacyjnych w obrębie grupy administracyjnej można wykorzystać punkty dystrybucji.

Po odebraniu pakietów instalacyjnych z Serwera administracyjnego, punkty dystrybucji automatycznie rozsyłają je na urządzenia klienckie, korzystając z multiemisji IP. Rozsyłanie nowych pakietów instalacyjnych w obrębie grupy administracyjnej przy użyciu multiemisji IP występuje tylko raz. Jeśli w momencie dystrybucji pakietów urządzenie klienckie było odłączone od sieci korporacyjnej, wówczas Agent sieciowy (na urządzeniu klienckim) automatycznie pobierze potrzebny pakiet instalacyjny z punktu dystrybucji po uruchomieniu zadania instalacji.

Przesyłanie rezultatów instalacji aplikacji do Kaspersky Security Center

Po utworzeniu pakietu instalacyjnego aplikacji możesz skonfigurować go tak, aby wszystkie informacje diagnostyczne dotyczące wyników instalacji aplikacji były przesyłane do Kaspersky Security Center. Dla pakietów instalacyjnych aplikacji firmy Kaspersky przesyłanie informacji diagnostycznych o wynikach instalacji aplikacji jest skonfigurowane domyślnie i nie jest konieczna dodatkowa konfiguracja.

W celu skonfigurowania przesyłania informacji diagnostycznych dotyczących wyników instalacji aplikacji do Kaspersky Security Center:

1. Przejdź do folderu z pakietem instalacyjnym utworzonym dla wybranej aplikacji przy użyciu Kaspersky Security Center. Folder można znaleźć w folderze współdzielonym wskazanym podczas instalacji Kaspersky Security Center.

2. Otwórz plik z rozszerzeniem .kpd lub .kud w programie umożliwiającym jego edycję (na przykład w notatniku systemu Microsoft Windows).

   Plik będzie miał format typowego pliku konfiguracyjnego .ini.

3. Dodaj do pliku następujące wiersze:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Polecenie to konfiguruje Kaspersky Security Center tak, aby program czekał na zakończenie instalacji aplikacji, dla której tworzony jest pakiet instalacyjny oraz na analizę kodu zwrotnego instalatora. Jeśli chcesz wyłączyć przesyłanie danych diagnostycznych, ustaw wartość klucza Wait na 0.

4. Dodaj opis kodów zwrotnych w celu pomyślnego zakończenia instalacji. W tym celu, do pliku dodaj następujące wiersze:

   ```
   [SetupProcessResult_SuccessCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   W nawiasach kwadratowych znajdują się opcjonalne klucze.

   Składnia dla wierszy:

   - `<return code>`. Dowolna liczba odpowiadająca kodowi zwrotnemu instalatora. Można podać dowolną liczbę kodów zwrotnych.
   - `<description>`. Opis tekstowy wyniku instalacji. Opis można pominąć.

5. Dodaj opis kodów zwrotnych dla instalacji zakończonej niepowodzeniem. W tym celu, do pliku dodaj następujące wiersze:

   ```
   [SetupProcessResult_ErrorCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   Składnia tych wierszy jest identyczna jak składnia wierszy zawierających kody zwrotne instalacji zakończonej powodzeniem.

6. Zapisz wszystkie zmiany i zamknij plik .kpd lub .kud.

Wyniki instalacji aplikacji określonej przez użytkownika zostaną zapisane w raportach programu Kaspersky Security Center i pojawią się na liście zdarzeń, w raportach i dziennikach wykonywania zadań.

Definiowanie adresu serwera proxy KSN pod kątem pakietów instalacyjnych

W przypadku zmiany adresu lub domeny Serwera administracyjnego, możesz zdefiniować adres serwera proxy KSN dla pakietu instalacyjnego.

W celu zdefiniowania adresu serwera proxy KSN dla pakietu instalacyjnego:

1. W drzewie konsoli, w folderze **Zdalna instalacja**, kliknij dwukrotnie podfolder **Pakiety instalacyjne**.
2. W otwartym menu wybierz **Właściwości**.
3. W otwartym oknie właściwości wybierz podsekcję **Ogólne**.
4. W podsekcji **Ogólne** okna właściwości wprowadź adres serwera proxy KSN.

Pakiety instalacyjne będą używać tego adresu domyślnie.

Pobieranie aktualnych wersji aplikacji

Kaspersky Security Center pozwala na pobieranie aktualnych wersji aplikacji korporacyjnych przechowywanych na serwerach Kaspersky.

W celu pobrania aktualnych wersji aplikacji korporacyjnych firmy Kaspersky:

1. Wykonaj jedną z poniższych czynności:

   - W drzewie konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego, upewnij się, że zakładka **Monitorowanie** jest wybrana, a w sekcji **Wdrażanie** kliknij odnośnik **Dostępne są nowe wersje produktów Kaspersky**.

     Odnośnik **Dostępne są nowe wersje produktów Kaspersky** stanie się widoczny, gdy Serwer administracyjny odnajdzie nową wersję aplikacji korporacyjnej na serwerze Kaspersky.

   - W drzewie konsoli wybierz **Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**, a w obszarze roboczym kliknij **Akcje dodatkowe** i z listy rozwijalnej wybierz **Wyświetl aktualne wersje aplikacji Kaspersky**.

   Zostanie wyświetlona lista bieżących wersji aplikacji Kaspersky.

2. Możesz filtrować listę aplikacji Kaspersky, aby uprościć wyszukiwanie wymaganej aplikacji.

   W górnej części okna **Aktualne wersje aplikacji** kliknij odnośnik **Filtr**, aby przefiltrować listę aplikacji według następujących kryteriów:

   - **Komponenty**. Użyj tego kryterium, aby przefiltrować listę aplikacji Kaspersky według obszarów ochrony używanych w Twojej sieci.
   - **Typ pobieranego oprogramowania**. Użyj tego kryterium, aby przefiltrować listę aplikacji Kaspersky według typu aplikacji.

- **Wyświetlane oprogramowanie i aktualizacje**. Użyj tego kryterium, aby wyświetlić dostępne aplikacje firmy Kaspersky według określonych wersji.

- **Wyświetlane wersje językowe oprogramowania i aktualizacji**. Użyj tego kryterium, aby wyświetlić aplikacje Kaspersky z określonym językiem lokalizacji.

Kliknij przycisk **Zastosuj**, aby zastosować wybrane filtry.

3. Z listy wybierz żądaną aplikację.

4. Pobierz pakiet dystrybucyjny aplikacji, klikając odnośnik w wierszu **Adres internetowy pakietu dystrybucyjnego**.

> Aktualizacje zarządzanych aplikacji mogą wymagać zainstalowania określonej minimalnej wersji Kaspersky Security Center. Jeśli ta wersja jest nowsza niż aktualna wersja, te aktualizacje są wyświetlane, ale nie można ich zatwierdzić. Ponadto żadne pakiety instalacyjne nie mogą być tworzone z takich aktualizacji, dopóki nie zaktualizujesz Kaspersky Security Center. Zostaniesz poproszony o uaktualnienie instancji Kaspersky Security Center do wymaganej wersji minimalnej.

Jeżeli dla wybranej aplikacji wyświetlony jest przycisk **Pobierz aplikacje i utwórz pakiety instalacyjne**, możesz go kliknąć w celu automatycznego pobrania pakietu dystrybucyjnego aplikacji i utworzenia pakietu instalacyjnego. Kaspersky Security Center pobierze pakiet dystrybucyjny aplikacji na Serwer administracyjny, do folderu współdzielonego określonego w trakcie instalacji Kaspersky Security Center. Automatycznie utworzony pakiet instalacyjny jest wyświetlany w drzewie konsoli, w folderze **Zdalna instalacja**, w podfolderze **Pakiety instalacyjne**.

> Po zamknięciu okna **Aktualne wersje aplikacji**, odnośnik **Dostępne są nowe wersje produktów Kaspersky** znika z sekcji **Wdrażanie**.

Możesz utworzyć pakiety instalacyjne dla nowych wersji aplikacji i zarządzać nowo utworzonymi pakietami instalacyjnymi w drzewie konsoli, w folderze **Zdalna instalacja**, podfolderze **Pakiety instalacyjne**.

Możesz także otworzyć okno **Aktualne wersje aplikacji**, klikając odnośnik **Wyświetl aktualne wersje aplikacji Kaspersky** w obszarze roboczym folderu **Pakiety instalacyjne**.

Przygotowanie urządzenia z systemem Windows do zdalnej instalacji

Zdalna instalacja aplikacji na urządzeniu klienckim może zakończyć się błędem z następujących powodów:

- Zadanie to było już wykonane na tym urządzeniu i zakończyło się powodzeniem.

  W tym przypadku zadanie nie musi być wykonywane ponownie.

- W momencie uruchamiania zadania urządzenie było wyłączone.

  W tym przypadku wyłącz urządzenie i ponownie uruchom zadanie.

- Nie istnieje połączenie między Serwerem administracyjnym a Agentem sieciowym zainstalowanym na urządzeniu klienckim.

  Aby określić przyczynę wystąpienia tego problemu, użyj narzędzia do zdalnej diagnostyki urządzeń klienckich (klactgui).

- Jeśli na urządzeniu nie ma zainstalowanego Agenta sieciowego, podczas zdalnej instalacji mogą wystąpić następujące problemy:
  - Na urządzeniu klienckim jest włączona opcja **Wyłącz proste udostępnianie plików**.
  - Na urządzeniu klienckim nie jest uruchomiona usługa serwera.
  - Na urządzeniu klienckim zamknięte są wymagane porty.
  - Konto, z poziomu którego wykonywane jest zadanie, ma niewystarczające uprawnienia.

  Aby uniknąć problemów, które mogą wystąpić podczas instalacji aplikacji na urządzeniu klienckim bez zainstalowanego Agenta sieciowego, należy postępować zgodnie z opisem procedury wymuszonego wdrożenie przy użyciu zadania zdalnej instalacji z Kaspersky Security Center.

Wcześniej wykorzystywano narzędzie riprep, aby przygotować urządzenie do zdalnej instalacji. Obecnie uważa się, że jest to przestarzała metoda konfiguracji systemów operacyjnych. Narzędzie riprep nie jest zalecane do stosowania w systemach operacyjnych nowszych niż Windows XP i Windows Server 2003 R2.

Przygotowanie urządzenia z systemem Linux i zdalna instalacja Agenta sieciowego na urządzeniu z systemem Linux

Instalacja Agenta sieciowego składa się z dwóch kroków:

- Przygotowanie urządzenia Linux
- Instalacja zdalnego Agenta sieciowego

Przygotowanie urządzenia Linux

W celu przygotowania urządzenia z systemem Linux do zdalnej instalacji Agenta sieciowego:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Agenta sieciowego dla systemu Linux, działa jedna z obsługiwanych dystrybucji systemu Linux.
2. Pobierz pakiet instalacyjny Agenta sieciowego, korzystając z interfejsu aplikacji lub ze strony internetowej Kaspersky.
3. Upewnij się, że następujące oprogramowanie jest zainstalowane na docelowym urządzeniu Linux:
   - Sudo (dla Ubuntu 10.04, wersja Sudo to 1.7.2p1 lub nowsza)
   - Perl language interpreter wersja 5.10 lub wyższa
   - narzędzie ps
4. Przetestuj konfigurację urządzenia:
   a. Sprawdź, czy możesz połączyć się z urządzeniem poprzez klienta SSH (np. PuTTY).

Jeśli nie możesz połączyć się z urządzeniem, otwórz plik `/etc/ssh/sshd_config` i upewnij się, że następujące ustawienia posiadają odpowiednie wartości przedstawione poniżej:

```
PasswordAuthentication no
ChallengeResponseAuthentication yes
```

> Nie modyfikuj pliku /etc/ssh/sshd_config, jeśli możesz połączyć się z urządzeniem bez problemów; w przeciwnym razie podczas uruchamiania zadania zdalnej instalacji może wystąpić błąd uwierzytelniania SSH.

Zapisz plik (jeśli to konieczne) i uruchom ponownie usługę SSH przy pomocy polecenia `sudo service ssh restart`.

b. Upewnij się, że port TCP 22 jest otwarty i dostępny na nieprzypisanym urządzeniu z systemem Linux. Port TCP 22 musi być dostępny do pomyślnej instalacji Agenta sieciowego dla systemu Linux.

c. Wyłącz hasło do programu sudo dla konta użytkownika, z poziomu którego nawiązywane jest połączenie.

d. Użyj polecenia `visudo` w sudo, aby otworzyć plik konfiguracyjny sudoers.

W otwartym pliku dodaj na końcu pliku następujący wiersz: `<username> ALL = (ALL) NOPASSWD: ALL`. W tym przypadku `<username>` to konto użytkownika, które będzie używane do łączenia urządzenia przy użyciu SSH. Jeśli używasz systemu operacyjnego Astra Linux, w pliku /etc/sudoers dodaj ostatni wiersz z następującym tekstem: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

e. Zapisz plik sudoers i zamknij go.

f. Ponownie nawiąż połączenie z urządzeniem poprzez SSH i upewnij się, że usługa Sudo nie żąda wprowadzenia hasła. Możesz to zrobić, korzystając z polecenia `sudo whoami`.

5. Otwórz plik `/etc/systemd/logind.conf`, a następnie wykonaj jedną z następujących czynności:

- Określ 'nie' jako wartość dla ustawienia `KillUserProcesses=no`.
- Dla ustawienia KillExcludeUsers wpisz nazwę użytkownika konta, z poziomu którego zdalna instalacja zostanie uruchomiona, na przykład, `KillExcludeUsers=root`.

Jeśli na urządzeniu docelowym działa system Astra Linux, dodaj ciąg `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` w pliku `/home/<nazwa użytkownika>/.bashrc`, gdzie `<nazwa użytkownika>` to konto użytkownika, które ma zostać użyte do połączenia urządzenia przez SSH.

W celu zastosowania zmienionych ustawień uruchom urządzenie Linux ponownie lub wykonaj następujące polecenie:

```
sudo systemctl restart systemd-logind.service
```

6. Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym SUSE Linux Enterprise Server 15, w pierwszej kolejności zainstaluj pakiet insserv-compat, aby skonfigurować Agenta sieciowego.

7. Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym Astra Linux działającym w trybie zamkniętego środowiska oprogramowania, wykonaj dodatkowe kroki w celu przygotowania urządzeń Astra Linux.

8. Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym RED OS 7.3.4 lub nowszym albo MSVSPHERE 9.2 lub nowszym, zainstaluj pakiet libxcrypt-compat, aby Agent sieciowy działał prawidłowo.

Instalacja zdalnego Agenta sieciowego

Zdalna instalacja Agenta sieciowego na urządzeniach Linux:

1. Pobierz i utwórz pakiet instalacyjny:

   a. Przed zainstalowaniem pakietu na urządzeniu upewnij się, że dla tego pakietu są już zainstalowane wszystkie zależności (programy i biblioteki).

   Dla każdego pakietu można wyświetlić jego zależności, korzystając z narzędzi specyficznych dla dystrybucji Linuksa, na którym ten pakiet ma zostać zainstalowany. Więcej informacji na temat narzędzi można znaleźć w dokumentacji do systemu operacyjnego.

   b. W celu utworzenia zdalnego pakietu instalacyjnego użyj następujących plików:

   - klnagent.kpd
   - akinstall.sh
   - Pakiet .deb lub .rpm Agenta sieciowego

2. Utwórz zadanie zdalnej instalacji z następującymi ustawieniami:

   - Na stronie **Settings** Kreatora tworzenia nowego zadania zaznacz pole **Using operating system resources through Administration Server**. Odznacz wszystkie pozostałe pola.
   - W oknie **Wybieranie konta do uruchomienia zadania** określ ustawienia konta użytkownika, które jest używane do łączenia urządzenia poprzez SSH.

3. Uruchom zadanie zdalnej instalacji. Użyj opcji polecenia `su`, aby zachować środowisko: `-m, -p, --preserve-environment`.

Przygotowanie urządzenia z systemem SUSE Linux Enterprise Server 15 do instalacji Agenta sieciowego

W celu zainstalowania Agenta sieciowego na urządzeniu z systemem operacyjnym SUSE Linux Enterprise Server 15,

przed instalacją Agenta sieciowego uruchom następujące polecenie:

```
sudo zypper install insserv-compat
```

To umożliwia zainstalowanie pakietu insserv-compat i poprawne skonfigurowanie Agenta sieciowego.

Uruchom polecenie `rpm -q insserv-compat`, aby sprawdzić, czy pakiet jest już zainstalowany.

Jeśli Twoja sieć obejmuje wiele urządzeń z systemem SUSE Linux Enterprise Server 15, możesz użyć specjalnego oprogramowania do konfigurowania i zarządzania infrastrukturą firmy. Korzystając z tego oprogramowania, możesz automatycznie zainstalować pakiet insserv-compat na wszystkich niezbędnych urządzeniach jednocześnie. Na przykład, możesz użyć Puppet, Ansible, Chef lub możesz utworzyć własny skrypt — użyj dowolnej wygodnej dla siebie metody.

Jeśli urządzenie nie ma kluczy podpisywania GPG dla SUSE Linux Enterprise, może pojawić się następujące ostrzeżenie: `Package header is not signed!` Wybierz `i` opcję, aby zignorować ostrzeżenie.

Oprócz instalacji pakietu insserv-compat, upewnij się, że całkowicie przygotowałeś swoje urządzenia z systemem Linux. Następnie, wdróż i zainstaluj Agenta sieciowego.

Przygotowanie urządzenia macOS do zdalnej instalacji Agenta sieciowego

W celu przygotowania urządzenia z systemem macOS do zdalnej instalacji Agenta sieciowego:

1. Upewnij się, że narzędzie sudo jest zainstalowane na docelowym urządzeniu macOS.

2. Przetestuj konfigurację urządzenia:

   a. Upewnij się, że port 22 jest otwarty na urządzeniu klienckim. Aby to zrobić w **Preferencjach systemowych** otwórz panel **Udostępnianie** i upewnij się, że pole **Zdalne logowanie** jest zaznaczone.

   Możesz połączyć się z urządzeniem klienckim przez Secure Shell (SSH) tylko przez port 22. Nie można zmienić numeru portu.

   Możesz użyć polecenia `ssh <nazwa_urządzenia>`, aby zdalnie zalogować się na urządzenie macOS. W panelu **Udostępnianie** możesz użyć opcji **Zezwalaj na dostęp przez**, aby określić zakres użytkowników, którzy mogą uzyskać dostęp do urządzenia macOS.

   b. Wyłącz hasło do programu sudo dla konta użytkownika, z poziomu którego nawiązywane jest połączenie.

   Użyj polecenia `sudo visudo` w Terminalu, aby otworzyć plik konfiguracyjny sudoers. W otwartym pliku, we wpisie `Specyfikacja uprawnień użytkownika` określ następujące elementy: `username ALL = (ALL) NOPASSWD: ALL`. W tym przypadku `username` to konto użytkownika, które będzie używane do łączenia urządzenia przy użyciu SSH.

   c. Zapisz plik sudoers i zamknij go.

   d. Ponownie nawiąż połączenie z urządzeniem poprzez SSH i upewnij się, że usługa Sudo nie żąda wprowadzenia hasła. Możesz to zrobić, korzystając z polecenia `sudo whoami`.

3. Pobierz i utwórz pakiet instalacyjny:

   a. Pobierz pakiet instalacyjny Agenta sieciowego, korzystając z jednej z następujących metod:

   - W drzewie konsoli, otwierając menu kontekstowe na **Zdalna instalacja → Pakiety instalacyjne** i wybierając **Pokaż aktualne wersje aplikacji**, aby wybrać z dostępnych pakietów
   - Pobierając odpowiednią wersję Agenta sieciowego ze strony internetowej pomocy technicznej: https://support.kaspersky.com/pl
   - Prosząc specjalistów z pomocy technicznej o pakiet

b. W celu utworzenia zdalnego pakietu instalacyjnego użyj następujących plików:

- klnagent.kud
- install.sh
- klnagentmac.dmg

4. Utwórz zadanie zdalnej instalacji z następującymi ustawieniami:

- Na stronie **Ustawienia** Kreatora tworzenia nowego zadania zaznacz pole **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**. Odznacz wszystkie pozostałe pola.
- Na stronie **Wybieranie konta do uruchomienia zadania** określ ustawienia konta użytkownika, które jest używane do łączenia urządzenia poprzez SSH.

Urządzenie klienckie jest gotowe do zdalnej instalacji Agenta sieciowego za pośrednictwem odpowiedniego zadania, które utworzyłeś.

Aplikacje Kaspersky: licencjonowanie i aktywacja

Ta sekcja opisuje funkcje Kaspersky Security Center związane z pracą z kluczami licencyjnymi dla zarządzanych aplikacji Kaspersky.

Kaspersky Security Center pozwala na wykonywanie scentralizowanego rozsyłania kluczy licencyjnych dla aplikacji Kaspersky na urządzenia klienckie, monitorowanie ich wykorzystania i odnawianie licencji.

Dodając klucz licencyjny przy pomocy Kaspersky Security Center, jego ustawienia są zapisywane na Serwerze administracyjnym. W oparciu o te informacje, aplikacja generuje raport użycia klucza licencyjnego i powiadamia administratora o wygaśnięciu licencji oraz naruszeniu ograniczeń licencyjnych, określonych we właściwościach kluczy licencyjnych. Możesz skonfigurować powiadomienia związane z korzystaniem z kluczy licencyjnych w ustawieniach Serwera administracyjnego.

Licencjonowanie zarządzanych aplikacji

Aplikacje Kaspersky, zainstalowane na zarządzanych urządzeniach, muszą być licencjonowane poprzez zastosowanie pliku klucza lub kodu aktywacyjnego do każdej z aplikacji. Plik klucza lub kod aktywacyjny może zostać rozesłany w następujące sposoby:

- Automatyczne wdrażanie
- Pakiet instalacyjny zarządzanej aplikacji
- Zadanie *Dodaj klucz licencyjny* dla zarządzanej aplikacji
- Ręczna aktywacja zarządzaną aplikacją

Możesz dodać nowy aktywny lub zapasowy klucz licencyjny za pomocą dowolnej z metod wymienionych powyżej. Aplikacja firmy Kaspersky używa w danej chwili aktywnego klucza i przechowuje klucz rezerwowy do zastosowania po wygaśnięciu aktywnego klucza. Aplikacja, dla której dodajesz klucz licencyjny, określa, czy klucz jest aktywny, czy zapasowy. Definicja klucza nie zależy od metody użytej do dodania nowego klucza licencyjnego.

Automatyczne wdrażanie

Jeśli używasz różnych zarządzanych aplikacji i musisz rozesłać określony plik klucza lub kod aktywacyjny na urządzenia, zdecyduj się na inne sposoby wdrożenia tego kodu aktywacyjnego lub pliku klucza.

Kaspersky Security Center umożliwia automatyczne rozesłanie dostępnych kluczy licencyjnych na urządzenia. Na przykład, trzy klucze licencyjne są przechowywane w repozytorium Serwera administracyjnego. Zaznaczyłeś pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia** dla wszystkich trzech kluczy licencyjnych. Aplikacja zabezpieczająca Kaspersky—na przykład Kaspersky Endpoint Security for Windows—jest zainstalowana na urządzeniach w organizacji. Zostanie wykryte nowe urządzenie, do którego musi być rozesłany klucz licencyjny. Aplikacja określi, na przykład, że na urządzenie mogą zostać rozesłane dwa klucze licencyjne z repozytorium: klucz licencyjny o nazwie *Key_1* oraz klucz licencyjny o nazwie *Key_2*. Jeden z tych kluczy licencyjnych zostanie zastosowany na urządzeniu. W tym przypadku nie można przewidzieć, który z dwóch kluczy licencyjnych zostanie wdrożony na urządzeniu, ponieważ automatyczne wdrażanie kluczy licencyjnych nie oferuje administratorowi podejmowania żadnych działań.

Podczas rozsyłania klucza licencyjnego urządzenia są zliczane dla tego klucza licencyjnego. Musisz upewnić się, że liczba urządzeń, na których klucz licencyjny został zastosowany, nie przekracza limitu określonego przez licencję. Jeśli liczba urządzeń przekracza limit określony przez licencję, wszystkie urządzenia, które nie zostały objęte licencją, otrzymają stan *Krytyczny*.

Przed wdrożeniem, plik klucza lub kod aktywacyjny musi zostać dodany do repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Automatyczne rozsyłanie kluczy licencyjnych

  lub
- Kaspersky Security Center Web Console:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Automatyczne rozsyłanie kluczy licencyjnych

Należy pamiętać, że automatycznie dystrybuowany klucz licencyjny może nie zostać wyświetlony w repozytorium wirtualnego Serwera administracyjnego w następujących przypadkach:

- Klucz licencyjny nie jest ważny dla aplikacji.
- Wirtualny Serwer administracyjny nie ma zarządzanych urządzeń.
- Klucz licencyjny został już użyty dla urządzeń zarządzanych przez inny wirtualny Serwer administracyjny i osiągnięto limit liczby urządzeń.

Dodawanie pliku klucza lub kodu aktywacyjnego do pakietu instalacyjnego zarządzanej aplikacji

Z powodów bezpieczeństwa, ta opcja nie jest zalecana. Plik klucza lub kod aktywacyjny dodane do pakietu instalacyjnego mogą być zagrożone.

Jeśli instalujesz zarządzaną aplikację przy użyciu pakietu instalacyjnego, możesz określić kod aktywacyjny lub plik klucza w tym pakiecie instalacyjnym lub w zasadzie aplikacji. Klucz licencyjny zostanie rozesłany na zarządzane urządzenia podczas kolejnej synchronizacji urządzenia z Serwerem administracyjnym.

Dostępne instrukcje:

- Konsola administracyjna:
  - Tworzenie pakietu instalacyjnego
  - Instalowanie aplikacji na urządzeniach klienckich

  lub
- Kaspersky Security Center Web Console: Dodawanie klucza licencyjnego do pakietu instalacyjnego

Wdrażanie poprzez zadanie Dodaj klucz licencyjny dla zarządzanej aplikacji

Jeśli zdecydujesz się na użycie zadania *Dodaj klucz licencyjny* dla zarządzanej aplikacji, możesz wybrać klucz licencyjny, który musi zostać rozesłany na urządzenia, oraz wybrać urządzenia w dowolny sposób—na przykład, wybierając grupę administracyjną lub wybór urządzeń.

Przed wdrożeniem, plik klucza lub kod aktywacyjny musi zostać dodany do repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Rozsyłanie klucza licencyjnego na urządzenia klienckie

  lub
- Kaspersky Security Center Web Console:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Rozsyłanie klucza licencyjnego na urządzenia klienckie

Ręczne dodawanie kodu aktywacyjnego lub pliku klucza do urządzeń

Możesz aktywować zainstalowaną aplikację Kaspersky lokalnie, przy użyciu narzędzi dostępnych w interfejsie aplikacji. Więcej informacji można znaleźć w dokumentacji dla zainstalowanej aplikacji.

Wyświetlanie informacji o używanych kluczach licencyjnych

W celu wyświetlenia informacji o używanych kluczach licencyjnych:

Z drzewa konsoli wybierz folder **Licencje Kaspersky**.

Obszar roboczy folderu wyświetli listę kluczy licencyjnych wykorzystywanych na urządzeniach klienckich.

Obok każdego z kluczy licencyjnych wyświetlana jest ikona odpowiadająca typowi użycia:

-  —informacja o aktualnie używanym kluczu licencyjnym jest uzyskiwana z urządzenia klienckiego podłączonego do Serwera administracyjnego. Plik tego klucza licencyjnego jest przechowywany poza Serwerem administracyjnym.
-  —Klucz licencyjny jest przechowywany w repozytorium Serwera administracyjnego. Automatyczne rozsyłanie jest wyłączone dla tego klucza licencyjnego.
-  —Klucz licencyjny jest przechowywany w repozytorium Serwera administracyjnego. Automatyczne rozsyłanie jest włączone dla tego klucza licencyjnego.

Możesz wyświetlić informacje dotyczące kluczy licencyjnych używanych do aktywacji aplikacji na urządzeniu klienckim, otwierając sekcję **Aplikacje** okna właściwości urządzenia klienckiego.

Aby określić aktualne ustawienia kluczy licencyjnych wirtualnego Serwera administracyjnego, Serwer administracyjny wysyła żądanie do serwerów aktywacji Kaspersky przynajmniej raz dziennie. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS.

Jeśli klucz licencyjny zostanie odebrany z urządzenia klienckiego, nie będzie można go wyeksportować jako plik.

Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego

W celu dodania klucza licencyjnego do repozytorium Serwera administracyjnego:

1. Z drzewa konsoli wybierz folder **Licencje Kaspersky**.
2. Uruchom zadanie dodawania kluczy licencyjnych w jeden z następujących sposobów:
   - Z menu kontekstowego listy kluczy licencyjnych wybierz **Dodaj kod aktywacyjny lub plik klucza**.
   - Kliknij odnośnik **Dodaj kod aktywacyjny lub plik klucza**, dostępny w obszarze roboczym listy kluczy licencyjnych.
   - Kliknij przycisk **Dodaj kod aktywacyjny lub plik klucza**.

   Zostanie uruchomiony kreator Kreator dodawania klucza licencyjnego.
3. Wybierz sposób aktywacji Serwera administracyjnego: przy użyciu kodu aktywacyjnego lub przy użyciu pliku klucza.
4. Określ kod aktywacyjny lub plik klucza.
5. Wybierz opcję **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**, jeśli chcesz natychmiast rozesłać odpowiedni klucz licencyjny w swojej sieci. Jeśli nie wybierzesz tej opcji, możesz ręcznie rozpowszechniać klucz licencyjny później.

W rezultacie plik klucza jest pobierany, a działanie Kreator dodawania klucza licencyjnego zakończone. Teraz dodany klucz licencyjny można znaleźć na liście licencji Kaspersky.

Usuwanie klucza licencyjnego Serwera administracyjnego

W celu usunięcia klucza licencyjnego z Serwera administracyjnego:

1. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego wybierz sekcję **Klucze licencyjne**.
3. Usuń klucz licencyjny, klikając przycisk **Usuń**.

Klucz licencyjny zostanie usunięty.

Jeśli dodano zapasowy klucz licencyjny, zapasowy klucz licencyjny automatycznie staje się aktywnym kluczem licencyjnym po wcześniejszym usunięciu aktywnego klucza licencyjnego.

Po usunięciu aktywnego klucza licencyjnego Serwera administracyjnego, funkcje Zarządzanie lukami i poprawkami i Zarządzanie urządzeniami mobilnymi staną się dostępne. Możesz ponownie dodać usunięty klucz licencyjny lub dodać nowy klucz licencyjny.

Rozsyłanie klucza licencyjnego na urządzenia klienckie

Kaspersky Security Center pozwala na rozesłanie klucza licencyjnego na urządzenia klienckie przy pomocy zadania *Rozsyłanie klucza licencyjnego*.

Przed wdrożeniem należy dodać klucz licencyjny do repozytorium Serwera administracyjnego.

W celu rozesłania klucza licencyjnego na urządzenia klienckie:

1. Z drzewa konsoli wybierz folder **Licencje Kaspersky**.
2. W obszarze roboczym listy kluczy licencyjnych kliknij przycisk **Automatycznie roześlij klucz licencyjny do zarządzanych urządzeń**.

   Zostanie uruchomiony **Kreator tworzenia zadania aktywacji aplikacji**. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Na liście aplikacji wybierz aplikację, dla której chcesz utworzyć zadanie.
4. W kroku **Dodaj klucz** kreatora dodaj klucz licencyjny, korzystając z jednej z następujących opcji:
   - Wybierz opcję **Kod aktywacyjny**, aby dodać kod aktywacyjny z repozytorium Kaspersky Security Center.

     Kliknij **Wybierz**. W oknie, które zostanie otwarte, wybierz kod aktywacyjny, a następnie kliknij **OK**.
   - Wybierz opcję **Plik klucza lub klucz**, a następnie wykonaj następujące czynności:

     a. Kliknij **Wybierz**.

     b. W menu kontekstowym wybierz jedną z opcji:

     - **Plik klucza z folderu**.

       W oknie, które zostanie otwarte, wybierz plik klucza ze swojego komputera i kliknij **Otwórz**.
     - **Klucz z repozytorium Kaspersky Security Center**.

       W otwartym oknie wybierz klucz z repozytorium Kaspersky Security Center, a następnie kliknij przycisk **OK**.
5. Jeśli chcesz zastąpić bieżący aktywny klucz licencyjny, odznacz domyślne pole wyboru **Użyj klucza jako zapasowego**.

   Na przykład jest to konieczne w przypadku zmiany organizacji i urządzenie wymaga klucza innej organizacji; lub jeśli klucz został wydany ponownie, a nowa licencja wygasa wcześniej niż bieżąca. Aby uniknąć błędów, odznacz pole wyboru **Użyj klucza jako zapasowego**.

   Jeśli chcesz uzyskać więcej informacji o problemach, które mogą wystąpić podczas dodawania klucza licencyjnego do Kaspersky Security Center Windows, oraz o sposobach ich rozwiązania, zapoznaj się z bazą wiedzy Kaspersky Security Center.
6. Sprawdź informacje o kluczu licencyjnym, a następnie kliknij **Dalej**.

7. W tym kroku kreatora wybierz urządzenia, do których chcesz przypisać zadanie dodawania klucza. Urządzenia można określić (maksymalnie do 1000 urządzeń) w jeden z następujących sposobów:

   - **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**. W tym przypadku zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

   - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**. Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

   - **Przypisz zadanie do wyboru urządzeń**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonym wyborze. Możesz określić predefiniowany lub niestandardowy wybór, który utworzyłeś.

   - **Przypisz zadanie do grupy administracyjnej**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonej grupie administracyjnej.

8. W kroku **Konfiguruj terminarz zadania** kreatora utwórz terminarz uruchomienia zadania:

   - **Zaplanowane uruchomienie**:

     - **Raz**

       Zadanie zostanie uruchomione raz, w określonym dniu i o określonej godzinie (domyślnie w dniu utworzenia zadania).

     - **Ręcznie**

       Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

       Domyślnie opcja ta jest zaznaczona.

     - **Po pobraniu nowych uaktualnień do repozytorium**

       Zadanie jest uruchamiane po pobraniu uaktualnień do repozytorium. Na przykład, możesz użyć tego terminarza dla zadania wyszukiwania luk i wymaganych aktualizacji.

     - **Po epidemii wirusa**

       Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

       - Ochrona antywirusowa stacji roboczych i serwerów plików
       - Ochrona antywirusowa bram internetowych
       - Ochrona antywirusowa serwerów pocztowych

       Domyślnie, zaznaczone są wszystkie typy aplikacji.

       Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

     - **Po zakończeniu wykonywania innego zadania**

       Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

- Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
- Kliknij ikonę sortowania, aby posortować zadania według nazwy.

  Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
- Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

9. W kroku **Określ nazwę zadania** kreatora podaj nazwę zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

10. W kroku **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

    Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Zadania utworzone przy pomocy **Kreator tworzenia zadania aktywacji aplikacji** dla określonych urządzeń są przechowywane w folderze **Zadania** drzewa konsoli.

Możesz również utworzyć grupowe lub lokalne zadanie rozsyłania klucza licencyjnego przy pomocy Kreatora tworzenia zadania dla grupy administracyjnej i dla urządzenia klienckiego.

Automatyczne rozsyłanie kluczy licencyjnych

Kaspersky Security Center umożliwia automatyczne instalowanie kluczy licencyjnych na zarządzanych urządzeniach, jeśli znajdują się one w repozytorium kluczy licencyjnych na Serwerze administracyjnym. Automatyczna dystrybucja kluczy licencyjnych nie dotyczy urządzeń znajdujących się w folderze **Urządzenia nieprzypisane**.

W celu automatycznego rozsyłania kluczy licencyjnych do zarządzanych urządzeń:

1. Z drzewa konsoli wybierz folder **Licencje Kaspersky**.
2. W obszarze roboczym folderu wybierz klucz licencyjny, który chcesz automatycznie rozesłać na urządzenia.
3. Otwórz okno właściwości wybranego klucza licencyjnego na jeden z następujących sposobów:
   - Z menu kontekstowego klucza licencyjnego wybierz **Właściwości**.
   - Klikając odnośnik **Pokaż właściwości klucza licencyjnego** w oknie z informacjami dla wybranego klucza licencyjnego.
4. W otwartym oknie właściwości klucza licencyjnego zaznacz pole **Klucz licencyjny rozesłany automatycznie**. Zamknij okno właściwości klucza licencyjnego.

Klucz licencyjny zostanie automatycznie rozesłany do wszystkich kompatybilnych urządzeń.

Rozsyłanie klucza licencyjnego odbywa się przy pomocy Agenta sieciowego. Dla aplikacji nie są tworzone żadne zadania rozsyłania kluczy licencyjnych.

Podczas automatycznego rozsyłania klucza licencyjnego brane jest pod uwagę ograniczenie licencyjne dotyczące liczby urządzeń (ograniczenie licencyjne jest ustawione we właściwościach klucza licencyjnego). Jeśli ograniczenie licencyjne zostanie osiągnięte, rozesłanie tego klucza licencyjnego na urządzenia zostanie przerwane automatycznie.

Wirtualny Serwer administracyjny automatycznie dystrybuuje klucze licencyjne ze swojego repozytorium oraz z repozytorium Serwera administracyjnego. Zalecamy:

- Użyj zadania *Dodaj klucz licencyjny*, aby wybrać klucz licencyjny do wdrożenia na urządzeniach.
- Unikaj wyłączania opcji **Zezwól na automatyczne wdrażanie kluczy licencyjnych z tego wirtualnego Serwera administracyjnego do jego urządzeń** w ustawieniach wirtualnego Serwera administracyjnego. W przeciwnym razie wirtualny Serwer administracyjny nie będzie dystrybuował kluczy licencyjnych do urządzeń, łącznie z kluczami licencyjnymi z repozytorium Serwera administracyjnego.

Jeśli zaznaczysz pole **Klucz licencyjny rozesłany automatycznie** w oknie właściwości klucza licencyjnego, klucz licencyjny jest natychmiast rozpowszechniany w Twojej sieci. Jeśli nie wybierzesz tej opcji, możesz ręcznie rozpowszechniać klucz licencyjny później.

Tworzenie i przeglądanie raportu użycia klucza licencyjnego

W celu utworzenia raportu z wykorzystania kluczy licencyjnych na urządzeniach klienckich:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Wybierz szablon raportu o nazwie **Raport użycia klucza licencyjnego** lub utwórz nowy szablon raportu tego samego typu.

Obszar roboczy raportu użycia klucza licencyjnego wyświetli informacje o aktywnych i zapasowych kluczach licencyjnych używanych na urządzeniach klienckich. Raport zawiera również informacje o urządzeniach, na których używane są klucze licencyjne, oraz o ograniczeniach określonych we właściwościach tych kluczy licencyjnych.

Przeglądanie informacji o kluczach licencyjnych aplikacji

W celu sprawdzenia, jakie klucze licencyjne są używane w aplikacji Kaspersky:

1. W drzewie konsoli Kaspersky Security Center wybierz węzeł **Zarządzane urządzenia** i przejdź na zakładkę **Urządzenia**.
2. Kliknij żądane urządzenie prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Właściwości**.
3. W otwartym oknie właściwości urządzenia wybierz sekcję **Aplikacje**.
4. Na liście aplikacji, która zostanie wyświetlona, wybierz aplikację, której klucze licencyjne chcesz przejrzeć, i kliknij przycisk **Właściwości**.
5. W oknie właściwości aplikacji wybierz sekcję **Klucze licencyjne**.

   Informacje są wyświetlane w obszarze roboczym tej sekcji.

Eksportowanie pliku klucza licencyjnego

Jeśli klucz licencyjny został przypadkowo usunięty i chcesz go przywrócić, możesz wyeksportować plik klucza licencyjnego z innego Serwera administracyjnego.

Aby wyeksportować plik klucza licencyjnego, musisz mieć opcję **Eksportuj plik klucza** w obszarze funkcjonalnym **Funkcje ogólne: Zarządzanie kluczami**.

Jeśli klucz licencyjny zostanie odebrany z urządzenia klienckiego, nie będzie można go wyeksportować.

Aby wyeksportować klucz licencyjny:

1. Z drzewa konsoli wybierz folder **Licencje Kaspersky**.
2. Na liście licencji wybierz klucz licencyjny, który chcesz wyeksportować jako plik.
3. W otwartym oknie informacyjnym kliknij łącze **Eksportuj plik klucza**.
4. W oknie, które zostanie otwarte, określ ścieżkę do folderu, w którym chcesz zapisać plik klucza licencyjnego, a następnie określ nazwę pliku. Następnie kliknij **Zapisz**.

Plik klucza licencyjnego w formacie .key zostanie wyeksportowany do wybranego folderu.

Jeśli klucz licencyjny, którego plik wyeksportowałeś został dodany do repozytorium Serwera administracyjnego jako kod aktywacyjny i chcesz dodać wyeksportowany plik klucza licencyjnego do repozytorium innego Serwera administracyjnego, musisz dodać go jako kod aktywacyjny, a nie jako plik klucza. W przeciwnym wypadku wystąpi błąd. Musisz otworzyć wyeksportowany plik klucza licencyjnego w dowolnym edytorze tekstu, a następnie skopiować kod aktywacyjny.

Konfigurowanie ochrony sieci

Ta sekcja zawiera informacje o ręcznej konfiguracji zasad i zadań, informacje o rolach użytkownika, informacje o tworzeniu struktury grupy administracyjnej oraz hierarchii zadań.

Scenariusz: Konfigurowanie ochrony sieci

Kreator wstępnej konfiguracji tworzy zasady i zadania z domyślnymi ustawieniami. Te ustawienia mogą okazać się nieoptymalne lub nawet niedopuszczalne przez organizację. Dlatego zalecane jest dostrojenie tych zasad i zadań oraz utworzenie innych zasad i zadań, jeśli są konieczne w Twojej sieci.

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Zainstalowano Serwer administracyjny Kaspersky Security Center
- Zainstalowano Kaspersky Security Center Web Console (opcjonalne)
- Zakończyłeś główny scenariusz instalacji Kaspersky Security Center

- Zakończono działanie kreatora wstępnej konfiguracji lub ręcznie utworzono następujące zasady i zadania w grupie administracyjnej **Zarządzane urządzenia**:
  - Zasada Kaspersky Endpoint Security
  - Grupowe zadanie aktualizacji Kaspersky Endpoint Security
  - Zasada Agenta sieciowego
  - Zadanie *Wyszukiwania luk i wymaganych aktualizacji*

Konfigurowanie ochrony sieci odbywa się w etapach:

1. **Konfiguracja i przesyłanie zasad i profili zasad aplikacji firmy Kaspersky**

   Aby skonfigurować i przesłać ustawienia dla aplikacji Kaspersky, zainstalowanych na zarządzanych urządzeniach, możesz użyć dwóch różnych metod zarządzania ochroną—skoncentrowaną na urządzeniu lub skoncentrowaną na użytkowniku. Te dwie metody można także połączyć. Aby zaimplementować zarządzanie ochroną skoncentrowaną na urządzeniu, możesz użyć narzędzi dostarczonych w Konsoli administracyjnej opartej na Microsoft Management Console lub Kaspersky Security Center Web Console. Zarządzanie ochroną skoncentrowaną na użytkowniku może zostać zaimplementowane tylko poprzez Kaspersky Security Center Web Console.

2. **Konfigurowanie zadań zdalnego zarządzania aplikacjami firmy Kaspersky**

   Sprawdź zadania utworzone przy pomocy kreatora wstępnej konfiguracji i dostosuj je (jeśli to konieczne).

   Dostępne instrukcje:

   - Konsola administracyjna:
     - Konfigurowanie grupowego zadania aktualizacji Kaspersky Endpoint Security
     - Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
   - Kaspersky Security Center Web Console:
     - Konfigurowanie grupowego zadania aktualizacji Kaspersky Endpoint Security
     - Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

   Jeśli to konieczne, utwórz dodatkowe zadania do zarządzania aplikacjami firmy Kaspersky, zainstalowanymi na urządzeniach klienckich.

3. **Oszacowanie i ograniczenie nagromadzenia zdarzeń w bazie danych**

   Informacje o zdarzeniach występujących podczas działania zarządzanych aplikacji są przesyłane z urządzenia klienckiego i zapisywane w bazie danych Serwera administracyjnego. Aby zmniejszyć obciążenie na Serwerze administracyjnym, oszacuj i ogranicz maksymalną liczbę zdarzeń przechowywanych w bazie danych.

   Dostępne instrukcje:

   - Konsola administracyjna: Konfigurowanie maksymalnej liczby zdarzeń
   - Kaspersky Security Center Web Console: Konfigurowanie maksymalnej liczby zdarzeń

Wyniki

Po zakończeniu tego scenariusza, Twoja sieć będzie chroniona przez konfigurację aplikacji Kaspersky, zadania i zdarzenia otrzymane przez Serwer administracyjny:

- Aplikacje firmy Kaspersky są konfigurowane zgodnie z zasadami i profilami zasad.
- Aplikacje są zarządzane za pośrednictwem zestawu zadań.
- Maksymalna liczba zdarzeń, jaka może być przechowywana w bazie danych, została ustawiona.

Jeśli konfiguracja ochrony sieci zostanie zakończona, możesz przejść do konfigurowania regularnych aktualizacji baz danych i aplikacji Kaspersky.

Więcej informacji o sposobie konfiguracji automatycznych odpowiedzi na zagrożenia wykryte przez Kaspersky Sandbox można znaleźć w pomocy online Kaspersky Sandbox 2.0.

Konfiguracja i przydzielanie zasad: Metoda skoncentrowana na urządzeniu

Po zakończeniu tego scenariusza, aplikacje zostaną skonfigurowane na wszystkich zarządzanych urządzeniach zgodnie z zasadami i profilami zasad aplikacji, które określiłeś.

Wymagania wstępne

Przed rozpoczęciem konfiguracji upewnij się, że pomyślnie zainstalowano Serwer administracyjny Kaspersky Security Center i Kaspersky Security Center Web Console (opcjonalnie). Jeśli zainstalowałeś Kaspersky Security Center Web Console, możesz wziąć pod uwagę zarządzania ochroną skoncentrowaną na użytkowniku jako alternatywę lub dodatkową opcję dla metody skoncentrowanej na urządzeniu.

Etapy

Scenariusz skoncentrowanego na urządzeniu zarządzania aplikacjami Kaspersky obejmuje następujące kroki:

1. **Konfigurowanie zasad aplikacji**

   Skonfiguruj ustawienia dla aplikacji firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach poprzez utworzenie zasady dla każdej aplikacji. Zestaw zasad zostanie przesłany na urządzenia klienckie.

   Podczas konfigurowania ochrony sieci w kreatorze szybkiego startu Kaspersky Security Center tworzy domyślną zasadę dla następujących aplikacji:

   - Kaspersky Endpoint Security for Windows — dla urządzeń klienckich z systemem Windows
   - Kaspersky Endpoint Security for Linux — dla urządzeń klienckich z Linux

Jeśli zakończyłeś proces konfiguracji przy użyciu tego kreatora, nie musisz tworzyć nowej zasady dla tej aplikacji. Przejdź do ręcznej konfiguracji zasady Kaspersky Endpoint Security.

Jeśli masz hierarchiczną strukturę kilku Serwerów administracyjnych i/lub grup administracyjnych, domyślnie podrzędne Serwery administracyjne i podrzędne grupy administracyjne dziedziczą zasady z głównego Serwera administracyjnego. Możesz wymusić dziedziczenie przez grupy podrzędne i podrzędne Serwery administracyjne, aby zabronić wszelkich modyfikacji ustawień skonfigurowanych w nadrzędnej zasadzie. Jeśli chcesz, żeby wymuszone było dziedziczenie tylko części ustawień, możesz zablokować je w zasadzie nadrzędnej. Pozostałe niezablokowane ustawienia będą dostępne do modyfikacji w zasadach podrzędnych. Utworzona hierarchia zasad umożliwi efektywne zarządzanie urządzeniami w grupach administracyjnych.

Dostępne instrukcje:

- Konsola administracyjna: Tworzenie zasady
- Kaspersky Security Center Web Console: Tworzenie zasady

2 Tworzenie profili zasad (opcjonalnie)

Jeśli chcesz, żeby urządzenia w jednej grupie administracyjnej były uruchamiane z różnymi ustawieniami zasady, utwórz profile zasad dla tych urządzeń. Profil zasad jest to inaczej podzbiór ustawień zasady. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z zasadą i uzupełnia ją zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowej" zasady, która jest aktywna na zarządzanym urządzeniu.

Korzystając z warunków aktywacji profilu, możesz zastosować różne profile zasad, na przykład, do urządzeń znajdujących się w określonej jednostce lub grupie bezpieczeństwa Active Directory, posiadającej określoną konfigurację sprzętową lub oznaczoną określonymi znacznikami. Użyj znaczników do filtrowania urządzeń, które spełniają określone kryteria. Na przykład, możesz utworzyć znacznik nazwany *Windows*, oznaczyć tym znacznikiem wszystkie urządzenia działające pod kontrolą systemu operacyjnego Windows, a następnie określić ten znacznik jako warunek aktywacji profilu zasad. W wyniku tego działania, aplikacje Kaspersky zainstalowane na wszystkich urządzeniach działających pod kontrolą systemu Windows będą zarządzane przez swój własny profil zasad.

Dostępne instrukcje:

- Konsola administracyjna:
  - Tworzenie profilu zasad
  - Tworzenie reguły aktywacji profilu zasad
- Kaspersky Security Center Web Console:
  - Tworzenie profilu zasad
  - Tworzenie reguły aktywacji profilu zasad

3 Przesyłanie zasad i profili zasad na zarządzane urządzenia

Domyślnie Serwer administracyjny automatycznie synchronizuje się z zarządzanymi urządzeniami co 15 minut. Możesz obejść automatyczną synchronizację i ręcznie uruchomić synchronizację przy pomocy polecenia Wymuś synchronizację. Synchronizacja jest również wymuszana po utworzeniu lub zmianie zasady lub profilu zasady. Podczas synchronizacji nowe lub zmienione zasady i profile zasad zostają rozesłane na zarządzane urządzenia.

Jeśli używasz Kaspersky Security Center Web Console, możesz sprawdzić, czy profile i profile zasad zostały dostarczone na urządzenie. Kaspersky Security Center określa datę i godzinę dostarczenia we właściwościach urządzenia.

Dostępne instrukcje:

- Konsola administracyjna: Wymuszona synchronizacja
- Kaspersky Security Center Web Console: Wymuszona synchronizacja

Wyniki

Po zakończeniu scenariusza skoncentrowanego na urządzeniu, aplikacje Kaspersky są konfigurowane zgodnie z ustawieniami określonymi i przesłanymi poprzez hierarchię zasad.

Skonfigurowane zasady i profile zasad aplikacji zostaną automatycznie zastosowane do nowych urządzeń dodanych do grup administracyjnych.

Informacje o metodach zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku

Możesz zarządzać ustawieniami zabezpieczeń z poziomu funkcji urządzenia i z poziomu roli użytkownika. Pierwsza metoda nosi nazwę *zarządzanie ochroną skoncentrowaną na urządzeniu*, a druga nazywa się *zarządzania ochroną skoncentrowaną na użytkowniku*. Aby zastosować różne ustawienia aplikacji na różnych urządzeniach, możesz użyć połączonych typów zarządzania. Aby zaimplementować zarządzanie ochroną skoncentrowaną na urządzeniu, możesz użyć narzędzi dostarczonych w Konsoli administracyjnej opartej na Microsoft Management Console lub Kaspersky Security Center Web Console. Zarządzanie ochroną skoncentrowaną na użytkowniku może zostać zaimplementowane tylko poprzez Kaspersky Security Center Web Console.

Zarządzanie bezpieczeństwem skoncentrowane na urządzeniu umożliwia zastosowanie różnych ustawień aplikacji zabezpieczającej na zarządzanych urządzeniach w zależności od funkcji charakterystycznych dla urządzeń. Na przykład, możesz zastosować różne ustawienia do urządzeń przydzielonych w różnych grupach administracyjnych. Możesz także rozróżnić urządzenia przy użyciu tych urządzeń w Active Directory lub ich specyfikacji sprzętowej.

Zarządzanie bezpieczeństwem skoncentrowanym na użytkowniku umożliwia zastosowanie różnych ustawień aplikacji zabezpieczającej do różnych ról użytkownika. Możesz utworzyć kilka ról użytkownika, przypisać odpowiednią rolę użytkownika do każdego użytkownika oraz określić różne ustawienia aplikacji do urządzeń należących do użytkowników z różnymi rolami. Na przykład, chcesz zastosować różne ustawienia aplikacji na urządzeniach księgowych i specjalistów z działu HR. W rezultacie, gdy zaimplementowane jest zarządzanie ochroną skoncentrowaną na użytkowniku, każdy dział—dział księgowych i dział HR—posiada swoją własną konfigurację ustawień dla aplikacji firmy Kaspersky. Konfiguracja ustawień definiuje, które ustawienia aplikacji mogą być zmieniane przez użytkowników i dla których wymuszone jest ustawienie i zablokowanie przez administratora.

Korzystając z zarządzania ochroną skoncentrowaną na użytkowniku, możesz zastosować określone ustawienia aplikacji do pojedynczych użytkowników. Może to być wymagane, gdy pracownik posiada unikatową rolę w firmie lub gdy chcesz monitorować problemy bezpieczeństwa dotyczące urządzeń określonej osoby. W zależności od roli tego pracownika w firmie, możesz rozszerzyć lub ograniczyć uprawnienia tej osoby do zmiany ustawień aplikacji. Na przykład, możesz rozszerzyć uprawnienia administratora systemu, który zarządza urządzeniami klienckimi w biurze lokalnym.

Możesz połączyć metody zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku. Na przykład, możesz skonfigurować określoną zasadę aplikacji dla każdej grupy administracyjnej, a następnie utworzyć profile zasad dla jednej lub kilku ról użytkownika Twojej firmy. W tym przypadku zasady i profile zasad są stosowane w następującej kolejności:

1. Zostaną zastosowane zasady utworzone dla zarządzania ochroną skoncentrowaną na urządzeniu.
2. Są one modyfikowane przez profile zasad zgodnie z priorytetami profili zasad.
3. Zasady są modyfikowane przez profile zasad skojarzone z rolami użytkownika.

Ręczna konfiguracja zasady Kaspersky Endpoint Security

W tej sekcji można znaleźć zalecenia dotyczące konfiguracji zasady Kaspersky Endpoint Security, który jest tworzony przez Kreator wstępnej konfiguracji. Możesz przeprowadzić konfigurację w oknie właściwości zasady.

Podczas modyfikowania ustawień należy pamiętać o kliknięciu ikony blokady nad odpowiednim ustawieniem, aby umożliwić jego użycie na stacji roboczej.

Konfigurowanie zasady w sekcji Zaawansowana ochrona przed zagrożeniami

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Zaawansowana ochrona przed zagrożeniami** możesz skonfigurować używanie Kaspersky Security Network dla Kaspersky Endpoint Security for Windows. Możesz także skonfigurować moduły Kaspersky Endpoint Security for Windows, takie jak Wykrywanie zachowań, Ochrona przed exploitami, Ochrona przed włamaniami oraz Silnik korygujący.

W podsekcji **Kaspersky Security Network** zalecane jest włączenie opcji **Kaspersky Security Network**. Użyj tej opcji do redystrybucji i optymalizacji ruchu w sieci. Jeśli opcja **Kaspersky Security Network** jest wyłączona, możesz włączyć bezpośrednie korzystanie z serwerów KSN.

Konfigurowanie zasady w sekcji Podstawowa ochrona przed zagrożeniami

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Podstawowa ochrona przed zagrożeniami** okna właściwości zasad, zalecamy określenie dodatkowych ustawień w podsekcjach **Zapora sieciowa** i **Ochrona plików**.

Podsekcja **Zapora sieciowa** zawiera ustawienia, które pozwalają kontrolować aktywność sieciową aplikacji na urządzeniach klienckich. Urządzenie klienckie korzysta z sieci, do której przypisany jest jeden z następujących statusów: publiczny, lokalny lub zaufany. W zależności od stanu sieci, Kaspersky Endpoint Security może zezwolić na aktywność sieciową na urządzeniu lub jej zabronić. Gdy dodajesz nową sieć do swojej organizacji, musisz przypisać jej odpowiedni status sieci. Na przykład, jeśli urządzeniem klienckim jest laptop, zalecamy, aby to urządzenie korzystało z sieci publicznej lub zaufanej, ponieważ laptop nie zawsze jest podłączony do sieci lokalnej. W podsekcji **Zapora sieciowa** możesz sprawdzić, czy prawidłowo przypisano stany do sieci używanych w Twojej organizacji.

W celu sprawdzenia listy sieci:

1. We właściwościach zasady przejdź do **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa**.
2. W sekcji **Dostępne sieci** kliknij przycisk **Ustawienia**.
3. W **Zapora sieciowa**, które zostanie otwarte, przejdź do zakładki **Sieci**, aby wyświetlić listę sieci.

W podsekcji **Ochrona plików** możesz wyłączyć skanowanie dysków sieciowych. Skanowanie dysków sieciowych może spowodować znaczne obciążenie dysków sieciowych. Praktyczniejsze jest wykonywanie bezpośredniego skanowania na serwerach plików.

W celu wyłączenia skanowania dysków sieciowych:

1. We właściwościach zasady przejdź do **Podstawowa ochrona przed zagrożeniami → Ochrona plików**.
2. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
3. W otwartym oknie **Ochrona plików**, na zakładce **Ogólne** odznacz pole **Wszystkie dyski sieciowe**.

Konfigurowanie zasady w sekcji Ustawienia ogólne

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Ustawienia ogólne** okna właściwości zasady zalecamy określenie dodatkowych ustawień w podsekcjach **Raporty i pliki danych** oraz **Interfejs**.

W podsekcji **Raporty i pliki danych** przejdź do sekcji **Przesyłanie danych do Serwera administracyjnego**. Pole **O uruchomionych aplikacjach** określa, czy baza danych Serwera administracyjnego ma zapisywać informacje o wszystkich wersjach wszystkich modułów oprogramowania na urządzeniach sieciowych. Jeśli to pole jest zaznaczone, zapisane informacje mogą wymagać znaczącej ilości miejsca na dysku dla bazy danych Kaspersky Security Center (kilkadziesiąt gigabajtów). Wyczyść pole **O uruchomionych aplikacjach**, jeśli jest ono zaznaczone w zasadach najwyższego poziomu.

Jeśli Konsola administracyjna zarządza ochroną antywirusową w sieci organizacji w trybie scentralizowanym, wyłącz wyświetlanie interfejsu użytkownika Kaspersky Endpoint Security for Windows na stacjach roboczych. W tym celu w podsekcji **Interfejs** przejdź do sekcji **Interakcja z użytkownikiem**, a następnie wybierz opcję **Nie wyświetlaj interfejsu użytkownika**.

Aby włączyć ochronę hasłem na stacjach roboczych, w podsekcji **Interfejs** przejdź do sekcji **Ochrona hasłem**, kliknij przycisk **Ustawienia**, a następnie zaznacz pole **Włącz ochronę hasłem**.

Konfigurowanie zasad w sekcji Konfiguracja zdarzenia

W sekcji **Konfiguracja zdarzenia** należy wyłączyć zapisywanie wszystkich zdarzeń na Serwerze administracyjnym, za wyjątkiem następujących:

- Na zakładce **Krytyczny**:
  - *Automatyczne uruchamianie aplikacji jest wyłączone*
  - *Dostęp zabroniony*
  - *Zabroniono uruchomienia aplikacji*
  - *Leczenie nie jest możliwe*
  - *Naruszenie umowy licencyjnej użytkownika końcowego*
  - *Nie można wczytać modułu szyfrującego*
  - *Nie można uruchomić dwóch zadań w tym samym czasie*
  - *Wykryto aktywne zagrożenie. Należy uruchomić zaawansowane leczenie*
  - *Wykryto atak sieciowy*
  - *Nie wszystkie składniki zostały zaktualizowane*
  - *Błąd aktywacji*
  - *Błąd podczas włączania trybu przenośnego*
  - *Błąd współdziałania z Kaspersky Security Center*
  - *Błąd podczas wyłączania trybu przenośnego*
  - *Błąd podczas zmiany składników aplikacji*
  - *Błąd podczas stosowania reguł szyfrowania/odszyfrowywania pliku*
  - *Zasada nie może zostać zastosowana*
  - *Działanie procesu zostało zakończone*
  - *Aktywność sieciowa jest zablokowana*
- Na zakładce **Błąd funkcjonalny**: *Nieprawidłowe ustawienia zadania. Ustawienia nie zostały zastosowane*

- Na karcie **Ostrzeżenie**:
  - *Autoochrona jest wyłączona*
  - *Nieprawidłowy klucz zapasowy*
  - *Użytkownik zrezygnował z zasady szyfrowania*
- Na karcie **Informacja**: *Zabroniono uruchomienia aplikacji w trybie testowym*

Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security

Optymalną i zalecaną opcją terminarza dla Kaspersky Endpoint Security w wersji 10 i nowszej jest **Po pobraniu nowych uaktualnień do repozytorium**, gdy zaznaczone jest pole **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Ręczna konfiguracja grupowego zadania skanowania urządzeń z zainstalowanym programem Kaspersky Endpoint Security

Kreator wstępnej konfiguracji tworzy grupowe zadanie skanowania urządzeń. Domyślnie skonfigurowano terminarz **uruchamiania zadania w piątki o godzinie 19:00** z automatyczną randomizacją i odznaczonym polem **Uruchom pominięte zadania**.

Oznacza to, że jeśli urządzenia w organizacji są wyłączone w piątki, na przykład o godzinie 18:30, zadanie skanowania urządzeń nigdy nie zostanie uruchomione. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego zadanie *Wyszukiwanie luk i wymaganych aktualizacji.* Domyślnie skonfigurowano terminarz **uruchamiania zadania we wtorki o godzinie 19:00** z automatyczną randomizacją i zaznaczonym polem **Uruchom pominięte zadania**.

Jeśli zasady obowiązujące w organizacji nakazują wyłączenie wszystkich urządzeń w tym czasie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* zostanie uruchomione, gdy urządzenia znowu zostaną włączone, czyli w środę rano. Takie działanie nie jest wskazane, ponieważ wykrywanie luk może zwiększać zużycie procesora i obciążenie podsystemów dysku. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Ręczna konfiguracja grupowego zadania instalacji uaktualnień i naprawy luk

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego grupowe zadanie instalacji uaktualnień i naprawy luk. Domyślnie skonfigurowano terminarz uruchamiania zadania codziennie o godzinie 01:00 z automatyczną randomizacją i wyłączoną opcją **Uruchom pominięte zadania**.

Jeśli reguły obowiązujące w organizacji nakazują wyłączanie urządzeń na noc, zadanie instalacji uaktualnień nigdy nie zostanie uruchomione. Terminarz dla zadania wykrywania luk należy skonfigurować w oparciu o zasady obowiązujące w organizacji. Należy pamiętać, że zadanie instalacji uaktualnień może wymagać ponownego uruchomienia urządzenia.

Określanie maksymalnej liczby zdarzeń w repozytorium zdarzeń

W sekcji **Repozytorium zdarzeń** okna właściwości Serwera administracyjnego możesz zmodyfikować ustawienia przechowywania zdarzeń w bazie danych Serwera administracyjnego, ograniczając liczbę wpisów zdarzeń i czas przechowywania wpisów. Jeśli określisz maksymalną liczbę zdarzeń, aplikacja oblicza przybliżoną ilość miejsca przechowywania, wymaganą dla określonej liczby. Możesz użyć tego przybliżonego obliczenia do oszacowania wystarczającej ilości wolnego miejsca na dysku, aby uniknąć przepełnienia bazy danych. Domyślna pojemność bazy danych Serwera administracyjnego wynosi 400 000 zdarzeń. Maksymalną dozwoloną pojemnością bazy danych jest 45 milionów zdarzeń.

Aplikacja sprawdza bazę danych co 10 minut. Jeśli liczba zdarzeń osiągnie określoną maksymalną wartość plus 10 000, aplikacja usunie najstarsze zdarzenia, tak aby pozostała tylko określona maksymalna liczba zdarzeń.

Jeśli Serwer administracyjny usuwa starsze zdarzenia, nie może zapisywać nowych zdarzeń do bazy danych. W tym czasie informacje o odrzuconych zdarzeniach są zapisywane w dzienniku zdarzeń aplikacji Kaspersky. Nowe zdarzenia zostają zakolejkowane, a następnie zapisane do bazy danych po zakończeniu operacji usuwania.

Aby ograniczyć liczbę zdarzeń, które mogą być przechowywane w repozytorium zdarzeń na Serwerze administracyjnym:

1. Kliknij Serwer administracyjny prawym klawiszem myszy, a następnie wybierz **Właściwości**.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. W obszarze roboczym sekcji **Repozytorium zdarzeń** określ maksymalną liczbę zdarzeń przechowywanych w bazie danych.

3. Kliknij **OK**.

Dodatkowo możesz zmienić ustawienia dowolnego zadania, aby zapisywać zdarzenia związane z postępem zadania lub zapisywać tylko wyniki wykonania zadania. Postępując w ten sposób, zmniejszysz liczbę zdarzeń w bazie danych, zwiększysz prędkość wykonywania scenariuszy skojarzonych z analizą tabeli zdarzeń w bazie danych, a także zmniejszysz ryzyko nadpisania krytycznych zdarzeń przez dużą liczbę zdarzeń.

Określenie maksymalnego okresu przechowywania informacji o wyeliminowanych lukach

W celu ustawienia maksymalnego okresu przechowywania w bazie danych informacji o lukach, które zostały już wyeliminowane na zarządzanych urządzeniach:

1. Kliknij Serwer administracyjny prawym klawiszem myszy, a następnie wybierz **Właściwości**.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. W obszarze roboczym sekcji **Repozytorium zdarzeń** określ maksymalny okres przechowywania informacji o wyeliminowanych lukach w bazie danych.

   Domyślnie okres przechowywania wynosi 90 dni.

3. Kliknij **OK**.

Maksymalny okres przechowywania informacji o wyeliminowanych lukach jest ograniczony do określonej liczby dni. Następnie zadanie konserwacji Serwera administracyjnego usunie nieaktualne informacje z bazy danych.

Zarządzanie zadaniami

Kaspersky Security Center zarządza aplikacjami zainstalowanymi na urządzeniach poprzez tworzenie i uruchamianie różnych zadań. Zadania są potrzebne do instalowania, uruchamiania i zatrzymywania działania aplikacji, skanowania plików, aktualizowania baz danych i modułów aplikacji, a także wykonywania innych działań na aplikacjach.

Zadania są podzielone na następujące typy:

- *Zadania grupowe*. Zadania wykonywane na urządzeniach wybranej grupy administracyjnej.
- *Zadania Serwera administracyjnego*. Zadania wykonywane przez Serwer administracyjny.
- *Zadania dla wskazanych urządzeń*. Zadania wykonywane na wybranych urządzeniach, niezależnie od tego, czy znajdują się w jakichkolwiek grupach administracyjnych.
- *Zadania lokalne*. Zadania wykonywane na określonym urządzeniu.

Zadanie aplikacji może być utworzone tylko wtedy, gdy wtyczka zarządzająca tą aplikacją jest zainstalowana na stacji roboczej administratora.

Możesz utworzyć listę urządzeń (maksymalnie do 1000 urządzeń), dla których zostanie utworzone zadanie, korzystając z jednej z następujących metod:

- Wybierz urządzenia z sieci wykryte przez Serwer administracyjny.
- Ręcznie określ listę urządzeń. Jako adresu urządzenia możesz użyć adresu IP (lub zakresu adresów IP), nazwy NetBIOS lub nazwy DNS.

- Zaimportuj listę urządzeń z pliku .txt zawierającego adresy dodawanych urządzeń (każdy adres powinien znajdować się w pojedynczej linii).

  Jeśli lista urządzeń jest importowana z pliku lub jest tworzona ręcznie, a urządzenia są identyfikowane po nazwie, lista może zawierać tylko urządzenia, o których informacje zostały już dodane do bazy danych Serwera administracyjnego podczas podłączania tych urządzeń lub podczas wyszukiwania urządzeń.

Dla każdej aplikacji można utworzyć dowolną liczbę zadań grupowych, zadań dla wskazanych urządzeń oraz zadań lokalnych.

Wymiana informacji o zadaniach między aplikacją zainstalowaną na urządzeniu a bazą danych Kaspersky Security Center odbywa się podczas łączenia Agenta sieciowego z Serwerem administracyjnym.

Możesz wprowadzać zmiany w ustawieniach zadań, przeglądać postęp ich wykonywania, a także kopiować, eksportować, importować i usuwać zadania.

Zadania są uruchamiane na urządzeniu tylko wtedy, gdy uruchomiona jest aplikacja, dla której utworzono zadanie. Jeżeli aplikacja jest wyłączona, wszystkie uruchomione zadania są anulowane.

Wyniki zakończonych zadań są zapisywane w dzienniku zdarzeń systemu Microsoft Windows oraz w raporcie zdarzeń Kaspersky Security Center na Serwerze administracyjnym i na każdym urządzeniu.

Nie używaj prywatnych danych w ustawieniach zadania. Na przykład, unikaj określania hasła administratora domeny.

Szczegóły dotyczące zarządzania zadaniami dla aplikacji z obsługą wielodostępności

Zadanie grupowe dla aplikacji z obsługą wielodostępności jest stosowane do aplikacji w zależności od hierarchii Serwerów administracyjnych i urządzeń klienckich. Wirtualny Serwer administracyjny, z którego tworzone jest zadanie, musi znajdować się w tej samej grupie administracyjnej lub w grupie administracyjnej niższego poziomu niż urządzenie klienckie, na którym zainstalowana jest aplikacja.

W zdarzeniach, które odpowiadają wynikom wykonania zadania, administratorowi dostawcy usługi wyświetlane są informacje o urządzeniu, na którym wykonywane jest zadanie. Natomiast administratorowi dzierżawczemu wyświetlany jest **Węzeł wielodostępowy**.

Tworzenie zadania

W Konsoli administracyjnej możesz tworzyć zadania bezpośrednio w folderze grupy administracyjnej, dla której tworzone jest zadanie grupowe, lub w obszarze roboczym folderu **Zadania**.

W celu utworzenia zadania grupowego w folderze grupy administracyjnej:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której chcesz utworzyć zadanie.
2. W obszarze roboczym grupy wybierz zakładkę **Zadania**.
3. Uruchom tworzenie zadania, klikając przycisk **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

*W celu utworzenia zadania w obszarze roboczym folderu **Zadania**:*

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania, klikając przycisk **Zakończ**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

Nie używaj prywatnych danych w ustawieniach zadania. Na przykład, unikaj określania hasła administratora domeny.

Tworzenie zadania Serwera administracyjnego

Serwer administracyjny wykonuje następujące zadania:

- Dostarczaj raporty
- Pobierz aktualizacje do repozytorium Serwera administracyjnego
- Tworzenie kopii zapasowych danych Serwera administracyjnego
- Konserwacja Serwera administracyjnego
- Wykonać synchronizację Windows Update
- Utwórz pakiet instalacyjny na podstawie obrazu systemu operacyjnego urządzenia odniesienia
- Zdalnie zainstalować aplikację
- Zdalnie odinstalować aplikację
- Roześlij pakiet instalacyjny
- Zdalnie zainstaluj aplikację na podrzędnych Serwerach administracyjnych

Na wirtualnym Serwerze administracyjnym dostępne jest tylko zadanie automatycznego dostarczania raportów oraz zadanie tworzenia pakietu instalacyjnego z obrazu systemu operacyjnego odpowiedniego urządzenia. Repozytorium wirtualnego Serwera administracyjnego wyświetla uaktualnienia pobrane na główny Serwer administracyjny. Kopia zapasowa danych wirtualnego Serwera administracyjnego jest wykonywana wraz z kopią zapasową danych głównego Serwera administracyjnego.

W celu utworzenia zadania Serwera administracyjnego:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania w jeden z następujących sposobów:
   - W drzewie konsoli, z menu kontekstowego folderu **Zadania** wybierz **Nowe** → **Zadanie**.
   - Kliknij przycisk **Utwórz zadanie** dostępny w obszarze roboczym folderu **Zadania**.

Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

Zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego, Wykonaj synchronizację Windows Update, Konserwacja Serwera administracyjnego oraz *Utwórz kopię zapasową danych Serwera administracyjnego* mogą zostać utworzone tylko raz. Jeśli zadania *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*, *Konserwacja Serwera administracyjnego*, *Kopia zapasowa danych Serwera administracyjnego* oraz *Wykonaj synchronizację Windows Update* zostały już utworzone dla Serwera administracyjnego, nie będą wyświetlane w oknie wyboru typu zadania Kreatora nowych zadań.

Tworzenie zadania dla określonych urządzeń

W Kaspersky Security Center możliwe jest utworzenie zadań dla określonych urządzeń. Urządzenia połączone w zbiór mogą należeć do różnych grup administracyjnych lub nie należeć do żadnej grupy administracyjnej. Kaspersky Security Center może wykonać następujące główne zadania dla określonych urządzeń:

- Zdalnie zainstalować aplikację
- Wysłać wiadomość do użytkownika
- Zmienić Serwer administracyjny
- Zarządzać urządzeniami
- Zweryfikować uaktualnienia
- Rozesłać pakiety instalacyjne
- Zdalnie zainstaluj aplikację na podrzędnych Serwerach administracyjnych
- Zdalnie odinstalować aplikację

W celu utworzenia zadania dla określonych urządzeń:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania w jeden z następujących sposobów:
   - Wybierając **Nowe** → **Zadanie** w menu kontekstowym folderu **Zadania** w drzewie konsoli.
   - Kliknij przycisk **Utwórz zadanie** dostępny w obszarze roboczym folderu **Zadania**.

Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

Tworzenie zadania lokalnego

W celu utworzenia zadania lokalnego dla urządzenia:

1. W obszarze roboczym grupy zawierającej urządzenie wybierz zakładkę **Urządzenia**.
2. Z listy urządzeń na zakładce **Urządzenia** wybierz urządzenie, dla którego powinno zostać utworzone zadanie lokalne.
3. Uruchom tworzenie zadania dla wybranego urządzenia w jeden z następujących sposobów:
   - Kliknij przycisk **Wykonaj akcję** i z listy rozwijalnej wybierz wartość **Utwórz zadanie**.
   - Kliknij przycisk **Utwórz zadanie** w obszarze roboczym urządzenia.
   - Zastosuj właściwości urządzenia w następujący sposób:
     a. Z otwartego menu kontekstowego urządzenia wybierz **Właściwości**.
     b. W oknie właściwości urządzenia, które zostanie otwarte, przejdź do sekcji **Zadania** i kliknij **Dodaj**.

Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

Szczegółowe instrukcje dotyczące sposobu tworzenia i konfiguracji zadań lokalnych są dostępne w podręcznikach dla odpowiednich aplikacji firmy Kaspersky.

Wyświetlanie dziedziczonego zadania grupowego w obszarze roboczym grupy zagnieżdżonej

W celu włączenia wyświetlania dziedziczonych zadań grupy zagnieżdżonej w obszarze roboczym:

1. W obszarze roboczym grupy zagnieżdżonej wybierz zakładkę **Zadania**.
2. W obszarze roboczym zakładki **Zadania** kliknij przycisk **Pokaż zadania dziedziczone**.

Zadania dziedziczone zostaną wyświetlone na liście zadań z jedną z poniższych ikon:

-  —jeśli były dziedziczone od grupy utworzonej na głównym Serwerze administracyjnym.
-  — jeśli były dziedziczone od grupy z wyższego poziomu hierarchii.

Jeżeli włączony jest tryb dziedziczenia, zadania dziedziczone będą mogły być modyfikowane tylko w grupie, w której zostały utworzone. Zadania dziedziczone nie mogą być modyfikowane w grupie, która dziedziczy zadania.

Automatyczne włączanie urządzeń przed uruchomieniem zadania

Kaspersky Security Center nie uruchamia zadań na wyłączonych urządzeniach. Możesz skonfigurować Kaspersky Security Center, aby automatycznie włączał te urządzenia przed uruchomieniem zadania, korzystając z funkcji Wake-on-LAN.

W celu skonfigurowania automatycznego uruchamiania urządzeń przed uruchomieniem zadania:

1. W oknie ustawień zadania wybierz sekcję **Terminarz**.
2. Aby skonfigurować działania na urządzeniach, kliknij łącze **Zaawansowane**.
3. W otwartym oknie **Zaawansowane** zaznacz pole **Włącz urządzenia przed uruchomieniem zadania (min) przy użyciu funkcji Wake-on-LAN** i określ przedział czasu w minutach.

W rezultacie na określoną liczbę minut przed uruchomieniem zadania Kaspersky Security Center włącza urządzenia i ładuje na nich system operacyjny za pomocą funkcji Wake-on-LAN. Po zakończeniu zadania urządzenia są automatycznie wyłączane, jeśli użytkownicy urządzeń nie zalogują się do systemu. Zauważ, że Kaspersky Security Center automatycznie wyłącza tylko te urządzenia, które są włączone przy użyciu funkcji Wake-on-LAN.

Kaspersky Security Center może automatycznie uruchamiać systemy operacyjne tylko na urządzeniach obsługujących standard Wake-on-LAN (WoL).

Automatyczne wyłączanie urządzenia po zakończeniu zadania

Kaspersky Security Center umożliwia konfigurowanie zadania w taki sposób, że urządzenia, do których się odnoszą, są automatycznie wyłączane po zakończeniu zadania.

W celu automatycznego wyłączenia urządzenia po zakończeniu zadania:

1. W oknie ustawień zadania wybierz sekcję **Terminarz**.
2. Kliknij odnośnik **Zaawansowane**, aby otworzyć okno, w którym można skonfigurować działania na urządzeniach.
3. W otwartym oknie **Zaawansowane** zaznacz pole **Wyłącz urządzenia po zakończeniu zadania**.

Ograniczanie czasu uruchamiania zadania

W celu ograniczenia czasu, w trakcie którego zadanie jest uruchamiane na urządzeniach:

1. W oknie ustawień zadania wybierz sekcję **Terminarz**.
2. Otwórz okno konfiguracji akcji wykonywanych na urządzeniach klienckich, klikając **Zaawansowane**.
3. W otwartym oknie **Zaawansowane** zaznacz pole **Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż (min)** i określ przedział czasu w minutach.

Jeżeli zadanie na urządzeniu nie zostało jeszcze zakończone po minięciu określonego przedziału czasu, Kaspersky Security Center automatycznie zatrzyma wykonywanie zadania.

Eksportowanie zadania

Zadania grupowe oraz zadania dla wskazanych urządzeń można wyeksportować do pliku. Nie można eksportować zadań Serwera administracyjnego.

W celu wyeksportowania zadania:

1. Z otwartego menu kontekstowego zadania wybierz **Wszystkie zadania** → **Eksportuj**.
2. W otwartym oknie **Zapisz jako** określ ścieżkę pliku.
3. Kliknij przycisk **Zapisz**.

Uprawnienia użytkowników lokalnych nie są eksportowane.

Importowanie zadania

Możliwe jest zaimportowanie zadań grupowych oraz zadań dla wskazanych urządzeń. Nie można importować zadań Serwera administracyjnego.

W celu zaimportowania zadania:

1. Wybierz listę, do której ma zostać zaimportowane zadanie:
   - Jeżeli chcesz zaimportować zadanie do listy zadań grupowych, w obszarze roboczym żądanej grupy administracyjnej wybierz zakładkę **Zadania**.
   - Jeżeli chcesz zaimportować zadanie do listy zadań dla wskazanych urządzeń, w drzewie konsoli wybierz folder **Zadania**.

2. W celu zaimportowania zadania wybierz jedną z następujących opcji:

   - Z menu kontekstowego listy zadań wybierz **Wszystkie zadania** → **Importuj**.
   - Kliknij odnośnik **Importuj zadanie z pliku** w sekcji zarządzania listą zadań.

3. W otwartym oknie określ ścieżkę dostępu do pliku, z którego chcesz zaimportować zadanie.
4. Kliknij przycisk **Otwórz**.

   Zadanie będzie wyświetlane na liście zadań.

Jeśli nowo importowane zadanie ma identyczną nazwę jak istniejące zadanie, nazwa importowanego zadania jest rozszerzana o indeks **(<następny numer porządkowy>)**, na przykład: **(1)**, **(2)**.

Konwertowanie zadań

Przy pomocy Kaspersky Security Center możesz konwertować zadania z poprzednich wersji aplikacji Kaspersky do zadań z aktualnych wersji tych aplikacji.

Konwersja jest dostępna dla zadań następujących aplikacji:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows

W celu konwertowania zadań:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz skonwertować zadania.
2. W menu kontekstowym Serwera administracyjnego wybierz **Wszystkie zadania** → **Kreator konwersji zasad i zadań**.

   Zostanie uruchomiony Kreator konwersji zasad i zadań. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu pracy kreatora zostaną utworzone nowe zadania, które korzystają z ustawień zadań z poprzednich wersji aplikacji.

Ręczne uruchamianie i zatrzymywanie zadania

Zadania można uruchamiać i zatrzymywać ręcznie przy użyciu jednej z następujących metod: z poziomu menu kontekstowego zadania lub w oknie właściwości urządzenia klienckiego, do którego zadanie zostało przypisane.

Uruchamianie zadań grupowych z poziomu menu kontekstowego urządzenia jest dozwolone tylko dla użytkowników należących do grupy **KLAdmins**.

W celu uruchomienia lub zatrzymania zadania z poziomu menu kontekstowego lub okna właściwości zadania:

1. Z listy zadań wybierz zadanie.
2. Uruchom lub zatrzymaj zadanie w jeden z następujących sposobów:
   - Wybierając **Uruchom** lub **Zatrzymaj** w menu kontekstowym zadania.
   - Klikając **Uruchom** lub **Zatrzymaj** w sekcji **Ogólne** okna właściwości zadania.

W celu uruchomienia lub zatrzymania zadania z poziomu menu kontekstowego lub okna właściwości urządzenia klienckiego:

1. Z listy urządzeń wybierz urządzenie.
2. Uruchom lub zatrzymaj zadanie w jeden z następujących sposobów:
   - Wybierając **Wszystkie zadania** → **Uruchom zadanie** z menu kontekstowego urządzenia. Wybierz odpowiednie zadanie z listy zadań.

     Lista urządzeń, do których zadanie jest przypisane, zostanie zastąpiona wybranym urządzeniem. Zadanie zostanie uruchomione.
   - Klikając przycisk () lub () w sekcji **Zadania** okna właściwości urządzenia.

Ręczne wstrzymywanie i wznawianie zadania

W celu ręcznego wstrzymania lub wznowienia wykonywania zadania:

1. Z listy zadań wybierz zadanie.
2. Wstrzymaj lub wznów zadanie w jeden z następujących sposobów:
   - Wybierając **Wstrzymaj** lub **Wznów** w menu kontekstowym zadania.
   - Wybierając sekcję **Ogólne** w oknie właściwości i klikając **Wstrzymaj** lub **Wznów**.

Monitorowanie wykonywania zadania

W celu monitorowania wykonywania zadania:

W oknie właściwości zadania wybierz sekcję **Ogólne**.

W środkowej części sekcji **Ogólne** wyświetlany jest bieżący stan zadania.

Przeglądanie wyników wykonywania zadań przechowywanych na Serwerze administracyjnym

Kaspersky Security Center umożliwia przeglądanie wyników wykonywania zadań grupowych, zadań dla wskazanych urządzeń oraz zadań Serwera administracyjnego.

W celu przejrzenia wyników wykonania zadania:

1. W oknie właściwości zadania wybierz sekcję **Ogólne**.
2. Kliknij odnośnik **Wyniki**, aby otworzyć okno **Wyniki zadania**.

Aby wyświetlić wyniki zadania dla podrzędnego Serwera administracyjnego:

1. W oknie właściwości zadania wybierz sekcję **Ogólne**.
2. Kliknij odnośnik **Wyniki**, aby otworzyć okno **Wyniki zadania**.
3. Kliknij **Statystyki z serwerów dodatkowych**.
4. Wybierz serwer dodatkowy, dla którego chcesz wyświetlić okno **Wyniki zadania**.

Konfigurowanie filtrowania informacji o wynikach wykonywania zadań

Kaspersky Security Center umożliwia filtrowanie informacji o wynikach wykonywania zadań grupowych, zadań dla wskazanych urządzeń oraz zadań Serwera administracyjnego. Opcja filtrowania nie jest dostępna dla zadań lokalnych.

W celu skonfigurowania filtrowania informacji o wynikach wykonywania zadania:

1. W oknie właściwości zadania wybierz sekcję **Ogólne**.
2. Kliknij odnośnik **Wyniki**, aby otworzyć okno **Wyniki zadania**.

   Tabela w górnej części okna zawiera listę wszystkich urządzeń, do których przydzielono zadanie. Tabela w dolnej części okna wyświetla wyniki zadania wykonywanego na wybranym urządzeniu.
3. Kliknij prawym klawiszem myszy odpowiednią tabelę, aby otworzyć menu kontekstowe, z którego wybierz **Filtr**.
4. W otwartym oknie **Ustaw filtr** zdefiniuj ustawienia filtra w sekcjach: **Zdarzenia**, **Urządzenia** i **Czas**. Kliknij **OK**.

Okno **Wyniki zadania** będzie wyświetlało informacje odpowiadające ustawieniom określonym w filtrze.

Modyfikowanie zadania. Wycofywanie zmian

W celu zmodyfikowania zadania:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. W obszarze roboczym folderu **Zadania** wybierz zadanie i przejdź do okna właściwości zadania, korzystając z menu kontekstowego.
3. Wprowadź niezbędne zmiany.

   W sekcji **Wykluczenia z zakresu zadania** możesz skonfigurować listę podgrup, do których zadanie nie jest stosowane.

4. Kliknij **Zastosuj**.

Zmiany wprowadzone w zadaniu zostaną zapisane w oknie właściwości zadania, w sekcji **Historia rewizji**.

Jeśli to konieczne, możesz wycofać zmiany wprowadzone w zadaniu.

W celu wycofania zmian wprowadzonych w zadaniu:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Wybierz zadanie, w którym należy wycofać zmiany, i przejdź do okna właściwości zadania, korzystając z menu kontekstowego.
3. W oknie właściwości zadania wybierz sekcję **Historia rewizji**.
4. Na liście rewizji zadania wybierz numer rewizji, do której chcesz wycofać zmiany.
5. Kliknij przycisk **Zaawansowane** i z listy rozwijalnej wybierz wartość **Wycofaj**.

Porównywanie zadań

Możesz porównać zadania tego samego typu: na przykład, możesz porównać dwa zadania skanowania w poszukiwaniu złośliwego oprogramowania, ale nie możesz porównać zadania skanowania pod kątem złośliwego oprogramowania i zadania instalacji aktualizacji. Po zakończeniu porównywania, uzyskasz raport wyszczególniający te ustawienia, które są takie same, oraz te, które są różne. Raport z porównania zadań można wydrukować lub zapisać do pliku. Porównanie zadań może być przydatne, gdy różne jednostki w firmie posiadają przypisane różne zadania tego samego typu. Na przykład, na urządzeniach pracowników z działu księgowości jest ustawione zadanie skanowania w poszukiwaniu złośliwego oprogramowania tylko dysków lokalnych, a na urządzeniach pracowników z działu sprzedaży ustawione jest zadanie skanowania antywirusowego dysków lokalnych i poczty. Nie musisz przeglądać wszystkich ustawień zadania, aby zauważyć tę różnicę. Wystarczy szybkie porównanie zadań.

Porównywać można tylko zadania tego samego typu.

Porównanie może odbywać się tylko parami.

Zadania można porównać w jeden z następujących sposobów: poprzez wybranie jednego zadania i porównanie go z innym lub poprzez porównanie dowolnych dwóch zadań z listy zadań.

W celu wybrania jednego zadania i porównanie go z innym:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. W obszarze roboczym folderu **Zadania** wybierz zadanie, które chcesz porównać z innym.
3. Z otwartego menu kontekstowego zadania wybierz **Wszystkie zadania** → **Porównaj z innym zadaniem**.
4. W oknie **Wybierz zadanie** wybierz zadanie do porównania.
5. Kliknij **OK**.

   Zostanie wyświetlony raport w formacie HTML z porównaniem dwóch zadań.

W celu porównania dwóch dowolnych zadań z listy zadań:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. W folderze **Zadania**, na liście zadań wciśnij klawisz **`Shift`** lub **`Ctrl`**, aby wybrać dwa zadania tego samego typu.
3. Z menu kontekstowego wybierz **Porównaj**.

   Zostanie wyświetlony raport w formacie HTML z porównaniem wybranych zadań.

Podczas porównywania zadań, gdy hasła różnią się, w raporcie z porównania zadań wyświetlane są gwiazdki (******).

Jeśli hasło zostało zmienione we właściwościach zadania, gwiazdki (******) są wyświetlane w raporcie z porównania rewizji (******).

Konta do uruchamiania zadań

Możesz określić konto, z poziomu którego ma być uruchamiane zadanie.

Na przykład, aby uruchomić zadanie skanowania na żądanie, musisz posiadać uprawnienia dostępu do skanowanego obiektu, natomiast żeby uruchomić zadanie aktualizacji, musisz posiadać uprawnienia autoryzowanego użytkownika serwera proxy. Możliwość określenia konta dla uruchamiania zadania pozwala uniknąć problemów z zadaniami skanowania na żądanie i zadaniami aktualizacji w sytuacji, gdy użytkownik uruchamiający zadanie nie posiada żądanych uprawnień dostępu.

Podczas wykonywania zadań zdalnej instalacji / dezinstalacji określone konto jest używane do pobierania na urządzenia klienckie plików wymaganych do zainstalowania / odinstalowania aplikacji w przypadku, gdy Agent sieciowy nie jest zainstalowany lub jest niedostępny. Jeśli Agent sieciowy jest zainstalowany i jest dostępny, konto jest używane, gdy zgodnie z ustawieniami zadań, dostarczanie plików jest wykonywane tylko przy użyciu narzędzi systemu Microsoft Windows z folderu współdzielonego. W tej sytuacji konto musi posiadać na urządzeniu następujące uprawnienia:

- Uprawnienie do zdalnego uruchamiania aplikacji.
- Uprawnienie do używania zasobu Admin$.
- Uprawnienie do *Zalogowania w trybie usługi*.

Jeśli pliki są dostarczane na urządzenia przez Agenta sieciowego, konto nie będzie używane. Wówczas wszystkie działania kopiowania i instalacji są wykonywane przez **Agenta sieciowego** (**konto LocalSystem**).

Eksportowanie historii wykonania zadania

Jeśli napotkasz jakiekolwiek problemy z zadaniem, może być konieczne zbadanie ich przyczyn. Aby to zrobić, możesz wyeksportować i szczegółowo przeanalizować historię wykonania zadania.

Aby wyeksportować historię wykonania zadania:

1. Utwórz pusty plik TXT w katalogu na swoim urządzeniu.

   Historia wykonania zadania zostanie wyeksportowana do tego pliku.

2. Otwórz okno wyników zadania.

3. W górnej części okna z wynikami zadania wybierz urządzenie, w którym występują problemy.

4. W dolnej części okna z wynikami zadania, gdzie wyświetlana jest historia wykonania dla wybranego urządzenia, wybierz jedno lub kilka zdarzeń.

   Aby zaznaczyć kilka zdarzeń, użyj klawisza **`Shift`** lub **`Ctrl`**.

5. Kliknij prawym przyciskiem myszy wybrane zdarzenie(-a), aby otworzyć menu kontekstowe i wybierz opcję **Eksportuj**.

   Zostanie uruchomiony Kreator eksportu zdarzeń.

6. Na etapie **Eksportuj plik** kreatora kliknij przycisk **Przeglądaj**, a następnie wybierz plik TXT utworzony w celu wyeksportowania historii wykonywania zadań.

Jeśli chcesz wyeksportować tylko wybrane zdarzenie(-a), zaznacz opcję **Eksportuj tylko wybrane zdarzenia**.

Jeśli chcesz wyeksportować całą historię wykonania zadania (wszystkie zdarzenia), opcja **Eksportuj tylko wybrane zdarzenia** musi być wyłączona.

7. Kliknij przycisk **Dalej**.

8. Na etapie **Format eksportu** kreatora włącz jedną z następujących opcji:

   - **Eksportuj jako tekst Unicode rozdzielany znakami tabulacji**

     Włącz tę opcję, jeśli eksportowane dane zawierają znaki specjalne i symbole z różnych języków i chcesz mieć pewność, że wszystkie znaki zostaną dokładnie zachowane, gdy plik TXT z eksportowanymi danymi będzie otwierany w różnych aplikacjach.

   - **Eksportuj jako tekst rozdzielany znakami tabulacji**

     Włącz tę opcję, jeśli chcesz zachować zgodność ze starszymi systemami lub aplikacjami, które mogą nie obsługiwać Unicode.

9. Kliknij przycisk **Dalej**, aby zakończyć działanie kreatora.

Historia wykonania zadania jest eksportowana do wybranego pliku TXT.

Kreator zmiany haseł w zadaniach

Dla zadania, które nie jest lokalne, możesz określić konto, z poziomu którego zadanie musi być uruchomione. Konto może zostać określone podczas tworzenia zadania lub we właściwościach istniejącego zadania. Jeśli określone konto jest używane zgodnie z instrukcjami bezpieczeństwa organizacji, te instrukcje mogą wymagać zmiany hasła do konta od czasu do czasu. Jeśli hasło do konta wygaśnie i ustawisz nowe, nie powiedzie się uruchomienie zadań, aż do momentu, gdy określisz nowe ważne hasło we właściwościach zadania.

Kreator zmiany haseł w zadaniach umożliwia automatyczne zastąpienie starego hasła nowym we wszystkich zadaniach, w których konto jest określone. Alternatywnie, możesz zrobić to ręcznie we właściwościach każdego zadania.

W celu uruchomienia kreatora zmiany haseł w zadaniach:

1. Z drzewa konsoli wybierz węzeł **Zadania**.

2. Z menu kontekstowego węzła wybierz **Kreator zmiany haseł w zadaniach**.

Postępuj zgodnie z instrukcjami kreatora.

Krok 1. Określanie danych uwierzytelniających

W polach **Konto** i **Hasło** określ nowe dane uwierzytelniające, które aktualnie są ważne w Twoim systemie (na przykład, w Active Directory). Jeśli przejdziesz do następnego kroku kreatora, Kaspersky Security Center sprawdzi, czy nazwa określonego konta odpowiada nazwie konta we właściwościach każdego zadania, które nie jest lokalne. Jeśli nazwy kont pasują do siebie, hasło we właściwościach zadania zostanie automatycznie zastąpione nowym.

Jeśli uzupełnisz pole **Stare hasło (opcjonalnie)**, Kaspersky Security Center zastępuje hasło tylko dla tych zadań, w których zostanie wykryta nazwa konta oraz stare hasło. Zastępowanie odbywa się automatycznie. We wszystkich pozostałych przypadkach musisz wybrać działanie, jakie ma zostać podjęte w kolejnym kroku kreatora.

Krok 2. Wybieranie działania, jakie ma zostać podjęte

Jeśli nie określiłeś starego hasła w pierwszym kroku kreatora lub stare hasło nie odpowiada hasłom w zadaniach, powinieneś wybrać działanie, jakie ma zostać wykonane na wykrytych zadaniach.

Dla każdego zadania, które posiada stan *Wymaga zatwierdzenia*, zdecyduj, czy chcesz usunąć hasło we właściwościach zadania lub zastąpić je nowym. Jeśli zdecydujesz się usunąć hasło, zadanie zostanie przełączone do uruchamiania z poziomu domyślnego konta.

Krok 3. Sprawdzanie wyników

W ostatnim kroku kreatora przejrzyj wyniki dla każdego wykrytego zadania. Aby zakończyć działanie kreatora, kliknij przycisk **Zakończ**.

Tworzenie hierarchii grup administracyjnych podległych wirtualnemu Serwerowi administracyjnemu

Po utworzeniu wirtualnego Serwera administracyjnego zawiera on domyślnie grupę administracyjną o nazwie **Zarządzane urządzenia**.

Procedura tworzenia hierarchii grup administracyjnych podległych wirtualnemu Serwerowi administracyjnemu jest identyczna jak procedura tworzenia hierarchii grup administracyjnych podległych fizycznemu Serwerowi administracyjnemu.

Nie możesz dodawać podrzędnych i wirtualnych Serwerów administracyjnych do grup administracyjnych podległych wirtualnemu Serwerowi administracyjnemu. Dzieje się tak ze względu na ograniczenia wirtualnych Serwerów administracyjnych.

Zasady i profile zasad

W Kaspersky Security Center Web Console możesz tworzyć zasady dla aplikacji Kaspersky. Ta sekcja opisuje zasady i profile zasad, a także zawiera instrukcje dotyczące ich tworzenia i modyfikowania.

Hierarchia zasad i korzystanie z zasad

W tej sekcji można znaleźć informacje dotyczące stosowania zasad do urządzeń w grupach administracyjnych. Ta sekcja zawiera również informacje o profilach zasad.

Hierarchia zasad

W Kaspersky Security Center zasad są używane do określenia jednego zestawu ustawień dla kilku urządzeń. Na przykład, obszar zasady aplikacji P zdefiniowanej dla grupy administracyjnej G zawiera zarządzane urządzenia z zainstalowaną aplikacją P, które zostały dodane do grupy G i wszystkich jej podgrup, za wyjątkiem podgrup, we właściwościach których odznaczono opcję **Dziedzicz z grupy nadrzędnej**.

Zasadę można odróżnić od lokalnego ustawienia po ikonach kłódki (🔒) obok jej ustawień. Jeśli ustawienie (lub grupa ustawień) jest zablokowane we właściwościach zasady, w pierwszej kolejności należy użyć tego ustawienia (lub grupy ustawień) podczas tworzenia obowiązującego ustawienia, a następnie należy zapisać ustawienie (lub grupę ustawień) do zasady podrzędnej.

Tworzenie obowiązujących ustawień można opisać w następujący sposób: wartości wszystkich ustawień, które nie zostały zablokowane, są kopiowane z zasady, a następnie są nadpisywane przez wartości ustawień lokalnych, a w kolejnym etapie wartości wynikowe są nadpisywane przez zablokowane ustawienia pobrane z zasady.

Zasady tej samej aplikacji oddziałują na siebie poprzez hierarchię grup administracyjnych: Zablokowane ustawienia z zasady nadrzędnej nadpisują te same ustawienia z zasady podrzędnej.

Dla użytkowników mobilnych istnieje specjalna zasada. Ta zasada jest aktywowana na urządzeniu, gdy to przełącza się do trybu użytkownika mobilnego. Zasady użytkowników mobilnych nie oddziałują na inne zasady poprzez hierarchię grup administracyjnych.

Profile zasad

Stosowanie zasad na urządzeniach tylko poprzez hierarchię grup administracyjnych może być niewygodne tylko w kilku przypadkach. Konieczne może być utworzenie kilku instancji jednej zasady, które różnią się jednym lub dwoma ustawieniami dla różnych grup administracyjnych, oraz zsynchronizowanie zawartości tych zasad w przyszłości.

Aby pomóc Ci uniknąć takich problemów, Kaspersky Security Center obsługuje *profile zasad*. Profil zasad jest to inaczej podzbiór ustawień zasady. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z zasadą i uzupełnia go zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowej" zasady, która jest aktywna na urządzeniu klienckim (komputerze lub urządzeniu mobilnym). Aktywacja profilu zmodyfikuje ustawienia zasad, które były aktywne na urządzeniu przed aktywacją profilu. Te ustawienia przyjmują wartości określone w profilu.

Aktualnie na profile zasad nałożone są następujące ograniczenia:

- Zasada może zawierać maksymalnie 100 profili.
- Profil zasad nie może zawierać innych profili.
- Profil zasad nie może zawierać ustawień powiadamiania.

Zawartość profilu

Profil zasad zawiera następujące elementy:

- Nazwa. Profile z takimi samymi nazwami wpływają na siebie poprzez hierarchię grup administracyjnych ze wspólnymi regułami.
- Podzbiór ustawień zasady. Profil zawiera tylko aktualnie wymagane ustawienia (ustawienia zablokowane).

- Warunek aktywacji to wyrażenie logiczne z właściwościami urządzenia. Profil jest aktywny (uzupełnia zasadę) tylko wtedy, gdy warunek aktywacji profilu jest prawdziwy. We wszystkich pozostałych przypadkach profil jest nieaktywny i jest ignorowany. W wyrażeniu logicznym mogą być uwzględnione następujące właściwości urządzenia:
  - Stan trybu użytkownika mobilnego.
  - Właściwości środowiska sieciowego — nazwa aktywnej reguły dla połączenia z Agentem sieciowym.
  - Obecność lub brak określonych znaczników na urządzeniu.
  - Lokalizacja urządzenia w jednostce Active Directory: jawna (urządzenie znajduje się w określonej jednostce OU) lub niejawna (urządzenie jest w jednostce OU, która znajduje się w określonej jednostce OU na dowolnym poziomie zagnieżdżenia).
  - Członkostwo urządzenia w grupie zabezpieczeń Active Directory (jawne lub niejawne).
  - Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory (jawne lub niejawne).
- Pole wyłączające profil. Wyłączone profile są zawsze ignorowane, a ich odpowiednie warunki aktywacji nie są sprawdzane.
- Priorytet profilu. Warunki aktywacji różnych profili są niezależne, a więc można aktywować kilka profili jednocześnie. Jeśli aktywne profile zawierają nienakładające się na siebie zbiory ustawień, nie pojawi się żaden problem. Jednakże dwa aktywne profile zawierające różne wartości tego samego ustawienia spowodują niejednoznaczność. Tę niejednoznaczność można wyeliminować poprzez priorytety profilu: Wartość niejednoznacznej zmiennej zostanie pobrana z profilu, który ma wyższy priorytet (ten, który znajduje się wyżej na liście profili).

Zachowanie profili, gdy zasady oddziałują na siebie poprzez hierarchię

Profile o tych samych nazwach zostają scalone zgodnie z regułami scalania zasad. Profile zasady nadrzędnej mają wyższy priorytet niż zasady podrzędnej. Jeśli modyfikowanie ustawień jest zabronione w zasadzie nadrzędnej (są zablokowane), zasada podrzędna używa warunków aktywacji profilu z zasady nadrzędnej. Jeśli modyfikowanie ustawień jest dozwolone w zasadzie nadrzędnej, używane są warunki aktywacji profilu z zasady podrzędnej.

Ponieważ w swoim warunku aktywacji profil zasad może zawierać opcję **Urządzenie jest w trybie offline**, profile całkowicie zastępują funkcję zasad dla użytkowników mobilnych, które nie będą już obsługiwane.

Zasada dla użytkowników mobilnych może zawierać profile, ale te profile mogą zostać aktywowane dopiero po przełączeniu urządzenia w tryb użytkownika mobilnego.

Dziedziczenie ustawień zasady

Zasada jest określona dla grupy administracyjnej. Ustawienia zasady mogą być *dziedziczone*, czyli otrzymywane w podgrupach (grupach podrzędnych) grupy administracyjnej, dla której zostały określone. Dalej zasada dla grupy nadrzędnej jest też zwana *zasadą nadrzędną*.

Możesz włączyć lub wyłączyć dwie opcje dziedziczenia: **Dziedzicz ustawienia z zasady nadrzędnej** i **Wymuś dziedziczenie ustawień w zasadach podrzędnych**:

- Jeśli włączysz **Dziedzicz ustawienia z zasady nadrzędnej** dla profilu potomnego i zablokuj niektóre ustawienia w profilu nadrzędnym, wówczas nie będziesz mógł zmienić tych ustawień dla grupy potomnej. Jednakże możesz zmienić ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

- Jeśli wyłączysz **Dziedzicz ustawienia z zasady nadrzędnej** dla profilu potomnego, wówczas możesz zmienić wszystkie ustawienia w grupie potomnej nawet wtedy, gdy niektóre ustawienia są zablokowane w profilu nadrzędnym.

- Jeśli włączysz **Wymuś dziedziczenie ustawień w zasadach podrzędnych** w grupie nadrzędnej, spowoduje to włączenie **Dziedzicz ustawienia z zasady nadrzędnej** dla każdego profilu potomnego. W tym przypadku nie możesz wyłączyć tej opcji dla żadnej zasady podrzędnej. Wszystkie ustawienia, które są zablokowane w zasadzie nadrzędnej, są dziedziczone w grupach podrzędnych w sposób wymuszony i nie możesz zmienić tych ustawień w grupach podrzędnych.

- W profilach dla grupy **Zarządzane urządzenia** opcja **Dziedzicz ustawienia z zasady nadrzędnej** nie wpływa na żadne ustawienia, ponieważ grupa **Zarządzane urządzenia** nie zawiera żadnych grup wyższego poziomu i dlatego nie dziedziczy żadnych profili.

Domyślnie, opcja **Wymuś dziedziczenie ustawień w zasadach podrzędnych** jest włączona dla nowego profilu.

Jeśli zasada zawiera profile, wszystkie zasady podrzędne dziedziczą te profile.

Zarządzanie zasadami

Ustawienia aplikacji zainstalowanych na urządzeniach klienckich są konfigurowane centralnie poprzez definiowanie zasad.

Zasady utworzone dla aplikacji w grupie administracyjnej są wyświetlane w obszarze roboczym, na zakładce **Zasady**. Przed nazwą każdej zasady wyświetlana jest ikona z jej stanem.

Po usunięciu lub anulowaniu zasady aplikacja będzie kontynuowała działanie z ustawieniami określonymi w zasadzie. Te ustawienia mogą być później modyfikowane ręcznie.

Stosowanie zasady odbywa się w następujący sposób: jeśli na urządzeniu uruchomione są zadania rezydentne (zadania ochrony w czasie rzeczywistym), ich wykonywanie będzie kontynuowane z użyciem nowych wartości. Każde uruchamiane zadanie okresowe (skanowanie na żądanie, aktualizacja baz danych aplikacji) działa z niezmienionymi wartościami ustawień. Następnym razem zostają uruchomione z nowymi wartościami ustawień.

Zasady dla aplikacji z obsługą wielodostępności są dziedziczone przez grupy administracyjne niższego poziomu, a także przez grupy administracyjne wyższego poziomu: zasada jest przekazywana do wszystkich urządzeń klienckich, na których zainstalowana jest aplikacja.

W przypadku, gdy Serwery administracyjne są ułożone hierarchicznie, podrzędne Serwery administracyjne otrzymają zasady od głównego Serwera administracyjnego, a następnie rozprowadzą je do urządzeń klienckich. Jeżeli włączone jest dziedziczenie, ustawienia zasady mogą być modyfikowane na głównym Serwerze administracyjnym. Następnie wszelkie zmiany dokonane w ustawieniach zasady są wprowadzane w zasadach dziedziczonych na podrzędnych Serwerach administracyjnych.

Jeżeli połączenie między głównym Serwerem administracyjnym a podrzędnym Serwerem administracyjnym zostanie zerwane, zasada na Serwerze podrzędnym nadal będzie używała zastosowanych ustawień. Ustawienia zasady modyfikowane na głównym Serwerze administracyjnym są rozsyłane do podrzędnego Serwera administracyjnego po ponownym nawiązaniu z nim połączenia.

Jeśli dziedziczenie jest wyłączone, ustawienia zasady mogą być modyfikowane na podrzędnym Serwerze administracyjnym niezależnie od głównego Serwera administracyjnego.

W przypadku, gdy połączenie między Serwerem administracyjnym a urządzeniem klienckim zostanie zerwane, urządzenie klienckie rozpocznie pracę z zasadą użytkownika mobilnego (jeśli został określony) lub zasada będzie dalej używać zastosowanych ustawień, aż do ponownego nawiązania połączenia.

Wyniki przesłania zasady do podrzędnego Serwera administracyjnego są wyświetlane w oknie właściwości zasady konsoli na głównym Serwerze administracyjnym.

Wyniki przesłania zasad do urządzeń klienckich są wyświetlane w oknie właściwości zasady Serwera administracyjnego, z którym są połączone.

Nie używaj prywatnych danych w ustawieniach zasad. Na przykład, unikaj określania hasła administratora domeny.

Tworzenie zasady

W Konsoli administracyjnej możesz tworzyć zasady bezpośrednio w folderze grupy administracyjnej, dla której tworzona jest zasada, lub w obszarze roboczym folderu **Zasady**.

W celu utworzenia zasady w folderze grupy administracyjnej:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której ma zostać utworzona zasada.
2. W obszarze roboczym grupy wybierz zakładkę **Zasady**.
3. Uruchom Kreator tworzenia nowej zasady, klikając przycisk **Nowa zasada**.

   Zostanie uruchomiony Kreator tworzenia nowej zasady. Postępuj zgodnie z instrukcjami kreatora.

*W celu utworzenia zasady w obszarze roboczym folderu **Zasady**:*

1. Z drzewa konsoli wybierz folder **Zasady**.
2. Uruchom Kreator tworzenia nowej zasady, klikając przycisk **Nowa zasada**.

   Zostanie uruchomiony Kreator tworzenia nowej zasady. Postępuj zgodnie z instrukcjami kreatora.

Dla jednej aplikacji z grupy możliwe jest utworzenie kilku zasad, ale tylko jedna z nich może być aktywna. Po utworzeniu nowej aktywnej zasady poprzednia staje się nieaktywna.

Podczas tworzenia zasady można skonfigurować minimalny zestaw ustawień wymaganych do prawidłowego działania aplikacji. Wszystkie pozostałe ustawienia posiadają domyślne wartości stosowane podczas lokalnej instalacji aplikacji. Po utworzeniu zasady możesz go zmienić.

Nie używaj prywatnych danych w ustawieniach zasad. Na przykład, unikaj określania hasła administratora domeny.

Ustawienia aplikacji firmy Kaspersky, które zostają zmienione po zastosowaniu zasad, zostały szczegółowo opisane w odpowiednich dokumentach.

Po utworzeniu zasady ustawienia, których modyfikowanie zostało zablokowane (ustawiona jest ikona kłódki ( )), będą obowiązywać na urządzeniach klienckich niezależnie od tego, które ustawienia były wcześniej określone dla aplikacji.

Wyświetlanie zasady dziedziczonej w podgrupie

W celu włączenia wyświetlania zasad dziedziczonych dla zagnieżdżonej grupy administracyjnej:

1. W drzewie konsoli wybierz grupę administracyjną, dla której powinny być wyświetlane zasady dziedziczone.
2. W obszarze roboczym wybranej grupy wybierz zakładkę **Zasady**.
3. Z menu kontekstowego listy profili wybierz **Widok** → **Zasady dziedziczone**.

Zasady dziedziczone zostaną wyświetlone na liście zasad z następującą ikoną:

- —jeśli były dziedziczone od grupy utworzonej na głównym Serwerze administracyjnym.
- —jeśli były dziedziczone od grupy z wyższego poziomu hierarchii.

Jeżeli włączony jest tryb dziedziczenia ustawień, zasady dziedziczone będą mogły być modyfikowane tylko w grupie, w której zostały utworzone. Modyfikowanie zasad dziedziczonych nie jest możliwe w grupie, która je dziedziczy.

Aktywowanie zasady

W celu aktywowania zasady dla wybranej grupy:

1. W obszarze roboczym grupy, na zakładce **Zasady** wybierz zasadę, którą chcesz aktywować.
2. W celu aktywowania zasady wykonaj jedno z następujących działań:
   - Z otwartego menu kontekstowego zasady wybierz **Zasada aktywna**.
   - W oknie właściwości zasady otwórz sekcję **Ogólne** i wybierz **Zasada aktywna** z grupy ustawień **Stan zasady**.

Zasada stanie się aktywna dla wybranej grupy administracyjnej.

Podczas stosowania zasady do dużej liczby urządzeń klienckich, zarówno obciążenie Serwera administracyjnego, jak i ruch sieciowy zostają znacząco zwiększone na pewien czas.

Aktywowanie zasady automatycznie po wystąpieniu zdarzenia Ataku wirusa

W celu skonfigurowania zasady tak, aby była aktywowana automatycznie po wystąpieniu Ataku wirusa:

1. W oknie właściwości Serwera administracyjnego otwórz sekcję **Epidemia wirusa**.
2. Otwórz okno **Aktywacja zasady**, klikając odnośnik **Skonfiguruj zasady, które zostaną aktywowane po wystąpieniu epidemii wirusa** i dodając zasadę do wybranej listy zasad aktywowanych po wystąpieniu epidemii wirusa.

Jeśli zasada została aktywowana po wystąpieniu zdarzenia *Epidemia wirusa*, możesz wrócić do poprzedniej zasady tylko przy użyciu trybu ręcznego.

Stosowanie zasady użytkownika mobilnego

Zasada użytkownika mobilnego jest aktywowany na urządzeniu w przypadku, gdy zostaje ono odłączone od sieci firmowej.

W celu zastosowania zasady użytkownika mobilnego:

W oknie właściwości zasady otwórz sekcję **Ogólne** i w grupie ustawień **Stan zasady** wybierz **Zasada użytkownika mobilnego**.

Zasada użytkownika mobilnego zostanie zastosowana na urządzeniach, jeśli są odłączone od sieci firmowej.

Modyfikowanie zasady. Wycofywanie zmian

W celu zmodyfikowania zasady:

1. Z drzewa konsoli wybierz folder **Zasady**.
2. W obszarze roboczym folderu **Zasady** wybierz zasadę i przejdź do okna właściwości zasady, korzystając z menu kontekstowego.
3. Wprowadź niezbędne zmiany.
4. Kliknij **Zastosuj**.

Zmiany wprowadzone w zasadzie zostaną zapisane we właściwościach zasady, w sekcji **Historia rewizji**.

Jeśli to konieczne, możesz wycofać zmiany wprowadzone w zasadzie.

W celu wycofania zmian wprowadoznych w zasadzie:

1. Z drzewa konsoli wybierz folder **Zasady**.
2. Wybierz zasadę, w której należy wycofać zmiany, i przejdź do okna właściwości zasady, korzystając z menu kontekstowego.

3. W oknie ustawień zasady wybierz sekcję **Historia rewizji**.

4. Na liście rewizji zasady wybierz numer rewizji, do której chcesz wycofać zmiany.

5. Kliknij przycisk **Zaawansowane** i z listy rozwijalnej wybierz wartość **Wycofaj**.

Porównywanie zasad

Dla jednej zarządzanej aplikacji możesz porównać dwie zasady. Po zakończeniu porównywania, uzyskasz raport wyszczególniający te ustawienia zasady, które są takie same, oraz te, które są różne. Może być, na przykład, konieczność porównania zasad, jeśli różni administratorzy w swoich biurach utworzyli kilka zasad dla jednej zarządzanej aplikacji lub jeśli zasada najwyższego poziomu został odziedziczony przez wszystkie lokalne biura i został zmodyfikowany dla każdego biura. Zasadę można porównać w jeden z następujących sposobów: poprzez wybranie jednej zasady i porównanie jej z inną lub poprzez porównanie dowolnych dwóch zasad z listy zasad.

Możesz porównywać wyłącznie zasady, które posiadają bieżące rewizje w historii rewizji.

W celu porównania jednej zasady z inną:

1. Z drzewa konsoli wybierz folder **Zasady**.

2. W obszarze roboczym folderu **Zasady** wybierz zasadę, którą chcesz porównać z inną.

3. W menu kontekstowym zasady wybierz **Porównaj zasadę z inną zasadą**.

4. W oknie **Wybierz zasadę** wybierz zasadę, z którą ma być porównana Twoja zasada.

5. Kliknij **OK**.

   Zostanie wyświetlony raport w formacie HTML z porównaniem dwóch zasad dla tej samej aplikacji.

W celu porównania dwóch dowolnych zasad z listy zasad:

1. W folderze **Zasady**, na liście zasad użyj klawisza **`Shift`** lub **`Ctrl`**, aby wybrać dwie zasady dla jednej zarządzanej aplikacji.

2. Z menu kontekstowego wybierz **Porównaj**.

   Zostanie wyświetlony raport w formacie HTML z porównaniem dwóch zasad dla tej samej aplikacji.

   Raport dotyczący porównania ustawień profilu dla Kaspersky Endpoint Security for Windows zawiera także szczegóły odnośnie porównania profili zasad. Możesz zminimalizować wyniki porównania profilu zasad. Aby zminimalizować sekcję, kliknij ikonę (▲) obok nazwy sekcji.

Przeglądanie wykresu stanu dystrybucji zasad

W Kaspersky Security Center możesz przejrzeć stan zastosowania zasady na każdym urządzeniu.

W celu wyświetlenia stanu dystrybucji zasady na każdym urządzeniu:

1. W obszarze roboczym grupy, na karcie **Zasady** wybierz zasadę, dla której chcesz wyświetlić stan dystrybucji.

   Wykres w prawym panelu przedstawia przegląd zastosowania zasad.

2. Kliknij **Szczegóły**.

   Otworzy się okno **Wyniki wymuszenia zasady**.

   Możesz wyeksportować wyniki zastosowania zasad do pliku CSV lub pliku TXT.

Usuwanie zasady

W celu usunięcia zasady:

1. W obszarze roboczym grupy administracyjnej, na zakładce **Zasady** wybierz zasadę, którą chcesz usunąć.
2. Usuń zasadę w jeden z następujących sposobów:
   - Wybierając **Usuń** z menu kontekstowego zasady.
   - Klikając odnośnik **Usuń zasadę** w oknie z informacjami dla wybranej zasady.

Kopiowanie zasady

W celu skopiowania zasady:

1. W obszarze roboczym żądanej grupy, na zakładce **Zasady** wybierz zasadę.
2. Z otwartego menu kontekstowego zasady wybierz **Kopiuj**.
3. W drzewie konsoli wybierz grupę, do której chcesz dodać zasadę.

   Możesz dodać zasadę do grupy, z której została skopiowana.
4. Z menu kontekstowego listy zasad dla wybranej grupy, na zakładce **Zasady** wybierz **Wklej**.

Zasada zostanie skopiowana ze wszystkimi swoimi ustawieniami i zastosowany na urządzeniach w obrębie grupy, do której została skopiowana. Jeżeli wkleisz zasadę do tej samej grupy, z której została skopiowana, do jej nazwy zostanie automatycznie dodany przyrostek **(<kolejny numer>)**, na przykład: **(1)**, **(2)**.

Podczas kopiowania aktywna zasada staje się nieaktywna. W razie konieczności będzie można aktywować ten profil.

Eksportowanie zasady

W celu wyeksportowania zasady:

1. Wyeksportuj zasadę w jeden z następujących sposobów:
   - Wybierając **Wszystkie zadania** → **Eksportuj** z menu kontekstowego zasady.
   - Klikając odnośnik **Eksportuj zasadę do pliku** w oknie z informacjami dla wybranej zasady.
2. W otwartym oknie **Zapisz jako** określ nazwę i ścieżkę dostępu pliku zasady. Kliknij przycisk **Zapisz**.

Importowanie zasady

W celu zaimportowania zasady:

1. W obszarze roboczym żądanej grupy, na zakładce **Zasady** wybierz jeden z następujących sposobów importowania zasad:
   - Wybierz **Wszystkie zadania** → **Importuj** z menu kontekstowego listy zasad.
   - Kliknij przycisk **Importuj zasadę z pliku** w sekcji zarządzania listą zasad.
2. W oknie, które zostanie otwarte, określ ścieżkę dostępu do pliku, z którego chcesz zaimportować zasadę. Kliknij przycisk **Otwórz**.

Zaimportowana zasada zostanie wyświetlona na liście zasad. Importowane są również ustawienia i profile zasad. Niezależnie od statusu zasady, który został wybrany podczas eksportu, importowana zasada jest nieaktywna. Możesz zmienić stan zasady we właściwościach zasady.

Jeżeli nowo importowana zasada ma nazwę identyczną z nazwą istniejącej zasady, nazwa importowanej zasady jest rozszerzana o indeks **(<następny numer kolejny>)**, na przykład: **(1)**, **(2)**.

Konwertowanie zasad

Kaspersky Security Center może konwertować zasady z wcześniejszych wersji zarządzanych aplikacji firmy Kaspersky na aktualne wersje tych samych aplikacji. Przekonwertowane zasady zachowują ustawienia aktualnego administratora sprzed aktualizacji, jak również zawierają nowe ustawienia z aktualnych wersji aplikacji. Jeśli zasada zostanie przekonwertowana na aktualną wersję zarządzanej aplikacji Kaspersky, nie będzie można otworzyć zasady na Serwerze administracyjnym, na którym jest zainstalowana starsza wersja wtyczki aplikacji. Wtyczki zarządzające dla aplikacji firmy Kaspersky określają, czy konwersja jest dostępna dla zasad tych aplikacji. Aby uzyskać informacje na temat konwertowania zasad dla każdej obsługiwanej aplikacji firmy Kaspersky, zapoznaj się z odpowiednią Pomocą z poniższej listy:

- **Aplikacje Kaspersky dla stacji roboczych:**
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux

- Kaspersky Endpoint Security for Linux Elbrus Edition
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security for Windows

- **Kaspersky Industrial CyberSecurity:**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks (scentralizowana zdalna instalacja nie jest obsługiwana)

- **Aplikacje firmy Kaspersky na urządzenia mobilne:**
  - Kaspersky Endpoint Security for Android
  - Kaspersky Security for iOS

- **Aplikacje Kaspersky dla serwerów plików:**
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux

- **Aplikacje Kaspersky dla maszyn wirtualnych:**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless

- **Aplikacje Kaspersky do wykrywania ataków ukierunkowanych:**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response

- **Aplikacje firmy Kaspersky na urządzenia KasperskyOS:**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite (wtyczka do Kaspersky Thin Client)

W celu konwertowania zasad:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz skonwertować zasady.
2. W menu kontekstowym Serwera administracyjnego wybierz **Wszystkie zadania → Kreator konwersji zasad i zadań**.

Zostanie uruchomiony Kreator konwersji zasad i zadań. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu pracy kreatora tworzone są nowe zasady, które wykorzystują ustawienia zasad bieżącego administratora oraz nowe ustawienia z aktualnych wersji aplikacji firmy Kaspersky.

Zarządzanie profilami zasad

Profil zasad to zestaw ustawień zasady, która jest aktywowana na urządzeniu klienckim (komputerze lub urządzeniu mobilnym), gdy urządzenie spełnia określone reguły aktywacji. Aktywacja profilu zmodyfikuje ustawienia zasad, które były aktywne na urządzeniu przed aktywacją profilu. Te ustawienia przyjmują wartości określone w profilu.

Profile zasad są niezbędne dla urządzeń w jednej grupie administracyjnej w celu uruchomienia z ustawieniami innych zasad. Taka sytuacja może mieć miejsce, na przykład, gdy ustawienia zasad muszą zostać zmodyfikowane dla niektórych urządzeń w grupie administracyjnej. W tym przypadku możesz skonfigurować profile zasad dla takiej zasady, co umożliwi zmodyfikowanie ustawień zasady dla wybranych urządzeń w grupie administracyjnej. Na przykład, zasada zabrania uruchamiania programu do nawigacji GPS na wszystkich urządzeniach w grupie Zarządzanie użytkownikami. Program do nawigacji GPS jest wymagany tylko na jednym urządzeniu w grupie Zarządzanie użytkownikami — na urządzeniu, które należy do użytkownika zatrudnionego w charakterze kuriera. Możesz oznaczyć to urządzenie jako „Kurier" i ponownie skonfigurować profil zasad, aby uruchamianie programu do nawigacji GPS możliwe było tylko na urządzeniu oznaczonym jako „Kurier", zachowując przy tym wszystkie pozostałe ustawienia zasady. W tym przypadku, jeśli urządzenie oznaczone jako „Kurier" pojawi się w grupie Zarządzanie użytkownikami, będzie można uruchamiać na nim program do nawigacji GPS. Uruchamianie programu do nawigacji GPS wciąż będzie zabronione na innych urządzeniach w grupie Zarządzanie użytkownikami do momentu oznakowania ich jako „Kurier".

Profile są obsługiwane tylko przez następujące zasady:

- Zasady Kaspersky Endpoint Security for Windows
- Zasady Kaspersky Endpoint Security for Mac
- Zasady wtyczki Kaspersky Mobile Device Management od wersji 10 Service Pack 1 do wersji 10 Service Pack 3 Maintenance Release 1
- Zasady wtyczki Kaspersky Device Management for iOS
- Zasady Kaspersky Security for Virtualization 5.1 Light Agent for Windows
- Zasady Kaspersky Security for Virtualization 5.1 Light Agent for Linux

Profile zasad upraszczają zarządzanie urządzeniami klienckimi, do których stosowane są zasady:

- Ustawienia profilu zasad mogą różnić się od ustawień zasady.
- Nie jest konieczne posiadanie i ręczne stosowanie kilku instancji jednej zasady, która różni się tylko kilkoma ustawieniami.

- Nie jest konieczne przydzielanie oddzielnej zasady do użytkowników mobilnych.
- Możesz wyeksportować lub zaimportować profile zasad, a także utworzyć nowe profile zasad w oparciu o istniejące profile.
- Jedna zasada może posiadać kilka aktywnych profili zasad. Tylko profile spełniające wymagania reguł aktywacji na urządzeniu zostaną zastosowane do tego urządzenia.
- Profile podlegają hierarchii zasad. Odziedziczona zasada zawiera wszystkie profile zasady wyższego poziomu.

Priorytety profili

Profile, które zostały utworzone dla zasad, są sortowane w kolejności malejącej priorytetu. Na przykład, jeśli profil X jest wyżej na liście profili niż profil Y, profil X posiada wyższy priorytet niż Y. Do jednego urządzenia można podłączyć kilka profili jednocześnie. Jeśli wartości ustawień różnią się w innych profilach, na urządzeniu zostanie zastosowana wartość z profilu najwyższego poziomu.

Reguły aktywacji profili

Profil zasad jest aktywowany na urządzeniu klienckim po wyzwoleniu reguły aktywacji. *Reguły aktywacji* to zestaw warunków, które, gdy zostaną spełnione, uruchamiają profil zasad na urządzeniu. Reguła aktywacji może zawierać następujące warunki:

- Agent sieciowy na urządzeniu klienckim łączy się z Serwerem administracyjnym przy użyciu określonego zestawu ustawień połączenia, takich jak adres Serwera administracyjnego, numer portu itd.
- Urządzenie klienckie jest offline.
- Do urządzenia klienckiego przypisano określone znaczniki.
- Urządzenia klienckie są jawnie (urządzenie jest natychmiast umieszczane w określonej jednostce) lub niejawnie (urządzenie jest umieszczane w jednostce, która znajduje się w określonej jednostce na dowolnym poziomie zagnieżdżenia) umieszczane w określonej jednostce Active Directory®, urządzenie lub jego właściciel znajduje się w grupie zabezpieczeń Active Directory.
- To urządzenie klienckie należy do określonego użytkownika lub właściciel urządzenia należy do wewnętrznej grupy bezpieczeństwa Kaspersky Security Center.
- Właścicielowi urządzenia klienckiego została przypisana określona rola.

Zasady w hierarchii grup administracyjnych

Jeśli tworzysz zasadę w grupie administracyjnej niskiego poziomu, ta nowa zasada odziedziczy wszystkie profile aktywnej zasady z grupy wyższego poziomu. Profile z identycznymi nazwami zostają scalone. Profile zasad dla grupy wyższego poziomu posiadają wyższy priorytet. Na przykład, w grupie administracyjnej *A*, zasada *P(A)* posiada profile *X1*, *X2* i *X3* (w kolejności malejącej priorytetu). W grupie administracyjnej *B*, która jest podgrupą grupy *A*, zasada *P(B)* została utworzona z profilami *X2*, *X4*, *X5*. Następnie zasada *P(B)* zostanie zmodyfikowana przez zasadę *P(A)*, co spowoduje, że lista profili zasady *P(B)* będzie wyglądać następująco: *X1*, *X2*, *X3*, *X4*, *X5* (w kolejności malejącej priorytetu). Priorytet profilu *X2* będzie zależał od początkowego stanu *X2* zasady *P(B)* i *X2* zasady *P(A)*. Po utworzeniu zasady *P(B)*, zasada *P(A)* nie będzie już wyświetlana w podgrupie *B*.

Aktywna zasada jest ponownie wyliczana za każdym razem, gdy uruchamiany jest Agent sieciowy, włączany i wyłączany jest tryb offline lub modyfikowana jest lista znaczników przydzielonych do urządzenia klienckiego. Na przykład, rozmiar pamięci RAM został zwiększony na urządzeniu, co spowodowało aktywowanie profilu zasad stosowanego na urządzeniach posiadających dużą ilość pamięci RAM.

Właściwości i ograniczenia profili zasad

Profile posiadają następujące właściwości:

- Profile nieaktywnej zasady nie mają wpływu na urządzenia klienckie.
- Jeśli dla zasady ustawiono stan **Zasada użytkownika mobilnego**, profile zasad będą także stosowane tylko wtedy, gdy urządzenie jest odłączone od sieci firmowej.
- Profile nie obsługują statycznej analizy dostępu do plików wykonywalnych.
- Profil zasad nie może zawierać żadnych ustawień powiadomień o zdarzeniach.
- Jeśli port UDP o numerze 15000 jest używany do łączenia urządzenia z Serwerem administracyjnym, w ciągu minuty od przydzielenia znacznika do urządzenia zostaje aktywowany odpowiedni profil zasad.
- Podczas tworzenia reguł aktywacji profilu zasad możesz korzystać z reguł dla połączenia Agenta sieciowego z Serwerem administracyjnym.

Tworzenie profilu zasad

Tworzenie profilu jest dostępne tylko dla zasad następujących aplikacji:

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows i nowsze wersje
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- Wtyczka Kaspersky Mobile Device Management w wersji 10 Service Pack 1 do wersji 10 Service Pack 3 Maintenance Release 1
- Wtyczka Kaspersky Device Management for iOS
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows i Linux

W celu utworzenia profilu zasad:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której profilu chcesz utworzyć profil zasad.
2. W obszarze roboczym grupy administracyjnej wybierz zakładkę **Zasady**.
3. Wybierz zasadę i przejdź do okna właściwości zasady, korzystając z menu kontekstowego.
4. Otwórz sekcję **Profile zasad** w oknie właściwości zasady, a następnie kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator nowego profilu zasad.
5. W oknie **Nazwa profilu zasad** określ następujące elementy:

   a. Nazwa profilu zasad

      Nazwa profilu nie może zawierać więcej niż 100 znaków.

   b. Stan profilu zasad (*Włączony* lub *Wyłączony*)

      Zalecamy utworzenie i włączenie nieaktywnych profili zasad dopiero po całkowitym zakończeniu pracy z ustawieniami i warunkami aktywacji profilu zasad.
6. Zaznacz pole **Po zamknięciu kreatora tworzenia nowej zasady, przejdź do konfiguracji reguły aktywacji profilu zasad**, aby uruchomić Kreator reguły aktywacji nowego profilu zasad. Postępuj zgodnie z instrukcjami kreatora.
7. Zmodyfikuj ustawienia profilu zasad w oknie właściwości profilu zasad w wybrany przez siebie sposób.
8. Zapisz zmiany, klikając **OK**.

   Profil zostanie zapisany. Profil zostanie aktywowany na urządzeniach, które spełniają warunki reguły aktywacji.

Dla jednej zasady można utworzyć kilka profili. Profile utworzone dla zasady są wyświetlane we właściwościach zasady, w sekcji **Profile zasad**. Możesz zmienić profil zasad i zmienić priorytet profilu, a także usunąć profil.

Modyfikowanie profilu zasad

Modyfikowanie ustawień profilu zasad

> Możliwość modyfikowania profilu zasad jest dostępna tylko dla profili Kaspersky Endpoint Security for Windows.

W celu zmodyfikowania profilu zasad:

1. W drzewie konsoli wybierz grupę administracyjną, dla której powinien zostać zmodyfikowany profil zasad.
2. W obszarze roboczym grupy wybierz zakładkę **Zasady**.
3. Wybierz zasadę i przejdź do okna właściwości zasady, korzystając z menu kontekstowego.
4. We właściwościach profilu otwórz sekcję **Profile zasad**.

   Ta sekcja zawiera listę zasad, które zostały utworzone dla zasad. Profile są wyświetlane na liście zgodnie z ich priorytetami.

5. Wybierz profil zasad i kliknij przycisk **Właściwości**.

6. Skonfiguruj profil w oknie właściwości:

   - Jeśli jest to konieczne, w sekcji **Ogólne** zmień nazwę profilu i włącz lub wyłącz profil, korzystając z pola **Włącz profil**.
   - W sekcji **Reguły aktywacji** zmodyfikuj reguły aktywacji profilu.
   - Zmodyfikuj ustawienia zasady w odpowiednich sekcjach.

7. Kliknij **OK**.

Zmodyfikowane ustawienia zostaną zastosowane po zsynchronizowaniu urządzenia z Serwerem administracyjnym (jeśli profil zasad jest aktywny) lub po wyzwoleniu reguły aktywacji (jeśli profil zasad jest nieaktywny).

Zmiana priorytetu profilu zasad

Priorytety profili zasad definiują kolejność aktywacji profili na urządzeniu klienckim. Priorytety są używane, jeśli dla różnych profili zasad ustawiono identyczne reguły aktywacji.

Na przykład utworzono dwa profile zasad: *Profil 1* i *Profil 2*, które różnią się wartościami jednego ustawienia (*Wartość 1* i *Wartość 2*). Priorytet *Profilu 1* jest wyższy niż priorytet *Profilu 2*. Co więcej, istnieją także profile, których priorytety są niższe niż *Profilu 2*. Reguły aktywacji dla tych profili są identyczne.

Jeśli zostanie wyzwolona reguła aktywacji, *Profil 1* zostanie aktywowany. Ustawienie na urządzeniu przyjmie *Wartość 1*. Jeśli usuniesz *Profil 1*, wówczas *Profil 2* będzie miał najwyższy priorytet, a ustawienie przyjmie *Wartość 2*.

Na liście profili zasad profile są wyświetlane zgodnie z ich priorytetami. Profil o najwyższym priorytecie znajduje się na liście na pierwszym miejscu. Priorytet profilu można zmienić za pomocą przycisku strzałki w górę  i strzałki w dół  .

Usuwanie profilu zasad

W celu usunięcia profilu zasad:

1. W drzewie konsoli należy wybrać grupę administracyjną, której profil zasad chcesz usunąć.

2. W obszarze roboczym grupy administracyjnej wybierz zakładkę **Zasady**.

3. Wybierz zasadę i przejdź do okna właściwości zasady, korzystając z menu kontekstowego.

4. Otwórz sekcję **Profile zasad** we właściwościach zasady Kaspersky Endpoint Security.

5. Wybierz profil zasad, który chcesz usunąć i kliknij przycisk **Usuń**.

Profil zasad zostanie usunięty. Stan Aktywny zostanie przydzielony innemu profilowi zasad, którego reguły aktywacji zostaną wyzwolone na urządzeniu, lub profilowi.

Tworzenie reguły aktywacji profilu zasad

W celu utworzenia reguły aktywacji profilu zasad:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której chcesz utworzyć regułę aktywacji profilu zasad.
2. W obszarze roboczym grupy wybierz zakładkę **Zasady**.
3. Wybierz zasadę i przejdź do okna właściwości zasady, korzystając z menu kontekstowego.
4. W oknie właściwości zasady otwórz sekcję **Profile zasad**.
5. Wybierz profil zasad, dla którego chcesz utworzyć regułę aktywacji, i kliknij przycisk **Właściwości**.

   Zostanie otwarte okno właściwości profilu zasad.

   Jeśli lista profili zasad jest pusta, możesz utworzyć profil zasad.
6. Wybierz sekcję **Reguły aktywacji** i kliknij przycisk **Dodaj**.

   Zostanie uruchomiony kreator nowej reguły aktywacji profilu zasad.
7. W oknie **Reguły aktywacji profilu zasad** zaznacz pola obok warunków, które mają wpływać na aktywację tworzonego profilu zasad:

   - **Główne reguły dotyczące aktywacji profilu zasad**

     Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od stanu trybu offline urządzenia, regułę połączenia z Serwerem administracyjnym, a także znaczniki przypisywane do urządzenia.

   - **Reguły dotyczące używania Active Directory**

     Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od obecności urządzenia w jednostce organizacyjnej Active Directory (OU) lub członkostwa urządzenia (lub jego właściciela) w grupie zabezpieczeń Active Directory.

   - **Reguły dla określonego właściciela urządzenia**

     Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od właściciela urządzenia.

   - **Reguły dla specyfikacji sprzętowej**

     Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od ilości pamięci oraz liczby procesów logicznych.

   Liczba dodatkowych okien w kreatorze zależy od ustawień wybranych w pierwszym kroku. Reguły aktywacji profili zasad można zmodyfikować w późniejszym czasie.

8. W oknie **Główne warunki** określ następujące ustawienia:

- W polu **Urządzenie jest w trybie offline**, na liście rozwijalnej określ warunek obecności urządzenia w sieci:

  - **Tak**

    Urządzenie jest w sieci zewnętrznej, co oznacza, że Serwer administracyjny nie jest dostępny.

  - **Nie**

    Urządzenie jest w sieci, więc Serwer administracyjny jest dostępny.

  - **Nie wybrano wartości**

    Kryterium nie będzie stosowane.

- W polu **Urządzenie znajduje się w określonej lokalizacji sieciowej** użyj listy rozwijalnej, aby skonfigurować aktywację profilu zasad, jeśli reguła połączenia z Serwerem administracyjnym jest wykonywana / nie jest wykonywana na tym urządzeniu:

  - **Wykonane / Niewykonane**

    Warunek aktywacji profilu zasad (czy reguła jest wykonywana).

  - **Nazwa reguły**

    Opis lokalizacji sieciowej urządzenia dla połączenia z Serwerem administracyjnym, którego warunki muszą być spełnione (lub nie muszą być spełnione) dla aktywacji profilu zasad.

    Opis lokalizacji sieciowej urządzeń dla połączenia z Serwerem administracyjnym może zostać utworzony lub skonfigurowany w regule przełączania Agenta sieciowego.

Okno **Główne warunki** jest wyświetlane, jeśli pole **Główne reguły dotyczące aktywacji profilu zasad** jest zaznaczone.

9. W oknie **Warunki używające znaczników** określ następujące ustawienia:

- **Lista znaczników**

  Na liście znaczników możesz określić regułę uwzględniania urządzenia w profilu zasad, zaznaczając pola obok odpowiednich znaczników.

  Możesz dodać nowe znaczniki do listy, wprowadzając je w polu nad listą i klikając przycisk **Dodaj**.

  Profil zasad obejmuje urządzenia z opisami zawierającymi wszystkie zaznaczone tagi. Jeśli pola nie są zaznaczone, kryterium nie jest stosowane. Domyślnie pola te nie są zaznaczone.

- **Zastosuj do urządzeń bez określonych znaczników**

  Włącz tę opcje, jeśli musisz odwrócić wybór znaczników.

  Jeśli ta opcja jest włączona, profil zasad obejmuje urządzenia z opisami, które nie zawierają żadnego z wybranych znaczników. Jeśli ta opcja jest wyłączona, kryterium nie zostanie zastosowane.

  Domyślnie opcja ta jest wyłączona.

Okno **Warunki używające znaczników** jest wyświetlane, jeśli pole **Główne reguły dotyczące aktywacji profilu zasad** jest zaznaczone.

10. W oknie **Warunki zawierające Active Directory** określ następujące ustawienia:

    - **Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory**

      Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu, którego właściciel jest członkiem określonej grupy zabezpieczeń. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

    - **Członkostwo urządzenia w grupie zabezpieczeń Active Directory**

      Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

    - **Alokacja urządzenia w jednostce organizacyjnej Active Directory**

      Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu, które jest uwzględnione w określonej jednostce organizacyjnej Active Directory. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane.

      Domyślnie opcja ta jest wyłączona.

    Okno **Warunki zawierające Active Directory** jest wyświetlane, jeśli pole **Reguły dotyczące używania Active Directory** jest zaznaczone.

11. W oknie **Warunki zawierające właściciela urządzenia** określ następujące ustawienia:

    - **Właściciel urządzenia**

      Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu zgodnie z jego właścicielem. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

      - Urządzenie należy do określonego właściciela (znak „=").
      - Urządzenie nie należy do określonego właściciela (znak „#").

        Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić właściciela urządzenia, gdy opcja jest włączona. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

    - **Właściciel urządzenia należy do wewnętrznej grupy zabezpieczeń**

      Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu według przynależności właściciela do wewnętrznej grupy zabezpieczeń Kaspersky Security Center. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

      - Właściciel urządzenia jest członkiem określonej grupy bezpieczeństwa (znak „=").
      - Właściciel urządzenia nie jest członkiem określonej grupy bezpieczeństwa (znak „#").

        Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić grupę zabezpieczeń Kaspersky Security Center. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

    - **Aktywuj profil zasad określoną rolą właściciela urządzenia**

      Wybierz te opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu w zależności od roli właściciela. Dodaj rolę ręcznie z listy istniejących ról.

      Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium.

Okno **Warunki zawierające właściciela urządzenia** wyświetlone zostanie, jeśli zaznaczymy pole **Reguły dla określonego właściciela urządzenia**.

12. W oknie **Warunki zawierające specyfikacje sprzętowe** określ następujące ustawienia:

    - **Rozmiar pamięci RAM, w MB**

      Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu według ilości pamięci RAM dostępnej na tym urządzeniu. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

      - Rozmiar pamięci RAM jest mniejszy niż określona wartość (znak „<").
      - Rozmiar pamięci RAM jest większy niż określona wartość (znak „>").

      Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić ilość pamięci RAM na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

    - **Liczba procesorów logicznych**

      Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu według liczby procesorów logicznych na tym urządzeniu. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

      - Liczba procesorów logicznych na urządzeniu jest mniejsza niż lub równa określonej wartości (znak „<").
      - Liczba procesorów logicznych na urządzeniu jest większa niż lub równa określonej wartości (znak „>").

      Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić liczbę procesorów logicznych na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

    Okno **Warunki zawierające specyfikacje sprzętowe** jest wyświetlane, jeśli pole **Reguły dla specyfikacji sprzętowej** jest zaznaczone.

13. W oknie **Nazwa reguły aktywacji profilu zasad**, w polu **Nazwa reguły** określ nazwę dla reguły.

Profil zostanie zapisany. Profil zostanie aktywowany na urządzeniu po wyzwoleniu reguł aktywacji.

Reguły aktywacji profilu zasad utworzone dla profilu będą wyświetlone we właściwościach profilu zasad, w sekcji **Reguły aktywacji**. Możesz zmodyfikować lub usunąć dowolną regułę aktywacji profilu zasad.

Jednocześnie może być wyzwolonych kilka reguł aktywacji.

Reguły przenoszenia urządzeń

Zalecane jest automatyczne przydzielanie urządzeń do grup administracyjnych poprzez użycie *reguł przenoszenia urządzeń*. Reguła przenoszenia urządzeń składa się z trzech głównych części: nazwy, warunku wykonania (wyrażenie logiczne z atrybutami urządzenia) oraz docelowej grupy administracyjnej. Reguła przenosi urządzenie do docelowej grupy administracyjnej, jeśli atrybuty urządzenia spełniają warunek wykonania reguły.

Wszystkie reguły przenoszenia urządzeń posiadają priorytety. Serwer administracyjny sprawdza, czy atrybuty urządzenia spełniają warunek wykonania każdej reguły, w rosnącej kolejności priorytetów. Jeśli atrybuty urządzenia spełniają warunek wykonania reguły, urządzenie zostaje przeniesione do grupy docelowej, a przetwarzanie reguły zostanie zakończone dla tego urządzenia. Jeśli atrybuty urządzenia spełniają warunki kilku reguł, urządzenie zostanie przeniesione do grupy docelowej reguły z najwyższym priorytetem (czyli tej, która znajduje się najwyżej na liście).

Reguły przenoszenia urządzeń mogą być tworzone pośrednio. Na przykład, we właściwościach pakietu instalacyjnego lub zadania zdalnej instalacji możesz określić grupę administracyjną, do której urządzenie musi zostać przeniesione po zainstalowaniu na nim Agenta sieciowego. Reguły przenoszenia urządzeń mogą być tworzone także bezpośrednio przez administratora Kaspersky Security Center na liście reguł przenoszenia. Lista ta znajduje się w Konsoli administracyjnej, we właściwościach grupy **Urządzenia nieprzypisane**.

Domyślnie reguła przenoszenia urządzeń jest przeznaczona do jednorazowego, wstępnego przydzielenia urządzeń do grup administracyjnych. Reguła przenosi urządzenia z grupy **Urządzenia nieprzypisane** tylko raz. Jeśli urządzenie był już raz przeniesione przy użyciu tej reguły, reguła ta nie przeniesie go już nawet wtedy, gdy ręcznie przeniesiesz urządzenie z powrotem do grupy **Urządzenia nieprzypisane**. Jest to zalecany sposób stosowania reguł przenoszenia.

Możesz przenieść urządzenia, które już zostały przydzielone do niektórych grup administracyjnych. Aby to zrobić, we właściwościach reguły odznacz pole **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**.

Stosowanie reguł przenoszenia do urządzeń, które już zostały przydzielone do niektórych grup administracyjnych, znacząco zwiększa obciążenie na Serwerze administracyjnym.

Pole wyboru **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych** jest zablokowane we właściwościach automatycznie tworzonych reguł przenoszenia. Takie reguły są tworzone podczas dodawania zadania *Zdalna instalacja aplikacji* lub tworzenia autonomicznego pakietu instalacyjnego.

Możesz utworzyć regułę przenoszenia, która będzie nieprzerwanie oddziaływać na jedno urządzenie.

Szczególnie zalecane jest unikanie ciągłego przenoszenia jednego urządzenia z jednej grupy do drugiej (na przykład, w celu zastosowania specjalnej zasady do tego urządzenia, uruchomienia specjalnego zadania grupowego lub zaktualizowania urządzenia poprzez punkt dystrybucji).

Takie scenariusze nie są obsługiwane, ponieważ w bardzo dużym stopniu zwiększają obciążenie na Serwerze administracyjnym oraz ruch sieciowy. Te scenariusze doprowadzają też do konfliktu z zasadami działania Kaspersky Security Center (szczególnie w obszarze uprawnień dostępu, zdarzeń i raportów). Należy znaleźć inne rozwiązanie, na przykład, poprzez użycie profili zasad, zadań dla wyborów urządzeń, przydzielania Agentów sieciowych zgodnie ze standardowym scenariuszem.

Klonowanie reguł przenoszenia urządzeń

Jeśli musisz utworzyć kilka reguł przenoszenia urządzeń z podobnymi ustawieniami, możesz sklonować istniejącą regułę i zmienić ustawienia sklonowanej reguły. Na przykład, jest to przydatne, gdy musisz mieć kilka identycznych reguł przenoszenia urządzeń z różnymi zakresami adresów IP i grupami docelowymi.

W celu sklonowania reguły przenoszenia urządzeń:

1. Otwórz okno główne aplikacji.
2. W folderze **Urządzenia nieprzypisane** kliknij **Konfiguruj reguły**.
   Zostanie otwarte okno **Właściwości: Urządzenia nieprzypisane**.
3. W sekcji **Przenieś urządzenia** wybierz regułę przenoszenia urządzeń, którą chcesz sklonować.
4. Kliknij **Sklonuj regułę**.

   Klon wybranej reguły przenoszenia urządzeń zostanie dodany na końcu listy.

Nowa reguła zostanie utworzona ze stanem wyłączenia. Regułę można edytować i włączać w dowolnym momencie.

Kategoryzacja oprogramowania

Głównym narzędziem do monitorowania uruchomień aplikacji są *kategorie Kaspersky* (zwane dalej *Kategorie KL*). Kategorie KL umożliwiają administratorom Kaspersky Security Center uproszczenie obsługi kategoryzacji oprogramowania i zminimalizowanie ruchu sieciowego skierowanego do zarządzanych urządzeń.

Kategorie użytkownika powinny być tworzone tylko dla aplikacji, których nie można zaklasyfikować do żadnej z istniejących kategorii KL (na przykład, dla oprogramowania wykonanego na zamówienie użytkownika). Kategorie użytkownika są tworzone na podstawie pakietu instalacyjnego aplikacji (MSI) lub folderu z pakietami instalacyjnymi.

Jeśli dostępna jest duża ilość programów, które nie zostały skategoryzowane poprzez kategorie KL, można utworzyć automatycznie aktualizowaną kategorię. Sumy kontrolne plików wykonywalnych będą automatycznie dodawane do tej kategorii po każdej modyfikacji folderu zawierającego pakiety dystrybucyjne.

Nie twórz automatycznie aktualizowanych kategorii oprogramowania dla folderów Moje dokumenty, %windir%, %Pliki programów% i %Pliki programów(x86)%. Pula plików w tych folderach podlega częstym zmianom, co prowadzi do zwiększonego obciążenia na Serwerze administracyjnym i zwiększonego ruchu sieciowego. Należy utworzyć dedykowany folder ze zbiorem oprogramowania i okresowo dodawać do niego nowe elementy.

Wymagania wstępne do zainstalowania aplikacji na urządzeniach w organizacji klienta

Proces zdalnej instalacji aplikacji na urządzeniach w organizacji klienta jest taki sam, jak proces zdalnej instalacji w obrębie korporacji.

W celu zainstalowania aplikacji na urządzeniach w organizacji klienta, należy wykonać następujące działania:

- Przed pierwszą instalacją aplikacji na urządzeniach w organizacji klienta zainstaluj na nich Agenta sieciowego.

Przy konfigurowaniu pakietu instalacyjnego Agenta sieciowego przez dostawcę usługi w Kaspersky Security Center, należy dostosować następujące ustawienia w oknie właściwości pakietu instalacyjnego:

- W sekcji **Połączenie**, w wierszu **Serwer administracyjny** określ adres tego samego wirtualnego Serwera administracyjnego, który określono w punkcie dystrybucji podczas lokalnej instalacji Agenta sieciowego.
- W sekcji **Zaawansowane** zaznacz pole **Połącz z Serwerem administracyjnym korzystając z bramy połączenia**. W wierszu **Adres bramy połączenia** określ adres punktu dystrybucji. Można użyć adresu IP lub nazwy urządzenia w sieci Windows.

- Wybierz **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji** jako metodę pobierania dla pakietu instalacyjnego Agenta sieciowego. Metodę pobierania można wybrać w następujący sposób:
  - Jeśli instalujesz aplikację, korzystając z zadania zdalnej instalacji, możesz określić metodę w jeden z następujących sposobów:
    - Podczas tworzenia zadania zdalnej instalacji w oknie **Ustawienia**
    - W oknie właściwości zadania zdalnej instalacji, w sekcji **Ustawienia**
  - Jeśli instalujesz aplikacje, korzystając z kreatora zdalnej instalacji, możesz wybrać metodę pobierania w oknie **Ustawienia** tego kreatora.
- Konto wykorzystywane przez punkt dystrybucji do autoryzacji musi mieć uprawnienia dostępu do zasobu Admin$ na wszystkich urządzeniach klienckich.

Przeglądanie i modyfikowanie lokalnych ustawień aplikacji

System administracyjny Kaspersky Security Center umożliwia zdalne zarządzanie lokalnymi ustawieniami aplikacji na urządzeniach z poziomu Konsoli administracyjnej.

Lokalne ustawienia aplikacji są ustawieniami aplikacji określonymi dla urządzenia. Możesz użyć Kaspersky Security Center do określenia lokalnych ustawień aplikacji na urządzeniach znajdujących się w grupach administracyjnych.

Szczegółowe opisy ustawień aplikacji firmy Kaspersky znajdują się w odpowiednich dokumentach.

W celu przejrzenia lub modyfikacji lokalnych ustawień aplikacji:

1. W obszarze roboczym grupy, do której należą żądane urządzenia, wybierz zakładkę **Urządzenia**.
2. W oknie właściwości urządzenia, w sekcji **Aplikacje** wybierz żądaną aplikację.
3. Otwórz okno właściwości aplikacji, klikając dwukrotnie nazwę aplikacji lub klikając przycisk **Właściwości**.

Zostanie otwarte okno lokalnych ustawień wybranej aplikacji, w którym będziesz mógł je przeglądać i modyfikować.

Możesz zmienić wartości ustawień, których modyfikowanie nie zostało zablokowane przez zasadę grupy (tzn. które nie są oznaczone ikoną kłódki (🔒) w zasadzie).

Aktualizowanie Kaspersky Security Center i zarządzanych aplikacji

Ta sekcja opisuje kroki, jakie musisz podjąć, aby zaktualizować Kaspersky Security Center i zarządzane aplikacje.

Scenariusz: Regularne aktualizowanie baz danych i aplikacji Kaspersky

Ta sekcja oferuje scenariusz regularnego aktualizowania baz danych, modułów i aplikacji firmy Kaspersky. Po zakończeniu Konfigurowania scenariusza ochrony sieci, musisz zachować niezawodność systemu ochrony, aby upewnić się, że Serwery administracyjne i zarządzane urządzenia są chronione przed różnymi zagrożeniami, w tym wirusami, atakami sieciowymi i atakami phishingowymi.

Aktualność ochrony sieci jest zapewniana przez regularne aktualizacje:

- Baz danych i modułów oprogramowania firmy Kaspersky
- Zainstalowane aplikacje firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające

Po zakończeniu tego scenariusza, możesz być pewny, że:

- Twoja sieć jest chroniona przez najaktualniejsze oprogramowanie firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające.
- Antywirusowe bazy danych i inne bazy danych Kaspersky krytyczne dla bezpieczeństwa sieci są zawsze aktualne.

Wymagania wstępne

Zarządzane urządzenia muszą mieć połączenie z Serwerem administracyjnym. Jeśli nie mają połączenia, rozważ ręczne zaktualizowanie baz danych, modułów i aplikacji Kaspersky lub bezpośrednio z serwerów aktualizacji Kaspersky.

Serwer administracyjny musi mieć połączenie z Internetem.

Przed rozpoczęciem upewnij się, że:

1. Wdrożono aplikacje zabezpieczające Kaspersky na zarządzanych urządzeniach zgodnie ze scenariuszem wdrażania aplikacji Kaspersky poprzez Kaspersky Security Center Web Console.
2. Utworzyłeś i skonfigurowałeś wszystkie wymagane zasady, profile zasad i zadania zgodnie ze scenariuszem konfigurowania ochrony sieci.
3. Przydzieliłeś odpowiednią liczbę punktów dystrybucji zgodnie z liczbą zarządzanych urządzeń i topologią sieci.

Aktualizowanie baz danych i aplikacji Kaspersky odbywa się w etapach:

1. **Wybranie schematu aktualizacji**

   Istnieje kilka schematów, których możesz użyć do zainstalowania aktualizacji dla komponentów Kaspersky Security Center i aplikacji zabezpieczających. Wybierz schemat lub kilka schematów, które najlepiej spełniają wymagania Twojej sieci.

2. **Tworzenie zadania pobierania aktualizacji do repozytorium Serwera administracyjnego**

   To zadanie jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Jeśli nie uruchamiałeś kreatora, utwórz zadanie teraz.

   To zadanie jest wymagane do pobrania uaktualnień z serwerów aktualizacji Kaspersky do repozytorium Serwera administracyjnego, a także do zaktualizowania baz danych i modułów Kaspersky dla aplikacji Kaspersky Security Center. Po pobraniu uaktualnień, mogą one zostać przesłane na zarządzane urządzenia.

   Jeśli w Twojej sieci są przypisane punkty dystrybucji, uaktualnienia są automatycznie pobierane z repozytorium Serwera administracyjnego do repozytoriów punktów dystrybucji. W tym przypadku zarządzane urządzenia, znajdujące się w obszarze punktu dystrybucji, pobierają uaktualnienia z repozytorium punktu dystrybucji zamiast repozytorium Serwera administracyjnego.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie zadania pobierania uaktualnień do repozytorium Serwera administracyjnego
   - Kaspersky Security Center Web Console: Tworzenie zadania pobierania uaktualnień do repozytorium Serwera administracyjnego

3. **Tworzenie zadania pobierania aktualizacji do repozytoriów punktów dystrybucji (opcjonalne)**

   Domyślnie, uaktualnienia są pobierane do punktów dystrybucji z Serwera administracyjnego. Możesz skonfigurować Kaspersky Security Center do pobierania uaktualnień do punktów dystrybucji bezpośrednio z serwerów aktualizacji Kaspersky. Pobranie do repozytoriów punktów dystrybucji jest preferowane, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktami dystrybucji jest droższy niż ruch sieciowy pomiędzy punktami dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu.

   Jeśli do Twojej sieci są przypisane punkty dystrybucji i utworzone jest zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, punkty dystrybucji pobiorą uaktualnienia z serwerów aktualizacji Kaspersky, a nie z repozytorium Serwera administracyjnego.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie zadania pobierania uaktualnień do repozytoriów punktów dystrybucji
   - Kaspersky Security Center Web Console: Tworzenie zadania pobierania uaktualnień do repozytoriów punktów dystrybucji

4. **Konfigurowanie punktów dystrybucji**

   Jeśli w Twojej sieci są przypisane punkty dystrybucji, upewnij się, że opcja **Roześlij aktualizacje** jest włączona we właściwościach wszystkich wymaganych punktów dystrybucji. Jeśli ta opcja jest włączona dla punktu dystrybucji, urządzenia znajdujące się w obszarze punktu dystrybucji pobierają uaktualnienia z repozytorium Serwera administracyjnego.

   Jeśli chcesz, żeby zarządzane urządzenia pobierały uaktualnienia tylko z punktów dystrybucji, włącz opcję **Rozsyłaj pliki tylko poprzez punkty dystrybucji** w zasadzie Agenta sieciowego.

5. **Optymalizowanie procesu aktualizacji przy użyciu trybu offline pobierania uaktualnień lub plików diff (opcjonalne)**

Możesz zoptymalizować proces aktualizacji przy użyciu trybu offline pobierania uaktualnień (włączone domyślnie) lub przy użyciu plików diff. Dla każdego segmentu sieci musisz wybrać, którą z tych dwóch funkcji włączyć, ponieważ nie mogą działać jednocześnie.

Jeśli tryb offline pobierania uaktualnień jest włączony, Agent sieciowy pobierze wymagane uaktualnienia na zarządzane urządzenie po pobraniu uaktualnień do repozytorium Serwera administracyjnego, zanim aplikacja zabezpieczająca zażąda uaktualnień. Zwiększy to niezawodność procesu aktualizacji. Aby korzystać z tej funkcji, włącz opcję **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)** w zasadzie Agenta sieciowego.

Jeśli nie używasz trybu offline pobierania uaktualnień, możesz zoptymalizować ruch sieciowy między Serwerem administracyjnym a zarządzanymi urządzeniami przy użyciu plików diff. Jeśli ta funkcja jest włączona, Serwer administracyjny lub punkt dystrybucji pobierze pliki diff zamiast całych plików baz danych lub modułów Kaspersky. Plik diff opisuje różnice między dwoma wersjami pliku bazy danych lub modułu programu. Dlatego też plik diff zajmuje mniej miejsca niż cały plik. Spowoduje to zmniejszenie ruchu sieciowego między Serwerem administracyjnym lub punktami dystrybucji a zarządzanymi urządzeniami. Aby użyć tej funkcji, włącz opcję **Pobierz pliki diff** we właściwościach zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* i/lub zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

Dostępne instrukcje:

- Używanie plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky
- Konsola administracyjna: Włączanie i wyłączanie trybu offline pobierania uaktualnień
- Kaspersky Security Center Web Console: Włączanie i wyłączanie trybu offline pobierania uaktualnień

6 Sprawdzanie pobranych uaktualnień (opcjonalne)

Przed zainstalowaniem pobranych uaktualnień możesz zweryfikować uaktualnienia poprzez zadanie *Weryfikacja uaktualnień*. To zadanie kolejno uruchamia zadania aktualizacji i zadania skanowania w poszukiwaniu złośliwego oprogramowania urządzeń, skonfigurowane poprzez ustawienia dla określonego zbioru urządzeń testowych. Po uzyskaniu wyników zadania, Serwer administracyjny uruchamia lub blokuje propagację aktualizacji na pozostałe urządzenia.

Zadanie *Weryfikacja uaktualnień* jest wykonywane jako część zadania *Pobierz uaktualnienia do repozytorium serwera administracyjnego*. We właściwościach zadania *Pobierz uaktualnienia do repozytorium serwera administracyjnego* włącz opcję **Zweryfikuj uaktualnienia przed rozesłaniem** przed dystrybucją w konsoli administracyjnej lub opcję **Uruchom weryfikację aktualizacji** w Kaspersky Security Center Web Console.

Dostępne instrukcje:

- Konsola administracyjna: Weryfikowanie pobranych uaktualnień
- Kaspersky Security Center Web Console: Weryfikowanie pobranych uaktualnień

7 Zatwierdzanie i odrzucanie aktualizacji oprogramowania

Domyślnie pobrane aktualizacje oprogramowania posiadają stan *Niezdefiniowane*. Możesz zmienić stan na *Zatwierdzone* lub *Odrzucone*. Zatwierdzone aktualizacje są zawsze instalowane. Jeśli aktualizacja wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej użytkownika końcowego, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia. Niezdefiniowane aktualizacje mogą zostać zainstalowane tylko na Agencie sieciowym, a inne komponenty Kaspersky Security Center zgodnie z ustawieniami zasady Agenta sieciowego. Aktualizacje, dla których ustawiłeś stan *Odrzucone*, nie zostaną zainstalowane na urządzeniach. Jeśli odrzucona aktualizacja dla aplikacji zabezpieczającej została wcześniej zainstalowana, Kaspersky Security Center spróbuje odinstalować aktualizację ze wszystkich urządzeń.

Zatwierdzanie i odrzucanie aktualizacji jest dostępne tylko w przypadku Agenta sieciowego i aplikacji zarządzanych Kaspersky zainstalowanych na urządzeniach klienckich z systemem Windows i Linux. Bezproblemowa aktualizacja Serwera administracyjnego, Kaspersky Security Center Web Console i webowych wtyczek administracyjnych nie jest obsługiwana.

Dostępne instrukcje:

- Konsola administracyjna: Zatwierdzanie i odrzucanie aktualizacji oprogramowania
- Kaspersky Security Center Web Console: Zatwierdzanie i odrzucanie aktualizacji oprogramowania

8. **Konfigurowanie automatycznej instalacji uaktualnień i poprawek dla komponentów Kaspersky Security Center**

   Pobrane aktualizacje i poprawki dla Agenta sieciowego i innych komponentów Kaspersky Security Center są instalowane automatycznie. Jeśli pozostawiłeś opcję **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany** włączoną we właściwościach Agenta sieciowego, wówczas wszystkie uaktualnienia zostaną zainstalowane automatycznie po ich pobraniu do repozytorium (lub kilku repozytoriów). Jeśli ta opcja jest wyłączona, poprawki Kaspersky, które zostały pobrane i oznaczone jako *Niezdefiniowane*, zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzone*.

   Dostępne instrukcje:

   - Konsola administracyjna: Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center
   - Kaspersky Security Center Web Console: Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center

9. **Instalacja uaktualnień dla Serwera administracyjnego**

   Aktualizacje oprogramowania dla Serwera administracyjnego nie zależą od stanów aktualizacji. Nie są instalowane automatycznie i muszą być wcześniej zatwierdzone przez administratora na zakładce **Monitorowanie** w Konsoli administracyjnej (**Serwer administracyjny** <nazwa serwera> → **Monitorowanie**) lub w sekcji **Powiadomienia** w Kaspersky Security Center Web Console (**Monitorowanie i raportowanie** → **Powiadomienia**). Następnie administrator musi wyraźnie uruchomić instalację uaktualnień.

10. **Konfigurowanie automatycznej instalacji uaktualnień dla aplikacji zabezpieczających**

    Utwórz zadania *Aktualizacji* dla zarządzanych aplikacji, aby zapewnić najnowsze aktualizacje aplikacji, modułów oprogramowania i baz danych Kaspersky, w tym antywirusowych baz danych. Aby zapewnić terminowe aktualizacje, zalecamy wybranie opcji **Po pobraniu nowych aktualizacji do repozytorium** podczas konfigurowania terminarza zadań.

    Jeśli Twoja sieć zawiera urządzenia obsługujące tylko protokół IPv6 i chcesz regularnie aktualizować aplikacje zabezpieczające zainstalowane na tych urządzeniach, upewnij się, że na zarządzanych urządzeniach zainstalowany jest Serwer administracyjny (w wersji nie wcześniejszej niż 13.2) oraz Agent sieciowy (w wersji nie wcześniejszej niż 13.2).

    Domyślnie, uaktualnienia dla Kaspersky Endpoint Security for Windows i Kaspersky Endpoint Security for Linux są instalowane dopiero po zmianie stanu aktualizacji na *Zatwierdzone*. Ustawienia aktualizacji można zmienić w zadaniu *Aktualizacja*.

    Jeśli aktualizacja wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej użytkownika końcowego, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia.

    Dostępne instrukcje:

    - Konsola administracyjna: Automatyczna instalacja uaktualnień dla Kaspersky Endpoint Security na urządzeniach
    - Kaspersky Security Center Web Console: Automatyczna instalacja uaktualnień dla Kaspersky Endpoint Security na urządzeniach

Wyniki

Po zakończeniu scenariusza, Kaspersky Security Center jest konfigurowany do aktualizowania baz danych Kaspersky i zainstalowanych aplikacji Kaspersky po pobraniu uaktualnień do repozytorium Serwera administracyjnego lub do repozytoriów punktów dystrybucji. Możesz przejść do monitorowania stanu sieci.

Informacje o aktualizowaniu baz danych, modułów i aplikacji Kaspersky

W celu upewnienia się, że ochrona Serwerów administracyjnych i zarządzanych urządzeń jest aktualna, w odpowiednim czasie należy dostarczać aktualizacje:

- Baz danych i modułów oprogramowania firmy Kaspersky

  Przed pobraniem baz danych i modułów oprogramowania Kaspersky oprogramowanie Kaspersky Security Center sprawdza, czy serwery Kaspersky są dostępne. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Jest to konieczne, aby zapewnić aktualizację antywirusowych baz danych oraz zachować poziom bezpieczeństwa zarządzanych urządzeń.

- Zainstalowane aplikacje firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające

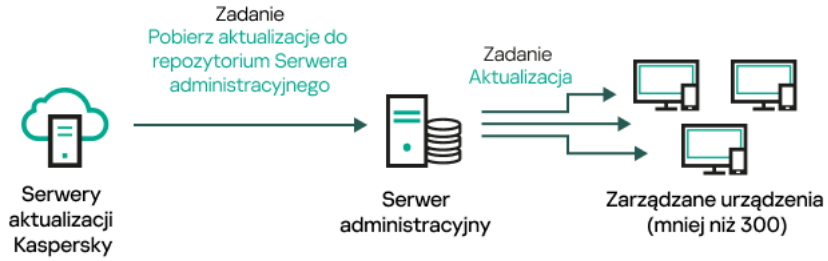
  Kaspersky Security Center umożliwia automatyczną aktualizację Agenta sieciowego i aplikacji Kaspersky zainstalowanych na urządzeniach klienckich z systemem Windows i Linux. Bezproblemowa aktualizacja Serwera administracyjnego, Kaspersky Security Center Web Console i webowych wtyczek administracyjnych nie jest obsługiwana. Aby zaktualizować aplikacje, pobierz najnowsze wersje aplikacji z witryny internetowej Kaspersky, a następnie zainstaluj je ręcznie.

W zależności od konfiguracji sieci, możesz użyć następujących schematów pobierania i rozsyłania żądanych aktualizacji na zarządzane urządzenia:

- Za pomocą jednego zadania: *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
- Używanie dwóch zadań:
  - Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
  - Zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*
- Ręcznie poprzez folder lokalny, folder współdzielony lub serwer FTP
- Bezpośrednio z serwerów aktualizacji Kaspersky do Kaspersky Endpoint Security na zarządzanych urządzeniach
- Poprzez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

Używanie zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego

W tym schemacie Kaspersky Security Center pobiera aktualizacje za pośrednictwem zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. W małych sieciach, które zawierają mniej niż 300 zarządzanych urządzeń w jednym segmencie sieci lub mniej niż 10 zarządzanych urządzeń w każdym segmencie sieci, aktualizacje są rozsyłane na zarządzane urządzenia bezpośrednio z repozytorium Serwera administracyjnego (patrz rysunek poniżej).

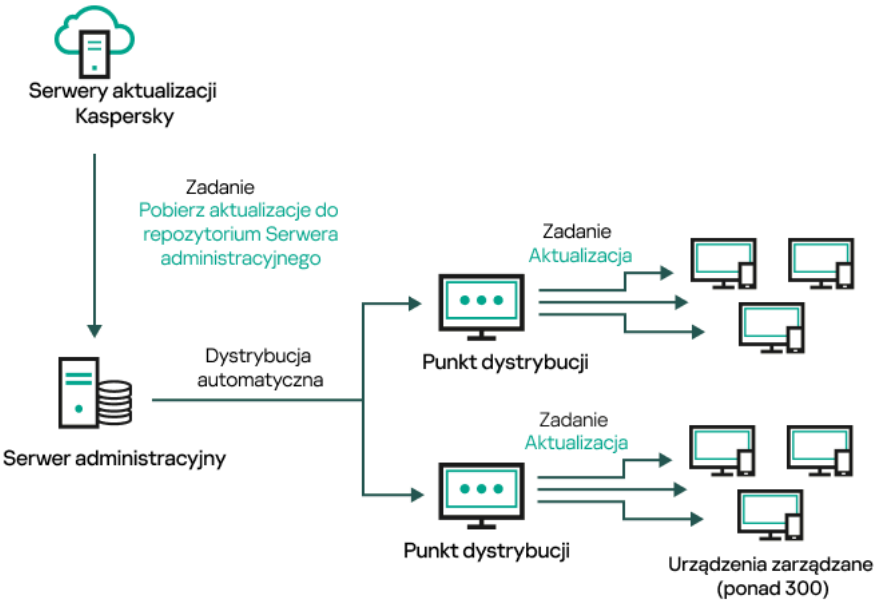


Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego bez punktów dystrybucji

Domyślnie, Serwer administracyjny komunikuje się z serwerami aktualizacji Kaspersky i pobiera uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny, aby używał protokołu HTTP zamiast HTTPS.

Jeśli sieć zawiera ponad 300 zarządzanych urządzeń w jednym segmencie sieci lub jeśli sieć zawiera kilka segmentów sieci z ponad 9 zarządzanymi urządzeniami w każdym segmencie sieci, zalecane jest użycie punktów dystrybucji do przesyłania aktualizacji na zarządzane urządzenia (patrz rysunek poniżej). Punkty dystrybucji zmniejszają obciążenie na Serwerze administracyjnym i optymalizują ruch sieciowy między Serwerem administracyjnym i zarządzanymi urządzeniami. Możesz obliczyć liczbę i konfigurację punktów dystrybucji wymaganych dla Twojej sieci.

W tym schemacie, uaktualnienia są automatycznie pobierane z repozytorium Serwera administracyjnego do repozytoriów punktów dystrybucji. Zarządzane urządzenia, znajdujące się w obszarze punktu dystrybucji, pobierają uaktualnienia z repozytorium punktu dystrybucji zamiast repozytorium Serwera administracyjnego.



Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego z punktami dystrybucji

Jeśli zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* zostało zakończone, z repozytorium Serwera administracyjnego zostają pobrane następujące aktualizacje:

- Bazy danych i moduły Kaspersky dla Kaspersky Security Center

  Te aktualizacje są instalowane automatycznie.

- Bazy danych i moduły Kaspersky dla aplikacji zabezpieczających na zarządzanych urządzeniach

  Te aktualizacje są instalowane poprzez zadanie Aktualizacja dla Kaspersky Endpoint Security for Windows.

- Aktualizacje dla Serwera administracyjnego

  Te aktualizacje nie są instalowane automatycznie. Administrator musi wyraźnie zatwierdzić i uruchomić instalację aktualizacji.

  > Uprawnienia lokalnego administratora są wymagane do zainstalowania łat na Serwerze administracyjnym.

- Aktualizacje dla komponentów Kaspersky Security Center

  Domyślnie, te aktualizacje są instalowane automatycznie. Możesz zmienić ustawienia w zasadzie Agenta sieciowego.

- Aktualizacje dla aplikacji zabezpieczających

  Domyślnie Kaspersky Endpoint Security for Windows zainstaluje tylko te aktualizacje, które zatwierdzisz. (Aktualizacje możesz zatwierdzić za pośrednictwem Konsoli administracyjnej lub za pośrednictwem konsoli Kaspersky Security Center Web Console). Aktualizacje są instalowane poprzez zadanie *Aktualizacja* i mogą zostać skonfigurowane we właściwościach tego zadania.

> Zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego* nie jest dostępne na wirtualnych Serwerach administracyjnych. Repozytorium wirtualnego Serwera administracyjnego wyświetla uaktualnienia pobrane na główny Serwer administracyjny.

Możesz skonfigurować sprawdzanie aktualizacji pod kątem łatwości obsługi i błędów na zestawie urządzeń testowych. Jeśli weryfikacja zostanie zakończona pomyślnie, aktualizacje będą rozsyłane na inne zarządzane urządzenia.

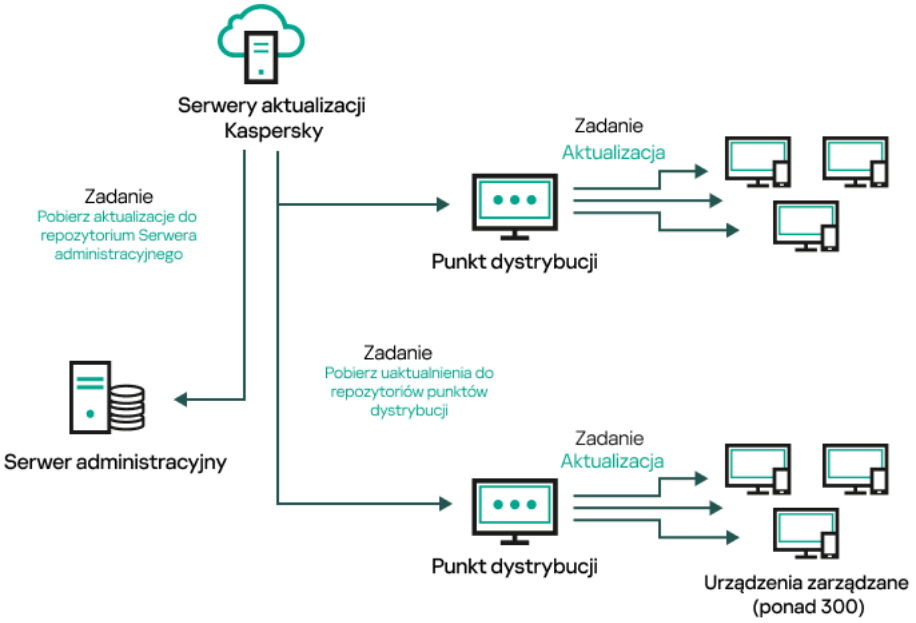
Każda aplikacja Kaspersky żąda wymaganych aktualizacji z Serwera administracyjnego. Serwer administracyjny gromadzi te żądania i pobiera tylko te uaktualnienia, które zostały zażądane przez aplikację. Dzięki temu te same uaktualnienia nie są pobierane kilka razy, a niepotrzebne uaktualnienia nie są pobierane wcale. Podczas wykonywania zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, Serwer administracyjny automatycznie wysyła następujące informacje do serwerów aktualizacji Kaspersky w celu zapewnienia pobrania najnowszych wersji baz danych i modułów aplikacji Kaspersky:

- Identyfikator i wersja aplikacji
- Identyfikator instalacji aplikacji
- Identyfikator aktywnego klucza
- ID uruchamiania zadania *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*

Żadna z przesyłanych informacji nie zawiera danych osobowych ani innych poufnych danych. Firma AO Kaspersky Lab chroni informacje zgodnie z wymogami wynikającymi z przepisów prawa.

Używanie dwóch zadań: zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego oraz zadanie Pobierz aktualizacje do repozytoriów punktów dystrybucji

Możesz pobrać aktualizacje do repozytoriów punktów dystrybucji bezpośrednio z serwerów aktualizacji Kaspersky zamiast repozytorium Serwera administracyjnego, a następnie rozesłać aktualizacje na zarządzane urządzenia (patrz rysunek poniżej). Pobranie do repozytoriów punktów dystrybucji jest preferowane, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktami dystrybucji jest droższy niż ruch sieciowy pomiędzy punktami dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu.



Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego oraz zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji

Domyślnie, Serwer administracyjny i punkty dystrybucji komunikują się z serwerami aktualizacji Kaspersky i pobierają uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny i/lub punkty dystrybucji do używania protokołu HTTP zamiast HTTPS.

Aby zaimplementować ten schemat, utwórz zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji* jako dodatek do zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Po pobraniu przez punkty dystrybucji aktualizacji z serwerów aktualizacji Kaspersky, a nie z repozytorium Serwera administracyjnego.

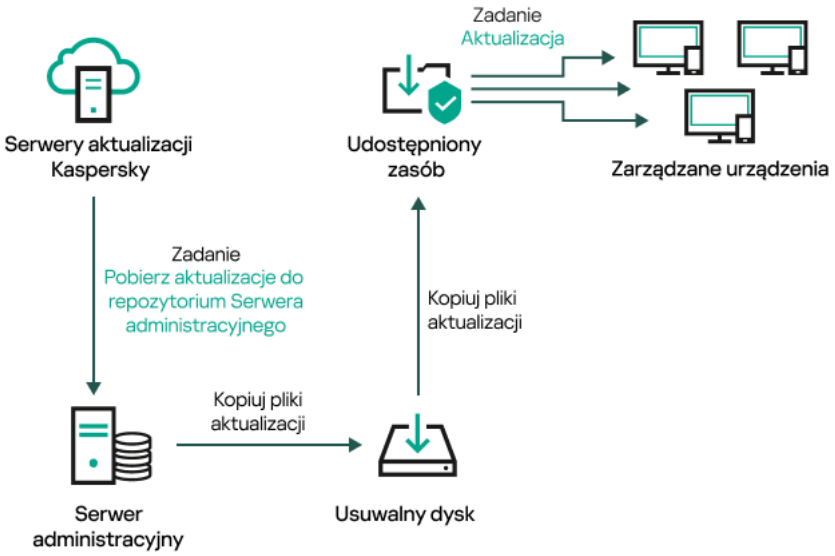
Urządzenia punktów dystrybucji działające pod kontrolą systemu operacyjnego macOS nie mogą pobierać uaktualnień z serwerów aktualizacji Kaspersky.

W przypadku, gdy jedno lub więcej urządzeń działających pod kontrolą systemu operacyjnego macOS znajduje się w obszarze zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, zadanie zostaje zakończone ze stanem *Niepowodzenie* nawet wtedy, gdy zadanie zostaje zakończone pomyślnie na wszystkich urządzeniach z systemem Windows.

Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* jest także wymagane dla tego schematu, ponieważ to zadanie jest używane do pobrania baz danych i modułów Kaspersky dla Kaspersky Security Center.

Ręcznie poprzez folder lokalny, folder współdzielony lub serwer FTP

Jeśli urządzenia klienckie nie mają połączenia z Serwerem administracyjnym, możesz użyć folderu lokalnego lub zasobu współdzielonego jako źródła dla aktualizacji baz danych, modułów i aplikacji Kaspersky. W tym schemacie możesz skopiować wymagane aktualizacje z repozytorium Serwera administracyjnego na dysk wymienny, a następnie skopiować aktualizacje do folderu lokalnego lub zasobu współdzielonego, określonego jako źródło uaktualnień w ustawieniach Kaspersky Endpoint Security (patrz rysunek poniżej).



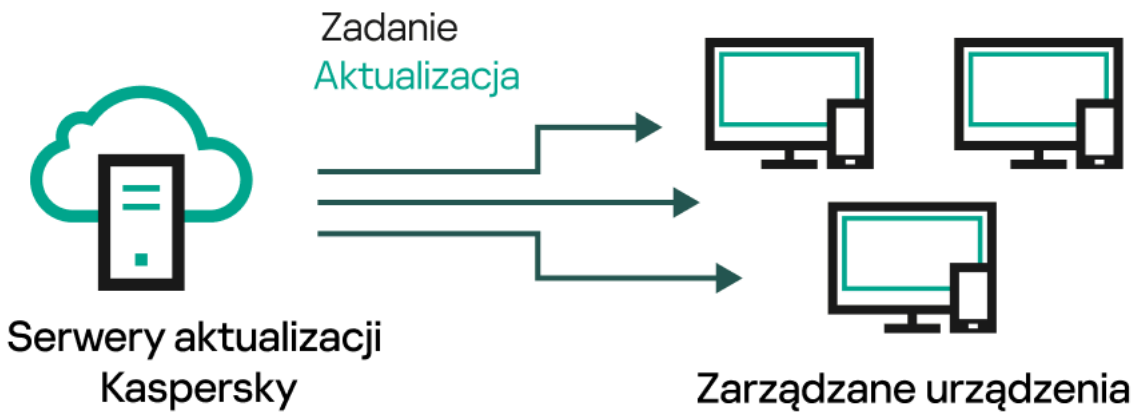
Aktualizowanie poprzez folder lokalny, folder współdzielony lub serwer FTP

Aby uzyskać więcej informacji na temat źródeł aktualizacji w Kaspersky Endpoint Security, zobacz następujące Pomoce:

- Pomoc Kaspersky Endpoint Security for Windows
- Pomoc Kaspersky Endpoint Security for Linux

Bezpośrednio z serwerów aktualizacji Kaspersky do Kaspersky Endpoint Security na zarządzanych urządzeniach

Na zarządzanych urządzeniach możesz skonfigurować Kaspersky Endpoint Security w celu pobierania aktualizacji bezpośrednio z serwerów aktualizacji Kaspersky (patrz rysunek poniżej).



Aktualizowanie aplikacji zabezpieczających bezpośrednio z serwerów aktualizacji Kaspersky

W tym schemacie aplikacja zabezpieczająca nie używa repozytoriów dostarczonych przez Kaspersky Security Center. Aby pobierać uaktualnienia bezpośrednio z serwerów aktualizacji Kaspersky, określ serwery aktualizacji Kaspersky jako źródło uaktualnień w interfejsie aplikacji zabezpieczającej. Aby uzyskać więcej informacji na temat tych ustawień, zobacz następujące Pomoce:

- Pomoc Kaspersky Endpoint Security for Windows
- Pomoc Kaspersky Endpoint Security for Linux

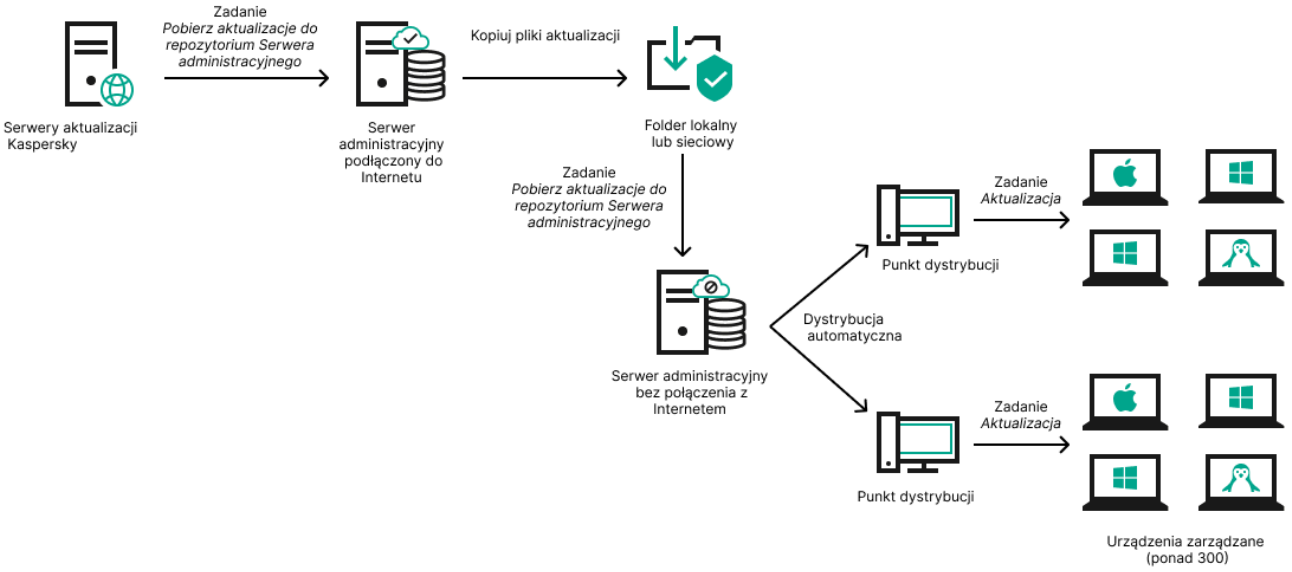
Poprzez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

Jeżeli Serwer administracyjny nie ma połączenia z Internetem, możesz skonfigurować zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, aby pobierać uaktualnienia z folderu lokalnego lub sieciowego. W takim przypadku należy od czasu do czasu kopiować wymagane pliki aktualizacji do określonego folderu. Na przykład możesz skopiować wymagane pliki aktualizacji z jednego z następujących źródeł:

- Serwer administracyjny z połączeniem internetowym (patrz rysunek poniżej)

  Ponieważ serwer administracyjny pobiera tylko aktualizacje wymagane przez aplikacje zabezpieczające, zestawy aplikacji zabezpieczających zarządzanych przez serwery administracyjne — ten, który ma połączenie z Internetem i ten, który go nie ma — muszą być zgodne.

Jeżeli Serwer administracyjny, którego używasz do pobierania uaktualnień, ma wersję 13.2 lub wcześniejszą, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję **Pobierz aktualizacje za pomocą starego schematu**.



Aktualizacja przez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

- Kaspersky Update Utility

  Ponieważ narzędzie to wykorzystuje stary schemat do pobierania uaktualnień, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję **Pobierz aktualizacje za pomocą starego schematu**.

Informacje o używaniu plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky

Jeśli Kaspersky Security Center pobiera uaktualnienia z serwerów aktualizacji Kaspersky, optymalizuje ruch sieciowy przy użyciu plików diff. Możesz także włączyć używanie plików diff przez urządzenia (Serwery administracyjne, punkty dystrybucji i urządzenia klienckie), które pobierają uaktualnienia z innych urządzeń w sieci.

Informacje o funkcji Pobierz pliki diff

Plik diff opisuje różnice między dwoma wersjami pliku bazy danych lub modułu programu. Użycie plików diff oszczędza ruch sieciowy w sieci firmowej, ponieważ pliki diff zajmują mniej miejsca niż całe pliki baz danych i modułów programu. Jeśli funkcja *Pobierz pliki diff* jest włączona na Serwerze administracyjnym lub w punkcie dystrybucji, pliki diff zostają zapisane na tym Serwerze administracyjnym lub w tym punkcie dystrybucji. W wyniku tego działania, urządzenia, które pobierają uaktualnienia z tego Serwera administracyjnego lub punktu dystrybucji, mogą używać zapisanych plików diff do aktualizacji swoich baz danych i modułów programu.

Aby zoptymalizować użycie plików diff, zalecana jest synchronizacja terminarza aktualizacji urządzeń z terminarzem aktualizacji Serwera administracyjnego lub punktu dystrybucji, z którego urządzenia pobierają uaktualnienia. Jednakże ruch sieciowy można oszczędzić nawet wtedy, gdy urządzenia są aktualizowane kilka razy rzadziej niż Serwer administracyjny lub punkt dystrybucji, z którego urządzenia pobierają uaktualnienia.

Funkcja Pobierz pliki diff może zostać włączona tylko na Serwerach administracyjnych i w punktach dystrybucji od wersji 11. Aby zapisać pliki diff na Serwerach administracyjnych i w punktach dystrybucji w wersjach wcześniejszych, zaktualizuj je do wersji 11 lub nowszej.

Funkcja Pobierz pliki diff jest niekompatybilna z trybem offline pobierania uaktualnień. Oznacza to, że Agenty sieciowe, które używają trybu offline pobierania uaktualnień nie pobierają plików diff nawet wtedy, gdy funkcja Pobierz pliki diff jest włączona na Serwerze administracyjnym lub w punkcie dystrybucji, który dostarcza uaktualnienia do tych Agentów sieciowych.

Punkty dystrybucji nie używają multiemisji IP do automatycznego rozsyłania plików diff.

Włączanie funkcji Pobierz pliki diff

Wymagania wstępne

Wymagania wstępne scenariusza są następujące:

- Serwery administracyjne i punkty dystrybucji zostają zaktualizowane do wersji 11 lub nowszej.
- Tryb offline pobierania uaktualnień jest wyłączony w ustawieniach zasady Agenta sieciowego.

Etapy

1. **Włączanie funkcji na Serwerze administracyjnym**

   Włącz funkcję w ustawieniach zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego.

2. **Włączanie funkcji dla punktu dystrybucji**

   Włącz funkcję dla punktu dystrybucji, który pobiera uaktualnienia przy użyciu zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji.

   Następnie włącz funkcję dla punktu dystrybucji, który pobiera uaktualnienia z Serwera administracyjnego.

   Funkcja jest włączona w ustawieniach zasady Agenta sieciowego i — jeśli punkty dystrybucji są przypisywane ręcznie i jeśli chcesz zastąpić ustawienia zasady — w sekcji **Punkty dystrybucji** właściwości Serwera administracyjnego.

Aby sprawdzić, czy funkcja Pobierz pliki diff została pomyślnie włączona, możesz zmierzyć wewnętrzny ruch sieciowy przed i po wykonaniu scenariusza.

Tworzenie zadania pobierania aktualizacji do repozytorium Serwera administracyjnego

Zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego* jest automatycznie tworzone podczas działania kreatora wstępnej konfiguracji Kaspersky Security Center. Możesz utworzyć tylko jedno zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*. Dlatego też zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego* możesz utworzyć tylko wtedy, gdy takie zadanie zostało usunięte z listy zadań Serwera administracyjnego.

W celu utworzenia zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania w jeden z następujących sposobów:
   - W drzewie konsoli, z menu kontekstowego folderu **Zadania** wybierz **Nowe → Zadanie**.
   - W obszarze roboczym folderu **Zadania** kliknij przycisk **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. W oknie **Wybierz typ zadania** wybierz **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.
4. W oknie **Ustawienia** określ ustawienia zadania w następujący sposób:
   - **Źródła aktualizacji**

     Jako źródła uaktualnień dla Serwera administracyjnego można użyć następujących zasobów:

     - Serwery aktualizacji Kaspersky

       Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji. Domyślnie, Serwer administracyjny komunikuje się z serwerami aktualizacji Kaspersky i pobiera uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny, aby używał protokołu HTTP zamiast HTTPS.

       Ta opcja jest wybrana domyślnie.

     - Główny Serwer administracyjny

       Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.

     - Folder lokalny lub sieciowy

       Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

       Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

- **Inne ustawienia**:

  - **Wymuś aktualizację podrzędnych Serwerów administracyjnych**

    Jeżeli ta opcja jest włączona, Serwer administracyjny uruchomi zadania aktualizacji na podrzędnych Serwerach administracyjnych zaraz po pobraniu nowych aktualizacji. Zadania aktualizacji są uruchamiane przy użyciu źródła aktualizacji skonfigurowanego we właściwościach zadania na podrzędnych Serwerach administracyjnych.

    Jeśli ta opcja jest wyłączona, zadania aktualizacji na podrzędnych Serwerach administracyjnych będą uruchamiane zgodnie ze swoimi terminarzami.

    Domyślnie opcja ta jest wyłączona.

  - **Kopiuj pobrane aktualizacje do dodatkowych folderów**

    Po otrzymaniu przez Serwer administracyjny uaktualnień skopiuje on je do określonych folderów. Użyj tej opcji, jeśli chcesz ręcznie zarządzać dystrybucją uaktualnień w sieci.

    Na przykład, chcesz użyć tej opcji w następującej sytuacji: sieć Twojej organizacji zawiera kilka niezależnych podsieci, a urządzenia z każdej podsieci nie mają dostępu do innych podsieci. Jednakże urządzenia we wszystkich podsieciach mają dostęp do wspólnego udziału sieciowego. W tym przypadku skonfiguruj Serwer administracyjny w jednej z podsieci tak, aby pobierał uaktualnienia z serwerów aktualizacji Kaspersky, włącz tę opcję, a następnie określ ten udział sieciowy. W zadaniach pobierania uaktualnień do repozytorium dla innych Serwerów administracyjnych określ ten sam udział sieciowy jako źródło uaktualnień.

    Jeżeli zdecydujesz się na skopiowanie pobranych aktualizacji do folderu lokalnego, musisz wskazać folder na urządzeniu, na którym jest zainstalowany Serwer administracyjny. Ścieżka do folderu zależy od systemu operacyjnego urządzenia. Ponieważ folder lokalny znajduje się na Serwerze administracyjnym opartym na systemie Linux, należy określić ścieżkę POSIX, na przykład: /path/to/dir.

    Wybierając folder sieciowy znajdujący się na Serwerze administracyjnym opartym na systemie Linux, należy wcześniej zapewnić dostęp do folderu sieciowego z urządzenia z zainstalowanym Serwerem administracyjnym, montując folder. Dostęp do folderu odbywa się za pomocą protokołu SMB.

    Domyślnie opcja ta jest wyłączona.

    - **Nie wymuszaj aktualizacji urządzeń i podrzędnych Serwerów administracyjnych przed zakończeniem kopiowania**

      Zadania pobierania aktualizacji na urządzenia klienckie i podrzędne Serwery administracyjne zostaną uruchomione dopiero po skopiowaniu aktualizacji z głównego folderu aktualizacji do dodatkowych folderów aktualizacji.

      Ta opcja musi być włączona, jeśli urządzenia klienckie i podrzędne Serwery administracyjne pobierają aktualizacje z dodatkowych folderów sieciowych.

      Domyślnie opcja ta jest wyłączona.

  - **Pobierz aktualizacje za pomocą starego schematu**

    Począwszy od wersji 14, Kaspersky Security Center pobiera aktualizacje baz danych i modułów oprogramowania przy użyciu nowego schematu. Aby aplikacja pobierała aktualizacje przy użyciu nowego schematu, źródło aktualizacji musi zawierać pliki aktualizacji z metadanymi zgodnymi z nowym schematem. Jeśli źródło aktualizacji zawiera pliki aktualizacji z metadanymi zgodnymi tylko ze starym schematem, włącz opcję **Pobierz aktualizacje za pomocą starego schematu**. W przeciwnym razie zadanie pobierania aktualizacji zakończy się niepowodzeniem.

Na przykład musisz włączyć tę opcję, gdy folder lokalny lub sieciowy jest określony jako źródło aktualizacji, a pliki aktualizacji w tym folderze zostały pobrane przez jedną z następujących aplikacji:

- Kaspersky Update Utility

  To narzędzie pobiera aktualizacje przy użyciu starego schematu.

- Kaspersky Security Center 13.2 lub wcześniejsza wersja

  Na przykład Twój serwer administracyjny 1 nie ma połączenia z Internetem. W takim przypadku możesz pobrać aktualizacje za pomocą serwera administracyjnego 2, który ma połączenie z Internetem, a następnie umieścić je w folderze lokalnym lub sieciowym, aby użyć go jako źródła uaktualnień dla serwera administracyjnego 1. Jeżeli serwer administracyjny 2 ma wersję 13.2 lub wcześniejszą, włącz opcję **Pobierz aktualizacje za pomocą starego schematu** w zadaniu dla serwera administracyjnego 1.

Domyślnie opcja ta jest wyłączona.

5. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- **Zaplanowane uruchomienie:**

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - **Co N godzin**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

  - **Co N dni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

    Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Co N tygodni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

    Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

  - **Co N minut**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

    Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

  - **Codziennie (czas letni nie jest obsługiwany)**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

    Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

    Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

- Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
- Kliknij ikonę sortowania, aby posortować zadania według nazwy.

  Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
- Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

6. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

7. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

   Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu pracy kreatora, zadanie **Pobierz aktualizacje do repozytorium serwera administracyjnego** pojawi się na liście zadań Serwera administracyjnego w obszarze roboczym.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Podczas wykonywania zadania *Pobierz aktualizacje do repozytorium serwera administracyjnego* Serwer administracyjny pobiera uaktualnienia baz danych i modułów programu ze źródła uaktualnień i przechowuje je w folderze współdzielonym Serwera administracyjnym. Jeśli tworzysz to zadanie dla grupy administracyjnej, zostanie ono zastosowane tylko do Agentów sieciowych umieszczonych w określonej grupie administracyjnej.

Uaktualnienia są rozsyłane do urządzeń klienckich i podrzędnych Serwerów administracyjnych z folderu współdzielonego Serwera administracyjnego.

Tworzenie zadania Pobierz uaktualnienia do repozytoriów punktów dystrybucji

Urządzenia punktów dystrybucji działające pod kontrolą systemu operacyjnego macOS nie mogą pobierać uaktualnień z serwerów aktualizacji Kaspersky.

W przypadku, gdy jedno lub więcej urządzeń działających pod kontrolą systemu operacyjnego macOS znajduje się w obszarze zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, zadanie zostaje zakończone ze stanem *Niepowodzenie* nawet wtedy, gdy zadanie zostaje zakończone pomyślnie na wszystkich urządzeniach z systemem Windows.

Możesz utworzyć zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji* dla grupy administracyjnej. To zadanie będzie uruchamiane dla punktów dystrybucji znajdujących się w określonej grupie administracyjnej.

Możesz użyć tego zadania, na przykład, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktem(ami) dystrybucji jest droższy niż ruch sieciowy pomiędzy punktem(ami) dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu. Jeśli punkt dystrybucji łączy się z Internetem za pośrednictwem serwera proxy, należy określić odpowiednie ustawienia w zasadach Agenta sieciowego.

W celu utworzenia zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji dla wybranej grupy administracyjnej:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. W obszarze roboczym tego folderu kliknij przycisk **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. W oknie **Wybierz typ zadania** wybierz węzeł Serwer administracyjny **Kaspersky Security Center**, rozwiń folder **Zaawansowane**, a następnie wybierz zadanie **Pobierz aktualizacje do repozytoriów punktów dystrybucji**.
4. W oknie **Ustawienia** określ ustawienia zadania w następujący sposób:

   - **Źródła aktualizacji**

     Jako źródła uaktualnień dla punktu dystrybucji można użyć następujących zasobów:

     - Serwery aktualizacji Kaspersky

Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji.

Opcja ta jest wybrana domyślnie.

- Folder lokalny lub sieciowy

  Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

  > Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

- **Folder do przechowywania aktualizacji**

  Ścieżka do określonego folderu na potrzeby przechowywania zapisanych aktualizacji. Możesz skopiować ścieżkę do określonego folderu do schowka. Nie możesz zmienić ścieżki do określonego folderu w przypadku zadania grupowego.

- **Pobierz aktualizacje za pomocą starego schematu**

  Począwszy od wersji 14, Kaspersky Security Center pobiera aktualizacje baz danych i modułów oprogramowania przy użyciu nowego schematu. Aby aplikacja pobierała aktualizacje przy użyciu nowego schematu, źródło aktualizacji musi zawierać pliki aktualizacji z metadanymi zgodnymi z nowym schematem. Jeśli źródło aktualizacji zawiera pliki aktualizacji z metadanymi zgodnymi tylko ze starym schematem, włącz opcję **Pobierz aktualizacje za pomocą starego schematu**. W przeciwnym razie zadanie pobierania aktualizacji zakończy się niepowodzeniem.

  Na przykład musisz włączyć tę opcję, gdy folder lokalny lub sieciowy jest określony jako źródło aktualizacji, a pliki aktualizacji w tym folderze zostały pobrane przez jedną z następujących aplikacji:

  - Kaspersky Update Utility

    To narzędzie pobiera aktualizacje przy użyciu starego schematu.

  - Kaspersky Security Center 13.2 lub wcześniejsza wersja

    Na przykład punkt dystrybucji jest skonfigurowany do pobierania aktualizacji z folderu lokalnego lub sieciowego. W takim przypadku aktualizacje można pobrać za pomocą serwera administracyjnego z połączeniem internetowym, a następnie umieścić je w folderze lokalnym w punkcie dystrybucji. Jeśli serwer administracyjny ma wersję 13.2 lub wcześniejszą, włącz opcję **Pobierz aktualizacje za pomocą starego schematu** w zadaniu *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

  Domyślnie opcja ta jest wyłączona.

5. W oknie **Wybierz Grupę administracyjną** kliknij **Przeglądaj** i wybierz grupę administracyjną, do której stosowane jest zadanie.

6. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

   - **Zaplanowane uruchomienie:**

     Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

     - **Co N godzin**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

       Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

     - **Co N dni**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

       Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

     - **Co N tygodni**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

       Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

     - **Co N minut**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

       Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

     - **Codziennie (czas letni nie jest obsługiwany)**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

       Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

       Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

     - **Co tydzień**

       Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

     - **Według dni tygodnia**

       Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

       Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

     - **Co miesiąc**

       Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

       W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

7. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

8. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

   Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu pracy kreatora, zadanie **Pobierz aktualizacje do repozytoriów punktów dystrybucji** pojawi się na liście zadań Agenta sieciowego w docelowej grupie administracyjnej i w obszarze roboczym **Zadania** konsoli.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Po wykonaniu zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji*, aktualizacje baz danych i modułów aplikacji zostaną pobrane ze źródła uaktualnień i będą przechowywane w folderze współdzielonym. Pobrane uaktualnienia zostaną użyte tylko przez punkty dystrybucji, które znajdują się w określonej grupie administracyjnej i dla których nie ustawiono zadania pobierania aktualizacji.

W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Punkty dystrybucji**. We właściwościach każdego punktu dystrybucji, w sekcji **Źródło uaktualnień** możesz określić źródło uaktualnień (**Pobierz z Serwera administracyjnego** lub **Użyj zadania do wymuszonego pobierania uaktualnień**). Domyślnie, opcja **Pobierz z Serwera administracyjnego** jest wybrana dla punktu dystrybucji wskazanego ręcznie lub automatycznie. Te punkty dystrybucji będą używać wyników wykonania zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji*.

Właściwości każdego punktu dystrybucji określają folder sieciowy, który został utworzony osobno dla tego punktu dystrybucji. Nazwy folderów mogą być różne dla innych punktów dystrybucji. Dlatego też nie jest zalecane zmienianie nazwy folderu sieciowego we właściwościach zadania, jeśli zadanie jest tworzone dla grupy urządzeń.

Jeśli tworzysz zadanie lokalne dla urządzenia, możesz zmienić folder sieciowy z aktualizacjami we właściwościach zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji*.

Konfigurowanie zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego

W celu skonfigurowania zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego:

1. W obszarze roboczym folderu **Zadania**, z listy zadań wybierz **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.

2. Otwórz okno właściwości zadania w jeden z następujących sposobów:

   - Wybierając **Właściwości** w menu kontekstowym zadania.

   - Klikając odnośnik **Konfiguruj zadanie** w oknie z informacjami dla wybranego zadania.

   Zostanie otwarte okno właściwości zadania *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*. W tym oknie możesz skonfigurować sposób pobierania uaktualnień do repozytorium Serwera administracyjnego.

Sprawdzanie pobranych uaktualnień

Przed zainstalowaniem aktualizacji na zarządzanych urządzeniach, w pierwszej kolejności możesz sprawdzić aktualizacje pod kątem łatwości obsługi i błędów poprzez zadanie *Weryfikacja uaktualnień*. Zadanie *Weryfikacja uaktualnień* jest wykonywane automatycznie jako część zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Serwer administracyjny pobierze uaktualnienia ze źródła, zapisze je w repozytorium tymczasowym i uruchomi *Weryfikacja uaktualnień*. Jeżeli zadanie zakończy się powodzeniem, uaktualnienia zostaną skopiowane z repozytorium tymczasowego do folderu współdzielonego na serwerze administracyjnym (<Folder instalacyjny Kaspersky Security Center>\Share\Updates). Zostaną one rozesłane do wszystkich urządzeń klienckich, dla których Serwer administracyjny jest źródłem uaktualnień.

Jeżeli zadanie *Weryfikacja uaktualnień* wykaże niepoprawność uaktualnień znajdujących się w repozytorium tymczasowym lub podczas wykonywania tego zadania wystąpi błąd, *Weryfikacja uaktualnień* nie zostaną skopiowane do folderu współdzielonego. Serwer administracyjny zachowa poprzedni zestaw uaktualnień. Zaplanowane zadania wykonywane zgodnie z opcją terminarza **Po pobraniu nowych uaktualnień do repozytorium** również nie zostaną uruchomione. Te działania są wykonywane podczas następnego uruchomienia zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, jeśli skanowanie nowych uaktualnień przebiegło bez problemów.

Zestaw uaktualnień jest uważany za nieprawidłowy, jeżeli przynajmniej na jednym urządzeniu testującym jest spełniony jeden z następujących warunków:

- Wystąpił błąd zadania aktualizacji.
- Stan ochrony w czasie rzeczywistym aplikacji zabezpieczającej zmienił się po zastosowaniu uaktualnień.
- W trakcie wykonywania zadania skanowania na żądanie wykryto zainfekowany obiekt.
- Wystąpił błąd w funkcjonowaniu aplikacji Kaspersky.

Jeśli żaden z powyższych warunków nie wystąpił na żadnym urządzeniu testującym, zestaw uaktualnień jest uważany za poprawny, a zadanie *Weryfikacja uaktualnień* uważa się za zakończone pomyślnie.

Zanim zaczniesz tworzyć zadanie *Weryfikacja uaktualnień*, zrealizuj wymagania wstępne:

1. Utwórz grupę administracyjną z kilkoma urządzeniami testowymi. Ta grupa będzie potrzebna do weryfikacji uaktualnień.

   Zaleca się korzystanie z urządzeń z najbardziej niezawodną ochroną i najpowszechniejszą konfiguracją aplikacji w całej sieci. Takie podejście zwiększa jakość i prawdopodobieństwo wykrycia wirusa podczas skanowania oraz minimalizuje ryzyko fałszywych alarmów. Jeśli na urządzeniach testujących zostaną wykryte wirusy, zadanie *weryfikacji uaktualnień* zakończy się niepowodzeniem.

2. Utwórz zadania *Aktualizuj* i *Skanowanie w poszukiwaniu złośliwego oprogramowania* do aplikacji obsługiwanej przez Kaspersky Security Center, na przykład Kaspersky Endpoint Security for Windows lub Kaspersky Security for Windows Server. Podczas tworzenia zadań *Aktualizuj* i *Skanowanie w poszukiwaniu złośliwego oprogramowania* określ grupę administracyjną z urządzeniami testowymi.

   Zadanie *Weryfikacja uaktualnień* uruchamia kolejno zadania *Aktualizuj* i *Skanowanie w poszukiwaniu złośliwego oprogramowania* na urządzeniach testowych, aby sprawdzić, czy wszystkie aktualizacje są prawidłowe. Ponadto podczas tworzenia zadania *Weryfikacja uaktualnień* musisz określić zadania *Aktualizuj* i *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

3. Utwórz zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

W celu skonfigurowania Kaspersky Security Center do sprawdzania pobranych uaktualnień przed rozesłaniem ich na urządzenia klienckie:

1. W obszarze roboczym folderu **Zadania**, z listy zadań wybierz zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.
2. Otwórz okno właściwości zadania w jeden z następujących sposobów:
   - Wybierając **Właściwości** w menu kontekstowym zadania.
   - Klikając odnośnik **Konfiguruj zadanie** w oknie z informacjami dla wybranego zadania.
3. Jeśli zadanie weryfikacji *Weryfikacja uaktualnień* istnieje, kliknij przycisk **Przeglądaj**. W oknie, które zostanie otwarte, wybierz zadanie *Weryfikacja uaktualnień* w grupie administracyjnej z urządzeniami testowymi.
4. Jeśli wcześniej nie utworzono zadania *Weryfikacja uaktualnień*, kliknij przycisk **Utwórz**.

   Zostanie uruchomiony Kreator zadania *Weryfikacja uaktualnień*. Postępuj zgodnie z instrukcjami kreatora.
5. Kliknij **OK**, aby zamknąć okno właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*

Automatyczna weryfikacja aktualizacji zostanie włączona. Teraz możesz uruchomić zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnegoi*.

Konfigurowanie zasad testowych i zadań pomocniczych

Podczas tworzenia zadania *weryfikacji uaktualnień* serwer administracyjny generuje zasady testowe, pomocnicze grupowe zadania aktualizacji i zadania skanowania na żądanie.

Pomocnicze grupowe zadania aktualizacji i zadania skanowania na żądanie zajmują trochę czasu. Zadania te są wykonywane podczas wykonywania zadania *weryfikacji uaktualnień*. Zadanie *weryfikacji* uaktualnień jest wykonywane podczas wykonywania zadania *pobierania* aktualizacji do repozytorium. Czas trwania zadania *Pobierz uaktualnienia do repozytorium* obejmuje pomocnicze grupowe zadania aktualizacji i skanowania na żądanie.

Możesz zmodyfikować ustawienia zasad testowych i zadań pomocniczych.

W celu zmodyfikowania ustawień zasady testowej lub zadania pomocniczego:

1. Z drzewa konsoli wybierz grupę, dla której tworzone jest zadanie *weryfikacji uaktualnień*.
2. W obszarze roboczym grupy wybierz jedną z następujących zakładek:
   - **Zasady**, jeżeli chcesz zmodyfikować ustawienia zasady testowej.
   - **Zadania**, jeżeli chcesz zmienić ustawienia zadania pomocniczego.
3. Na zakładce obszaru roboczego wybierz zasadę lub zadanie, którego ustawienia chcesz zmodyfikować.
4. Otwórz okno właściwości zasady (zadania) w jeden z następujących sposobów:
   - Wybierając **Właściwości** z menu kontekstowego zasady (zadania).
   - Klikając odnośnik **Konfiguruj zasadę** (**Konfiguruj zadanie**) w oknie z informacjami dla wybranej zasady (zadania).

W celu sprawdzenia poprawności uaktualnień, na modyfikację ustawień zasad testowych i zadań pomocniczych powinny zostać nałożone następujące ograniczenia:

- W ustawieniach zadania pomocniczego:
  - Zapisz wszystkie zadania z priorytetem **Zdarzenie krytyczne** i **Błąd funkcjonalny** na Serwerze administracyjnym. Przy użyciu tych typów zdarzeń Serwer administracyjny analizuje działanie aplikacji.
  - Użyj Serwera administracyjnego jako źródła uaktualnień.
  - Określ typ terminarza zadania: **Ręcznie**.

- W ustawieniach zasad testowych:
  - Wyłącz technologie przyspieszające skanowanie iChecker i iSwift (**Podstawowa ochrona przed zagrożeniami → Ochrona plików → Ustawienia → Dodatkowe → Technologie skanowania**).
  - Wybierz działania na zainfekowanych obiektach: **Wylecz; usuń, jeśli leczenie nie powiedzie się** / **Wylecz; zablokuj, jeśli leczenie nie powiedzie się** / **Zablokuj** (**Podstawowa ochrona przed zagrożeniami → Ochrona plików → Akcja po wykryciu zagrożenia**).
- W ustawieniach zasad testowych i zadań pomocniczych:

  Jeżeli po zainstalowaniu uaktualnień modułów oprogramowania konieczne jest ponowne uruchomienie urządzenia, należy to zrobić natychmiast. Jeżeli urządzenie nie zostanie uruchomione ponownie, niemożliwe będzie przetestowanie tego typu uaktualnień. Dla niektórych aplikacji instalacja uaktualnień wymagająca ponownego uruchomienia komputera może zostać zablokowana lub skonfigurowana tak, aby najpierw pytać użytkownika o potwierdzenie. Ograniczenia te powinny zostać wyłączone w ustawieniach zasad testowych i zadań pomocniczych.

Wyświetlanie pobranych uaktualnień

W celu wyświetlenia listy pobranych uaktualnień:

W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder **Aktualizacje baz danych i modułów oprogramowania Kaspersky**.

Obszar roboczy folderu **Aktualizacje baz danych i modułów oprogramowania Kaspersky** wyświetla listę aktualizacji zapisanych na Serwerze administracyjnym.

Automatyczna instalacja uaktualnień dla Kaspersky Endpoint Security na urządzeniach

Możesz skonfigurować automatyczne aktualizowanie baz danych i modułów aplikacji Kaspersky Endpoint Security na urządzeniach klienckich.

W celu skonfigurowania pobierania i automatycznej instalacji uaktualnień dla Kaspersky Endpoint Security na urządzeniach:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Utwórz zadanie **Aktualizacja** w jeden z następujących sposobów:
   - Wybierając **Nowe → Zadanie** w menu kontekstowym folderu **Zadania** w drzewie konsoli.
   - Kliknij przycisk **Nowe zadanie** dostępny w obszarze roboczym folderu **Zadania**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. W oknie **Wybierz typ zadania** kreatora, jako typ zadania wybierz **Kaspersky Endpoint Security**, a następnie, jako podtyp zadania wskaż **Aktualizacja**.

4. Wykonaj pozostałe instrukcje kreatora.

   Po zakończeniu pracy kreatora zostanie utworzone zadanie aktualizacji dla Kaspersky Endpoint Security. Nowo utworzone zadanie będzie wyświetlane na liście zadań, w obszarze roboczym folderu **Zadania**.

5. W obszarze roboczym folderu **Zadania** wybierz utworzone zadanie aktualizacji.

6. Z menu kontekstowego zadania wybierz **Właściwości**.

7. W otwartym oknie właściwości zadania, w panelu **Sekcje** wybierz **Opcje**.

   W sekcji **Opcje** możesz zdefiniować ustawienia zadania aktualizacji w trybie lokalnym lub mobilnym:

   - **Ustawienia aktualizacji dla trybu lokalnego**: Połączenie jest nawiązywane między urządzeniem a Serwerem administracyjnym.

   - **Ustawienia aktualizacji dla trybu mobilnego**: Połączenie pomiędzy Kaspersky Security Center a urządzeniem nie jest nawiązywane (na przykład, jeśli urządzenie nie jest podłączone do internetu).

8. Kliknij przycisk **Ustawienia**, aby wybrać źródło uaktualnień.

9. Wybierz opcję **Pobierz uaktualnienia modułów aplikacji**, aby pobrać i zainstalować uaktualnienia modułów aplikacji wraz z bazami danych aplikacji.

   Jeśli pole jest zaznaczone, Kaspersky Endpoint Security powiadamia użytkownika o dostępnych uaktualnieniach modułów aplikacji i włącza uaktualnienia modułów aplikacji do pakietu aktualizacyjnego podczas wykonywania zadania aktualizacji. Skonfiguruj użycie modułów aktualizacji:

   - **Zainstaluj krytyczne i zatwierdzone aktualizacje**. Jeśli dla modułów aplikacji dostępne są jakiekolwiek aktualizacje, Kaspersky Endpoint Security automatycznie zainstaluje te ze stanem *Krytyczne*. Pozostałe aktualizacje zostaną zainstalowane, jak je zatwierdzisz.

   - **Zainstaluj tylko zatwierdzone aktualizacje**. Jeśli dla modułów aplikacji dostępne są jakiekolwiek aktualizacje, Kaspersky Endpoint Security zainstaluje je po zatwierdzeniu ich instalacji. Zostaną one zainstalowane lokalnie, poprzez interfejs aplikacji lub poprzez Kaspersky Security Center.

   Jeśli do zainstalowania uaktualnień modułów aplikacji wymagane jest przejrzenie i zaakceptowanie warunków Umowy licencyjnej i Polityki prywatności, aplikacja zainstaluje uaktualnienia po zaakceptowaniu warunków Umowy licencyjnej i Polityki prywatności przez użytkownika.

10. Wybierz opcję **Kopiuj uaktualnienia do folderu**, aby aplikacja zapisywała pobrane uaktualnienia w folderze, a następnie kliknij przycisk **Przeglądaj**, aby określić folder.

11. Kliknij **OK**.

Podczas wykonywania zadania **Aktualizacja** aplikacja wysyła żądanie do serwerów aktualizacji Kaspersky.

Niektóre aktualizacje wymagają zainstalowania najnowszych wersji wtyczek zarządzających.

Tryb offline pobierania aktualizacji

Agent sieciowy na zarządzanych urządzeniach może czasami nie nawiązać połączenia z Serwerem administracyjnym w celu pobrania uaktualnień. Na przykład Agent sieciowy mógł zostać zainstalowany na laptopie, który czasami nie ma połączenia z internetem oraz nie ma dostępu do sieci lokalnej. Co więcej, administrator mógł ograniczyć czas połączenia urządzeń z siecią. W takich przypadkach, urządzenia z zainstalowanym Agentem sieciowym nie mogą pobierać uaktualnień z Serwera administracyjnego zgodnie z istniejącym terminarzem. Jeśli skonfigurowałeś aktualizację zarządzanych aplikacji (na przykład Kaspersky Endpoint Security) przy użyciu Agenta sieciowego, każda aktualizacja będzie wymagała połączenia z Serwerem administracyjnym. Jeśli połączenie między Agentem sieciowym a Serwerem administracyjnym nie zostanie nawiązane, aktualizacja nie będzie mogła zostać przeprowadzona. Możesz skonfigurować połączenie między Agentem sieciowym a Serwerem administracyjnym tak, aby Agent sieciowy łączył się z Serwerem administracyjnych w określonych przedziałach czasu. W najgorszym razie, jeśli określone odstępy między połączeniami pokrywają się z przedziałami czasu, gdy połączenie jest dostępne, bazy danych nigdy nie zostaną zaktualizowane. Dodatkowo, gdy kilka zarządzanych aplikacji jednocześnie spróbuje uzyskać dostęp do Serwera administracyjnego w celu pobrania uaktualnień, mogą pojawić się problemy. W tej sytuacji, Serwer administracyjny może przestać odpowiadać na żądania (podobnie, jak w przypadku ataku DDoS).

Aby uniknąć wyżej opisanych problemów, w Kaspersky Security Center zaimplementowano tryb offline do pobierania uaktualnień i modułów zarządzanych aplikacji. Ten tryb oferuje mechanizm dystrybucji uaktualnień, niezależnie od tymczasowych problemów spowodowanych przez brak dostępności kanałów komunikacyjnych Serwera administracyjnego. Ten model zmniejsza także obciążenie na Serwerze administracyjnym.

Działanie trybu offline pobierania uaktualnień

Jeśli Serwer administracyjny pobierze uaktualnienia, powiadomi Agenta sieciowego (na urządzeniach, na których jest zainstalowany) o uaktualnieniach, które będą wymagane dla zarządzanych aplikacji. Jeśli Agent sieciowy otrzyma informacje o tych uaktualnieniach, pobierze odpowiednie pliki z Serwera administracyjnego z wyprzedzeniem. Przy pierwszym nawiązaniu połączenia z Agentem sieciowym, Serwer administracyjny inicjuje pobranie aktualizacji. Jeśli Agent sieciowy pobierze wszystkie uaktualnienia na urządzenie klienckie, staną się one dostępne dla aplikacji na tym urządzeniu.

Jeśli zarządzana aplikacja na urządzeniu klienckim spróbuje uzyskać dostęp do Agenta sieciowego w celu uzyskania uaktualnień, Agent sieciowy sprawdzi, czy posiada wszystkie wymagane uaktualnienia. Jeśli uaktualnienia zostały pobrane z Serwera administracyjnego nie więcej niż 25 godzin przed zażądaniem ich przez zarządzaną aplikację, Agent sieciowy nie nawiąże połączenia z Serwerem administracyjnym, ale dostarczy zarządzanej aplikacji uaktualnienia z lokalnej pamięci podręcznej. Połączenie z Serwerem administracyjnym może nie zostać nawiązane, gdy Agent sieciowy dostarcza uaktualnienia aplikacji na urządzeniach klienckich, ale połączenie nie jest wymagane w celu przeprowadzenia aktualizacji.

Aby równomiernie rozłożyć obciążenie Serwera administracyjnego, Agent sieciowy na urządzeniu nawiązuje połączenie z Serwerem administracyjnym i pobiera uaktualnienia w kolejności losowej w obrębie przedziału czasu określonego przez Serwer administracyjny. Długość tego przedziału czasu zależy od liczby urządzeń z zainstalowanym Agentem sieciowym, który pobiera uaktualnienia, oraz od rozmiaru tych uaktualnień. Aby zmniejszyć obciążenie na Serwerze administracyjnym, jako punkty dystrybucji można użyć Agenty sieciowe.

Jeśli tryb offline pobierania uaktualnień jest wyłączony, uaktualnienia są rozsyłane zgodnie z terminarzem zadania pobierania uaktualnień.

Domyślnie włączony jest tryb offline pobierania uaktualnień.

Tryb offline do pobierania uaktualnień jest używany tylko na zarządzanych urządzeniach, na których dla zadania pobierania uaktualnień przez zarządzane aplikacje jako typ terminarza wybrano **Po pobraniu nowych uaktualnień do repozytorium**. Dla innych zarządzanych urządzeń wykorzystywany jest standardowy schemat pobierania uaktualnień z Serwera administracyjnego w czasie rzeczywistym.

Zalecane jest wyłączenie trybu offline do pobierania uaktualnień przy użyciu ustawień zasad Agenta sieciowego odpowiednich grup administracyjnych w następujących przypadkach: jeśli dla zarządzanych aplikacji pobieranie uaktualnień nie zostało ustawione z Serwera administracyjnego, ale z serwerów Kaspersky lub z folderu sieciowego, a dla zadania pobierania uaktualnień wybrano typ terminarza **Po pobraniu nowych uaktualnień do repozytorium**.

Włączanie i wyłączanie trybu offline pobierania uaktualnień

Nie jest zalecane wyłączanie trybu offline pobierania uaktualnień. Wyłączenie tego trybu może spowodować błędy w dostarczeniu uaktualnień na urządzenia. W niektórych przypadkach specjalista z pomocy technicznej Kaspersky może zalecić odznaczenie pola **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem**. Następnie upewnij się, że zadanie pobierania uaktualnień dla aplikacji firmy Kaspersky zostało skonfigurowane.

W celu włączenia lub wyłączenia trybu offline pobierania uaktualnień dla grupy administracyjnej:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której chcesz włączyć tryb offline pobierania uaktualnień.
2. W obszarze roboczym grupy otwórz zakładkę **Zasady**.
3. Na zakładce **Zasady** wybierz zasadę Agenta sieciowego.
4. Z otwartego menu kontekstowego zasady wybierz **Właściwości**.

   Otwórz okno właściwości zasady Agenta sieciowego.
5. W oknie właściwości zasady wybierz sekcję **Zarządzaj poprawkami i aktualizacjami**.
6. Zaznacz lub odznacz pole **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)**, aby włączyć lub wyłączyć model offline pobierania uaktualnień.

   Domyślnie włączony jest tryb offline pobierania uaktualnień.

Tryb offline pobierania uaktualnień zostanie włączony lub wyłączony.

Automatyczne aktualizowanie i instalowanie poprawek dla komponentów Kaspersky Security Center

Domyślnie wszelkie pobrane uaktualnienia i poprawki są instalowane automatycznie dla następujących komponentów aplikacji:

- Agent sieciowy dla systemu Windows
- Konsola administracyjna
- Serwer iOS MDM

Automatyczne aktualizowanie i instalowanie poprawek dla komponentów Kaspersky Security Center jest dostępne tylko dla urządzeń działających pod kontrolą systemu Windows. Możesz wyłączyć automatyczne aktualizowanie i instalowanie poprawek dla tych komponentów. W tym przypadku wszelkie pobrane uaktualnienia i poprawki zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzono*. Uaktualnienia i łaty ze stanem *Nie zdefiniowano* nie zostaną zainstalowane.

Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center

Automatyczna instalacja uaktualnień i łat dla komponentów Kaspersky Security Center jest włączona domyślnie podczas instalacji Agenta sieciowego na urządzeniu. Możesz to wyłączyć podczas instalacji Agenta sieciowego lub wyłączyć później przy użyciu zasady.

W celu wyłączenia automatycznej aktualizacji i instalacji poprawek dla komponentów Kaspersky Security Center podczas lokalnej instalacji Agenta sieciowego na urządzeniu:

1. Uruchom lokalną instalację Agenta sieciowego na urządzeniu.
2. W kroku **Ustawienia zaawansowane** odznacz pole **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**.
3. Postępuj zgodnie z instrukcjami kreatora.

Na urządzeniu zostanie zainstalowany Agent sieciowy z wyłączoną automatyczną aktualizacją i instalacją łat dla komponentów Kaspersky Security Center. Automatyczne aktualizowanie i instalowanie poprawek można włączyć w późniejszym czasie, korzystając z zasady.

W celu wyłączenia automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center podczas instalacji Agenta sieciowego na urządzeniu przy użyciu pakietu instalacyjnego:

1. Z drzewa konsoli wybierz folder **Zdalna instalacja** → **Pakiety instalacyjne**.
2. W menu kontekstowym pakietu **Agent sieciowy Kaspersky Security Center <numer wersji>** wybierz **Właściwości**.
3. We właściwościach pakietu instalacyjnego, w sekcji **Ustawienia** odznacz pole **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**.

Z tego pakietu zostanie zainstalowany Agent sieciowy z wyłączoną automatyczną aktualizacją i instalacją łat dla komponentów Kaspersky Security Center. Automatyczne aktualizowanie i instalowanie poprawek można włączyć w późniejszym czasie, korzystając z zasady.

Jeśli to pole zostało zaznaczone (lub odznaczone) podczas instalacji Agenta sieciowego na urządzeniu, możesz włączyć (lub wyłączyć) automatyczne aktualizowanie przy użyciu zasady Agenta sieciowa.

W celu włączenia lub wyłączenia automatycznego aktualizowania i instalowania poprawek dla składników Kaspersky Security Center przy użyciu zasady Agenta sieciowego:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której chcesz włączyć lub wyłączyć automatyczne aktualizowanie i instalowanie poprawek.
2. W obszarze roboczym grupy otwórz zakładkę **Zasady**.
3. Na zakładce **Zasady** wybierz zasadę Agenta sieciowego.
4. Z otwartego menu kontekstowego zasady wybierz **Właściwości**.

   Otwórz okno właściwości zasady Agenta sieciowego.
5. W oknie właściwości zasady wybierz sekcję **Zarządzaj poprawkami i aktualizacjami**.
6. Zaznacz lub odznacz pole **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**, aby włączyć lub wyłączyć automatyczne aktualizowanie i instalowanie poprawek.
7. Ustaw blokadę dla tego pola.

Zasada zostanie zastosowana na wybranych urządzeniach, a automatyczne aktualizowanie i instalowanie poprawek dla komponentów Kaspersky Security Center zostanie włączone (lub wyłączone) na tych urządzeniach.

Automatyczne rozsyłanie uaktualnień

Kaspersky Security Center pozwala na automatyczne rozsyłanie i instalację uaktualnień na urządzeniach klienckich i podrzędnych Serwerach administracyjnych.

Automatyczne rozsyłanie uaktualnień do urządzeń klienckich

W celu automatycznego rozesłania uaktualnień wybranych aplikacji do urządzeń klienckich natychmiast po ich pobraniu do repozytorium Serwera administracyjnego:

1. Nawiąż połączenie z Serwerem administracyjnym, który zarządza urządzeniami klienckimi.
2. Utwórz zadanie zdalnej instalacji uaktualnień dla wybranych urządzeń klienckich w jeden z następujących sposobów:
   - Jeśli chcesz rozesłać uaktualnienia do urządzeń klienckich należących do wybranej grupy administracyjnej, utwórz zadanie dla wybranej grupy.
   - Jeżeli chcesz rozesłać uaktualnienia do urządzeń klienckich należących do różnych grup administracyjnych lub nie będących w żadnej grupie administracyjnej, utwórz zadanie dla wskazanych urządzeń.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z jego instrukcjami i wykonaj następujące czynności:

   a. W oknie **Typ zadania**, w węźle żądanej aplikacji wybierz zadanie rozsyłania uaktualnień.

      Nazwa zadania rozsyłania uaktualnień wyświetlana w oknie **Typ zadania** zależy od aplikacji, dla której utworzyłeś to zadanie. Szczegółowe informacje o nazwach zadań aktualizacji dla wybranych aplikacji Kaspersky znajdziesz w odpowiedniej dokumentacji.

   b. W oknie kreatora **Terminarz**, w polu **Zaplanowane uruchomienie** wybierz **Po pobraniu nowych uaktualnień do repozytorium**.

   Nowo utworzone zadanie rozsyłania uaktualnień będzie uruchamiane dla wybranych urządzeń za każdym razem po pobraniu uaktualnień do repozytorium Serwera administracyjnego.

Jeśli zadanie rozsyłania uaktualnień dla wybranej aplikacji zostało utworzone dla wybranych urządzeń, aby automatycznie rozesłać uaktualnienia na urządzenia klienckie, w oknie właściwości zadania, w sekcji **Terminarz** wybierz opcję **Po pobraniu nowych uaktualnień do repozytorium** w polu **Zaplanowane uruchomienie**.

Automatyczne rozsyłanie uaktualnień do podrzędnych Serwerów administracyjnych

W celu rozesłania uaktualnień wybranych aplikacji do podrzędnych Serwerów administracyjnych natychmiast po ich pobraniu do repozytorium nadrzędnego Serwera administracyjnego:

1. W drzewie konsoli, w węźle głównego Serwera administracyjnego wybierz folder **Zadania**.
2. Na liście zadań w obszarze roboczym wybierz zadanie Serwera administracyjnego: Pobierz uaktualnienia do repozytorium Serwera administracyjnego.

3. Otwórz sekcję **Ustawienia** wybranego zadania w jeden z następujących sposobów:

   - Wybierając **Właściwości** w menu kontekstowym zadania.
   - Klikając odnośnik **Modyfikuj ustawienia** w oknie z informacjami dla wybranego zadania.

4. W sekcji **Ustawienia**, dostępnej w oknie właściwości zadania, przejdź do podsekcji **Inne ustawienia** i kliknij odnośnik **Konfiguruj**.

5. W otwartym oknie **Inne ustawienia** zaznacz pole **Wymuś aktualizację podrzędnych Serwerów administracyjnych**.

6. W oknie ustawień zadania pobierania uaktualnień Serwera administracyjnego, na zakładce **Ustawienia** zaznacz pole **Wymuś aktualizację podrzędnych Serwerów administracyjnych**.

Po pobraniu aktualizacji przez główny Serwer administracyjny, zadania pobierania aktualizacji zostaną automatycznie uruchomione na podrzędnych Serwerach administracyjnych bez względu na ich terminarz.

Główny Serwer Administracyjny aktualizuje antywirusowe bazy danych na podstawie aplikacji zainstalowanych na podrzędnych Serwerach Administracyjnych. Instalacja dodatkowych wtyczek i tworzenie pakietów instalacyjnych na głównym Serwerze administracyjnym nie jest wymagane.

Automatyczne przypisywanie punktów dystrybucji

Zalecane jest automatyczne przypisywanie punktów dystrybucji. Kaspersky Security Center sam wybierze urządzenia, które mają być punktami dystrybucji.

Aby automatycznie przypisać punkty dystrybucji:

1. Otwórz okno główne aplikacji.

2. W drzewie konsoli należy wybrać węzeł z nazwą Serwera administracyjnego, dla którego chcesz automatycznie przypisać punkty dystrybucji.

3. W menu kontekstowym Serwera administracyjnego kliknij **Właściwości**.

4. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Punkty dystrybucji**.

5. W prawej części okna wybierz opcję **Automatycznie przypisz punkty dystrybucji**.

   Jeśli włączone jest automatyczne wskazywanie urządzeń jako punktów dystrybucji, nie można ręcznie skonfigurować punktów dystrybucji, ani też zmodyfikować listy punktów dystrybucji.

6. Kliknij **OK**.

Serwer administracyjny automatycznie przypisze i skonfiguruje punkty dystrybucji.

Ręczne wskazywanie urządzenia jako punktu dystrybucji

Kaspersky Security Center umożliwia wskazanie urządzeń do pełnienia roli punktów dystrybucji.

Zalecane jest automatyczne przypisywanie punktów dystrybucji. W tym przypadku, Kaspersky Security Center sam wybierze urządzenia, które mają być punktami dystrybucji. Jednakże, jeśli z jakiegoś powodu musisz zrezygnować z automatycznego przypisywania punktów dystrybucji (na przykład, jeśli chcesz korzystać ze specjalnie wybranych serwerów), możesz ręcznie przypisać punkty dystrybucji po obliczeniu ich liczby i konfiguracji.

Urządzenia pełniące rolę punktów dystrybucji muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

W celu ręcznego wskazania urządzenia jako punktu dystrybucji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji** i kliknij przycisk **Dodaj**. Ten przycisk jest dostępny, jeśli zaznaczono opcję **Ręcznie przypisz punkty dystrybucji**.

   Spowoduje to otwarcie okna **Dodaj punkt dystrybucji**.
4. W oknie **Dodaj punkt dystrybucji** wykonaj następujące działania:

   a. Wybierz urządzenie, które będzie pełniło rolę punktu dystrybucji (wybierz je z grupy administracyjnej lub określ adres IP urządzenia). Podczas wybierania urządzenia pamiętaj o zasadach działania punktów dystrybucji i wymaganiach ustawionych dla urządzenia pełniącego rolę punktu dystrybucji.

   b. Wskaż określone urządzenia, na które punkt dystrybucji roześle uaktualnienia. Możesz określić opis grupy administracyjnej lub lokalizacji sieciowej.
5. Kliknij **OK**.

   Dodany punkt dystrybucji będzie wyświetlany na liście punktów dystrybucji, w sekcji **Punkty dystrybucji**.
6. Na liście wskaż nowo dodany punkt dystrybucji i kliknij przycisk **Właściwości**, aby otworzyć jego okno właściwości.
7. Skonfiguruj punkt dystrybucji w oknie właściwości:

   - Sekcja **Ogólne** zawiera ustawienia interakcji pomiędzy punktem dystrybucji a urządzeniami klienckimi.

     - **Port SSL**

       Numer portu SSL do nawiązywania zaszyfrowanych połączeń między urządzeniami klienckimi a punktem dystrybucji przy użyciu SSL.

       Domyślnie wykorzystywany jest port 13000.

     - **Użyj multiemisji**

       Jeśli ta opcja jest włączona, multicasting IP będzie używany do automatycznego rozsyłania pakietów instalacyjnych na urządzenia klienckie w obrębie grupy.

       Multiemisja IP zmniejsza czas wymagany do zainstalowania aplikacji z pakietu instalacyjnego w grupie urządzeń klienckich, ale zwiększa czas instalacji, gdy instalujesz aplikację na jednym urządzeniu klienckim.

- **Adres IP multiemisji**

  Adres IP, który będzie używany do multiemisji. Możesz zdefiniować adres IP z zakresu 224.0.0.0 – 239.255.255.255

  Domyślnie, Kaspersky Security Center automatycznie przypisze unikatowy adres IP multiemisji w obrębie danego zakresu.

- **Numer portu multiemisji IP**

  Numer portu do multiemisji IP.

  Domyślnym numerem portu jest 15001. Jeśli jako punkt dystrybucji określono urządzenie, na którym działa Serwer administracyjny, domyślnie dla połączenia SSL używany jest port 13001.

- **Roześlij aktualizacje**

  Aktualizacje są dystrybuowane na zarządzane urządzenia z następujących źródeł:

  - Ten punkt dystrybucji, jeśli ta opcja jest włączona.
  - Inne punkty dystrybucji, Serwer administracyjny lub serwery aktualizacji Kaspersky, jeśli ta opcja jest wyłączona.

  Jeśli używasz punktów dystrybucji do wdrażania aktualizacji, możesz zmniejszyć ruch, ponieważ zmniejszasz liczbę pobrań. Możesz także odciążyć Serwer administracyjny i przenieść obciążenie między punktami dystrybucji. Możesz obliczyć liczbę punktów dystrybucji w Twojej sieci w celu optymalizacji ruchu i obciążenia.

  Jeśli wyłączysz tę opcję, liczba pobrań aktualizacji i obciążenia Serwera administracyjnego mogą wzrosnąć. Domyślnie opcja ta jest włączona.

- **Roześlij pakiety instalacyjne**

  Pakiety instalacyjne są dystrybuowane na zarządzane urządzenia z następujących źródeł:

  - Ten punkt dystrybucji, jeśli ta opcja jest włączona.
  - Inne punkty dystrybucji, Serwer administracyjny lub serwery aktualizacji Kaspersky, jeśli ta opcja jest wyłączona.

  Jeśli używasz punktów dystrybucji do wdrażania pakietów instalacyjnych, możesz zmniejszyć ruch, ponieważ zmniejszasz liczbę pobrań. Możesz także odciążyć Serwer administracyjny i przenieść obciążenie między punktami dystrybucji. Możesz obliczyć liczbę punktów dystrybucji w Twojej sieci w celu optymalizacji ruchu i obciążenia.

  Jeśli wyłączysz tę opcję, liczba pobrań pakietów instalacyjnych i obciążenie Serwera administracyjnego może wzrosnąć. Domyślnie opcja ta jest włączona.

- **Użyj tego punktu dystrybucji jako serwera push**

  W Kaspersky Security Center punkt dystrybucji może działać jako serwer push dla urządzeń zarządzanych za pośrednictwem protokołu mobilnego. Na przykład, serwer push musi być włączony, jeśli chcesz mieć możliwość wymuszenia synchronizacji urządzeń KasperskyOS z Serwerem administracyjnym. Serwer push posiada ten sam obszar zarządzanych urządzeń jako punkt dystrybucji, na którym włączono serwer push. Jeśli posiadasz kilka punktów dystrybucji przypisanych dla tej samej grupy administracyjnej, możesz włączyć serwer push na każdym punkcie dystrybucji. W tym przypadku Serwer administracyjny rozkłada obciążenie między punkty dystrybucji.

  Jeśli zarządzasz urządzeniami z zainstalowanym KasperskyOS lub planujesz to zrobić, musisz użyć punktu dystrybucji jako serwera push. Możesz także użyć punktu dystrybucji jako serwera push, jeśli chcesz wysłać powiadomienia push na urządzenia klienckie.

- **Port serwera push**

  Port na punkcie dystrybucji, którego urządzenia klienckie użyją do nawiązania połączenia. Domyślnie wykorzystywany jest port 13295.

- W sekcji **Zakres** określ obszar, w jakim punkt dystrybucji będzie rozsyłał uaktualnienia (grupy administracyjne i/lub lokalizacja sieciowa).

- W sekcji **KSN Proxy** możesz skonfigurować aplikację, aby używała punktu dystrybucji do przesyłania żądań KSN z zarządzanych urządzeń.

  - **Włącz KSN Proxy po stronie punktu dystrybucji**

    Usługa KSN proxy jest uruchamiana na urządzeniu, które jest używane jako punkt dystrybucji. Użyj tej funkcji do redystrybucji i optymalizacji ruchu w sieci.

    Punkt dystrybucji wysyła statystyki KSN, które zostały wymienione w Oświadczeniu Kaspersky Security Network, do Kaspersky.

    Domyślnie opcja ta jest wyłączona. Włączenie tej opcji działa, jeśli opcje **Użyj Serwera administracyjnego jako serwera proxy** i **Zgadzam się na korzystanie z Kaspersky Security Network** zostały włączone w oknie właściwości Serwera administracyjnego.

    Możesz przypisać węzeł klastra aktywny-pasywny do punktu dystrybucji i włączyć serwer proxy KSN na tym węźle.

  - **Przesyłaj żądania KSN do Serwera administracyjnego**

    Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do Serwera administracyjnego.

    Domyślnie opcja ta jest włączona.

  - **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**

    Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do chmury KSN lub KPSN. Żądania KSN wygenerowane na samym punkcie dystrybucji są także wysyłane bezpośrednio do chmury KSN lub KPSN.

    Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej), nie mogą uzyskać bezpośredniego dostępu do KPSN. Jeśli chcesz ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do KPSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji.

    Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 12 (lub późniejszej), mogą uzyskać bezpośredni dostęp do KPSN.

  - **Ignoruj ustawienia serwera proxy w przypadku łączenia z KPSN**

    Włącz tę opcję, jeśli skonfigurowałeś ustawienia serwera proxy we właściwościach punktu dystrybucji lub w zasadzie Agenta sieciowego, ale architektura Twojej sieci wymaga bezpośredniego korzystania z KPSN. W przeciwnym razie, żądania z zarządzanych aplikacji nie będą mogły dotrzeć do KPSN.

    Ta opcja jest dostępna, jeśli wybierzesz opcję **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**.

  - **Port TCP**

    Numer portu TCP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny numer portu to 13111.

- **Port UDP**

  Jeśli chcesz, żeby Agent Sieciowy nawiązywał połączenie z Serwerem administracyjnym poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **Numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z Serwerem administracyjnym to 15000.

- **Port HTTPS**

  Jeśli chcesz, aby zarządzane urządzenia nawiązywały połączenie z serwerem KSN Proxy poprzez port HTTPS, włącz opcję **Użyj HTTPS** i określ numer **HTTPS przez port**. Domyślny port HTTPS do nawiązywania połączenia z serwerem KSN Proxy to 17111.

- W sekcji **Wykrywanie urządzeń** skonfiguruj przeszukiwanie domen Windows, Active Directory i zakresów IP przez punkt dystrybucji.

  - **Domeny Windows**

    Możesz włączyć wykrywanie urządzeń dla domen Windows i ustawić terminarz dla wyszukiwania.

  - **Active Directory**

    Możesz włączyć przeszukiwanie sieci dla Active Directory i ustawić terminarz dla przeszukiwania.

    Jeśli korzystasz z punktu dystrybucji systemu Windows, możesz wybrać jedną z następujących opcji:

    - **Przeszukaj bieżącą domenę Active Directory**.
    - **Przeszukaj las domen Active Directory**.
    - **Przeszukaj tylko wybrane domeny Active Directory**. Jeśli wybierzesz tę opcję, dodaj jedną lub kilka domen Active Directory do listy.

    Jeśli korzystasz z punktu dystrybucji systemu Linux z zainstalowanym Agentem sieciowym w wersji 15, możesz odpytywać tylko domeny Active Directory, dla których określisz adres i poświadczenia użytkownika. Sondowanie bieżącej domeny Active Directory i lasu domeny Active Directory nie jest dostępne.

  - **Zakresy IP**

    Możesz włączyć wykrywanie urządzeń dla zakresów IPv4 i sieci IPv6.

    Jeśli włączysz opcję **Włącz przeszukiwanie zakresów**, możesz dodać skanowane zakresy i skonfigurować dla nich terminarz. Możesz dodać zakresy IP do listy skanowanych zakresów.

    Jeśli włączysz opcję **Użyj Zeroconf do przeszukiwania sieci IPv6**, punkt dystrybucji automatycznie odpytuje sieć IPv6 za pomocą zero-configuration networking (zwany również *Zeroconf*). W takim przypadku określone zakresy adresów IP są ignorowane, ponieważ punkt dystrybucji przeszukuje całą sieć. Opcja **Użyj Zeroconf do przeszukiwania sieci IPv6** jest dostępna, jeśli w punkcie dystrybucji działa system Linux. Aby korzystać z odpytywania Zeroconf IPv6, musisz zainstalować narzędzie avahi-browse w punkcie dystrybucji.

- W sekcji **Zaawansowane** określ folder, którego punkt dystrybucji musi używać do przechowywania rozsyłanych danych.

  - **Użyj domyślnego folderu**

    Jeśli wybierzesz tę opcję, aplikacja użyje folderu instalacyjnego Agenta sieciowego na urządzeniu działającym jako punkt dystrybucji.

- **Użyj określonego folderu**

  Jeśli wybierzesz tę opcję, w polu poniżej możesz określić ścieżkę dostępu do wybranego folderu. Może to być folder lokalny na urządzeniu działającym jako punkt dystrybucji lub folder na dowolnym urządzeniu w obrębie sieci korporacyjnej.

  Konto użytkownika używane na urządzeniu działającym jako punkt dystrybucji do uruchamiania Agenta sieciowego musi mieć uprawnienia do odczytu/zapisu określonego folderu.

Wybrane urządzenia będą pełnić rolę punktów dystrybucji.

Tylko urządzenia działające pod kontrolą systemu operacyjnego Windows mogą determinować swoją lokalizację sieciową. Lokalizacja sieciowa nie może zostać określona dla urządzeń z zainstalowanymi innymi systemami operacyjnymi.

Usuwanie urządzenia z listy punktów dystrybucji

W celu usunięcia urządzenia z listy punktów dystrybucji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w sekcji **Punkty dystrybucji** wybierz urządzenie, które pełni rolę punktu dystrybucji, i kliknij przycisk **Usuń**.

Urządzenie zostanie usunięte z listy punktów dystrybucji i przestanie działać jako punkt dystrybucji.

Urządzenia nie można usunąć z listy punktów dystrybucji, jeśli zostało przypisane automatycznie przez Serwer administracyjny.

Pobieranie uaktualnień przez punkty dystrybucji

Kaspersky Security Center umożliwia punktom dystrybucji pobieranie uaktualnień z Serwera administracyjnego, serwerów Kaspersky bądź też folderu lokalnego lub sieciowego.

Jeśli nie ma potrzeby określania źródła aktualizacji, zalecamy użycie zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla grupy administracyjnej. Aby uzyskać szczegółowe informacje, zapoznaj się z poniższym tematem: Tworzenie zadania Pobierz uaktualnienia do repozytoriów punktów dystrybucji.

W celu skonfigurowania pobierania uaktualnień dla punktu dystrybucji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w sekcji **Punkty dystrybucji** wybierz punkt dystrybucji, przez którego uaktualnienia będą dostarczane na urządzenia klienckie w grupie.

4. Kliknij przycisk **Właściwości**, aby otworzyć okno właściwości wybranego punktu dystrybucji.

5. W oknie właściwości punktu dystrybucji wybierz sekcję **Źródła aktualizacji**.

6. Wskaż źródło uaktualnień dla punktu dystrybucji:

   - Aby zezwolić punktowi dystrybucji na pobieranie uaktualnień z Serwera administracyjnego, zaznacz opcję **Pobierz z Serwera administracyjnego**:

     - **Pobierz pliki diff**

       Ta opcja włącza funkcję pobierania plików diff.

       Domyślnie opcja ta jest włączona.

   - Aby zezwolić punktowi dystrybucji na pobieranie uaktualnień przy użyciu zadania, wybierz **Użyj zadania do wymuszonego pobierania uaktualnień**:

     - Kliknij przycisk **Przeglądaj**, jeśli takie zadanie już istnieje na urządzeniu, i wybierz zadanie z listy, która zostanie wyświetlona.

     - Kliknij przycisk **Nowe zadanie**, aby utworzyć zadanie, jeśli nie ma go na urządzeniu. Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

     Zadanie Pobierz uaktualnienia do repozytoriów punktów dystrybucji to zadanie lokalne. Należy utworzyć nowe zadanie dla każdego urządzenia pełniącego rolę punktu dystrybucji.

Punkt dystrybucji będzie pobierał uaktualnienia z określonego źródła.

Usuwanie aktualizacji oprogramowania z repozytorium

W celu usunięcia aktualizacji oprogramowania z repozytorium Serwera administracyjnego:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.

2. W obszarze roboczym folderu **Aktualizacje oprogramowania** wybierz uaktualnienie, które chcesz usunąć.

3. W menu kontekstowym uaktualnienia wybierz **Usuń pliki aktualizacji**.

Aktualizacje oprogramowania zostaną usunięte z repozytorium Serwera administracyjnego.

Instalacja poprawki dla aplikacji Kaspersky w trybie klastra

Kaspersky Security Center obsługuje tylko ręczną instalacje łat dla aplikacji Kaspersky w trybie klastra.

W celu zainstalowania łaty dla aplikacji Kaspersky:

1. Pobierz łatę do każdego węzła klastra.
2. Uruchom instalację łaty na aktywnym węźle.
3. Poczekaj na pomyślne zainstalowanie łaty.
4. Uruchom łatę na wszystkich podwęzłach klastra po kolei.

   Jeśli uruchamiasz poprawkę z poziomu wiersza poleceń, użyj klucza `-CLUSTER_SECONDARY_NODE`.

   Łata zostanie zainstalowana na wszystkich węzłach klastra.
5. Uruchom usługi klastra Kaspersky ręcznie.

Każdy węzeł klastra jest wyświetlany w Konsoli administracyjnej jako urządzenie z zainstalowanym Agentem sieciowym.

Informacje na temat zainstalowanych łat można znaleźć w folderze **Aktualizacje oprogramowania** lub w raporcie o wersjach aktualizacji modułów aplikacji Kaspersky.

Zarządzanie aplikacjami firm trzecich na urządzeniach klienckich

Kaspersky Security Center umożliwia zarządzanie aplikacjami firmy Kaspersky i innych producentów, które są zainstalowane na urządzeniach klienckich.

Administrator może wykonywać następujące akcje:

- Tworzyć kategorie aplikacji w oparciu o określone kryteria.
- Zarządzać kategoriami aplikacji przy pomocy reguł utworzonych specjalnie do tego celu.
- Zarządzać aplikacjami uruchomionymi na urządzeniach.
- Przeprowadzać inwentaryzację i utrzymywać rejestr oprogramowania zainstalowanego na urządzeniach.
- Naprawiać luki w oprogramowaniu zainstalowanym na urządzeniach.
- Instalować uaktualnienia z Windows Update i od producentów innego oprogramowania na urządzeniach.
- Monitorować korzystanie z kluczy licencyjnych dla grup licencjonowanych aplikacji.

Informacje o aplikacjach innych firm

Kaspersky Security Center może pomóc w aktualizacji oprogramowania firm trzecich, zainstalowanego na urządzeniach klienckich, a także w eliminacji luk w oprogramowaniu firm trzecich. Kaspersky Security Center może aktualizować oprogramowanie innych firm tylko z bieżącej wersji do najnowszej wersji.

Listę oprogramowania innych firm można zmieniać i jest ona aktualizowana na bieżąco. Możesz sprawdzić, czy możesz zaktualizować oprogramowanie innych firm (zainstalowane na urządzeniach użytkowników) za pomocą Kaspersky Security Center poprzez przejrzenie listy dostępnych aktualizacji w Konsoli administracyjnej opartej na MMC i w Kaspersky Security Center Web Console.

Opisana poniżej procedura służy wyłącznie do przeglądania listy oprogramowania innych firm, które można aktualizować za pomocą Kaspersky Security Center. Poniższe kroki mają na celu uzyskanie dostępu do odpowiednich informacji bez konieczności inicjowania jakichkolwiek zadań.

Aby wyświetlić listę oprogramowania innych firm, które można aktualizować za pomocą Kaspersky Security Center w Kaspersky Security Center Web Console:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. W kroku **Ustawienia nowych zadań** kreatora określ następujące ustawienia:

   a. Z listy rozwijanej **Aplikacja** wybierz **Kaspersky Security Center**.

   b. W polu **Typ zadania** wybierz **Zainstaluj wymagane aktualizacje i napraw luki**.
4. W kroku **Zakres zadania** kreatora wybierz opcję **Zarządzane urządzenia**.
5. W kroku **Określ reguły instalacji aktualizacji** kreatora kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
6. W kroku **Wybierz typ reguły** kreatora wybierz opcję **Reguła dla aktualizacji firm trzecich**.
7. W kroku **Kryteria ogólne** kreatora wybierz opcję **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**, a następnie kliknij przycisk **Dalej**.

Wyświetlana jest lista oprogramowania innych firm.

Aby wyświetlić listę oprogramowania innych firm, które można aktualizować za pomocą Kaspersky Security Center w konsoli opartej na MMC, potrzebna jest licencja na zarządzanie lukami i poprawkami. W przeciwnym razie zadanie **Zainstaluj wymagane aktualizacje i napraw luki** nie będzie dostępne.

1. W drzewie konsoli wybierz folder **Zarządzane urządzenia**.
2. W obszarze roboczym wybierz zakładkę **Zadania**.

3. Kliknij przycisk **Utwórz zadanie**, aby uruchomić Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.

4. W oknie **Wybierz typ zadania** wybierz **Zainstaluj wymagane aktualizacje i napraw luki**.

5. W kroku **Określ reguły instalacji aktualizacji** kreatora kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

6. W kroku **Wybierz typ reguły** kreatora wybierz opcję **Reguła dla aktualizacji firm trzecich**.

7. W kroku **Kryteria ogólne** kreatora wybierz opcję **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**, a następnie kliknij przycisk **Dalej**.

Wyświetlana jest lista oprogramowania innych firm.

Instalowanie aktualizacji oprogramowania firm trzecich

Kaspersky Security Center umożliwia zarządzanie aktualizacjami oprogramowania zainstalowanego na urządzeniach klienckich oraz wyeliminowanie luk w aplikacjach Microsoft i produktach innych dostawców poprzez zainstalowanie żądanych aktualizacji.

Kaspersky Security Center wyszukuje aktualizacje przy pomocy zadania wyszukiwania aktualizacji i pobiera je do repozytorium uaktualnień. Po zakończeniu wyszukiwania aktualizacji, aplikacja udostępnia administratorowi informacje o dostępnych aktualizacjach i lukach w aplikacji, które mogą zostać naprawione dzięki tym aktualizacjom.

Informacje o aktualizacjach dostępnych dla Microsoft Windows są dostępne poprzez usługę Windows Update. Serwer administracyjny może zostać użyty jako serwer Windows Server Update Services (WSUS). Aby używać Serwera administracyjnego jako serwera WSUS, powinieneś skonfigurować synchronizację aktualizacji z Windows Update. Po skonfigurowaniu synchronizacji danych z Windows Update, Serwer administracyjny zapewnia aktualizacje dla usług Windows Update na urządzeniach w trybie scentralizowanym i z określoną częstotliwością.

Możesz również zarządzać aktualizacjami oprogramowania poprzez zasadę Agenta sieciowego. W tym celu, w odpowiednich oknach Kreatora tworzenia nowej zasady powinieneś utworzyć zasadę Agenta sieciowego i skonfigurować aktualizowanie oprogramowania.

Administrator może przeglądać listę dostępnych aktualizacji w podfolderze **Aktualizacje oprogramowania** znajdującym się w folderze **Zarządzanie aplikacjami**. Ten folder zawiera listę uaktualnień pobranych przez Serwer administracyjny dla aplikacji Microsoft i innych producentów oprogramowania, które mogą być przesyłane na urządzenia. Po przejrzeniu informacji o dostępnych aktualizacjach, administrator może zainstalować je na urządzeniach.

Kaspersky Security Center aktualizuje niektóre aplikacje poprzez usunięcie poprzedniej wersji aplikacji i instalację nowej.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Upewnij się, że opcja **Wyświetl zarządzanie lukami i poprawkami** jest włączona w oknie **Konfiguruj interfejs** dla głównego i podrzędnego Serwera administracyjnego. W przeciwnym razie zadanie wyszukiwania aktualizacji obsługuje tylko aktualizacje WSUS.

Ze względów bezpieczeństwa wszelkie aktualizacje oprogramowania innych firm, które instalujesz za pomocą funkcji Zarządzanie lukami i poprawkami, są automatycznie skanowane w poszukiwaniu szkodliwego oprogramowania przez technologie firmy Kaspersky. Technologie te są używane do automatycznego sprawdzania plików i obejmują skanowanie antywirusowe, analizę statyczną, analizę dynamiczną, analizę zachowania w środowisku sandbox i uczenie maszynowe.

Eksperci firmy Kaspersky nie przeprowadzają ręcznej analizy aktualizacji oprogramowania innych firm, które są instalowane przez funkcję Zarządzanie lukami i poprawkami. Ponadto eksperci z firmy Kaspersky nie wyszukują luk (znanych lub nieznanych) ani nieudokumentowanych funkcji w takich aktualizacjach, a także nie przeprowadzają innych rodzajów analizy aktualizacji innych, niż określone w powyższym akapicie.

Przed zainstalowaniem uaktualnień na wszystkich urządzeniach możesz przeprowadzić instalację testową, aby upewnić się, że zainstalowane uaktualnienia nie spowodują błędu w działaniu aplikacji na urządzeniach.

Scenariusz: Aktualizowanie oprogramowania innej firmy

Ta sekcja oferuje scenariusz aktualizacji oprogramowania innej firmy, zainstalowanego na urządzeniach klienckich. Oprogramowanie firm trzecich obejmuje aplikacje firmy Microsoft oraz programy innych firm. Aktualizacje dla aplikacji firmy Microsoft są dostarczane przez usługę Windows Update.

Wymagania wstępne

Serwer administracyjny musi mieć połączenie z Internetem, aby zainstalować aktualizacje oprogramowania firm trzecich innego niż oprogramowanie firmy Microsoft.

Domyślnie połączenie internetowe w przypadku Serwera administracyjnego nie jest wymagane w celu instalowania aktualizacji oprogramowania firmy Microsoft na zarządzanych urządzeniach. Na przykład zarządzane urządzenia mogą pobierać aktualizacje oprogramowania firmy Microsoft bezpośrednio z serwerów Microsoft Update lub z systemu Windows Server z programem Microsoft Windows Server Update Services (WSUS) wdrożonymi w sieci organizacji. Serwer administracyjny musi być połączony z Internetem, jeśli jest on używany jako serwer WSUS.

Etapy

Aktualizowanie oprogramowania firm trzecich odbywa się w etapach:

1. **Wyszukiwanie wymaganych aktualizacji**

   Aby odnaleźć aktualizacje oprogramowania firm trzecich dla zarządzanych urządzeń, uruchom zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Kaspersky Security Center pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania.

   Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie przez Kreator wstępnej konfiguracji Serwera administracyjnego. Jeśli nie uruchomiono kreatora, utwórz zadanie lub uruchom Kreator wstępnej konfiguracji teraz.

   Dostępne instrukcje:

   - Konsola administracyjna: Skanowanie aplikacji w poszukiwaniu luk, Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
   - Kaspersky Security Center Web Console: Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji, Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

2. **Analizowanie listy wykrytych aktualizacji**

   Przejrzyj listę **Aktualizacje oprogramowania** i zdecyduj, które aktualizacje chcesz zainstalować. Aby przejrzeć szczegółowe informacje o każdej aktualizacji, kliknij nazwę aktualizacji na liście. Dla każdej aktualizacji na liście możesz także przejrzeć statystyki dotyczące instalacji aktualizacji na urządzeniach klienckich.

   Dostępne instrukcje:

   - Konsola administracyjna: Przeglądanie informacji o dostępnych aktualizacjach
   - Kaspersky Security Center Web Console: Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich

3. **Konfigurowanie instalacji aktualizacji**

   Jeśli Kaspersky Security Center odebrał listę aktualizacji oprogramowania firm trzecich, możesz zainstalować je na urządzeniach klienckich przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki* lub zadania *Zainstaluj aktualizacje Windows Update*. Utwórz jedno z tych zadań. Możesz utworzyć te zadania na zakładce **Zadania** lub korzystając z listy **Aktualizacje oprogramowania**.

   Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do zainstalowania aktualizacji dla aplikacji firmy Microsoft, w tym aktualizacji dostarczonych przez usługę Windows Update, a także aktualizacji produktów innych producentów. Pamiętaj, że to zadanie może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami.

   Zadanie *Zainstaluj aktualizacje Windows Update* nie wymaga licencji, ale może zostać użyte tylko do zainstalowania aktualizacji Windows Update.

   Aby zainstalować niektóre aktualizacje oprogramowania, należy zaakceptować Umowę licencyjną użytkownika końcowego (EULA) do zainstalowania oprogramowania. Jeśli odrzucisz Umowę licencyjną użytkownika końcowego, aktualizacja oprogramowania nie zostanie zainstalowana.

   Możesz uruchomić zadanie instalacji aktualizacji zgodnie z terminarzem. Podczas określania terminarza zadania upewnij się, że zadanie instalacji aktualizacji jest uruchamiane po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

Dostępne instrukcje:

- Konsola administracyjna: Naprawianie luk w aplikacjach, Przeglądanie informacji o dostępnych aktualizacjach
- Kaspersky Security Center Web Console: Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki, Tworzenie zadania Zainstaluj aktualizacje Windows Update, Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich

4 **Konfigurowanie terminarza zadań**

Aby upewnić się, że lista aktualizacji jest zawsze aktualna, skonfiguruj terminarz zadania *Wyszukiwanie luk i wymaganych aktualizacji* tak, aby było uruchamiane automatycznie od czasu do czasu. Domyślnie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest ustawione na uruchamianie ręczne.

Jeśli utworzyłeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz skonfigurować terminarz tak, aby zadanie było uruchamiane z tą samą częstotliwością co zadanie *Wyszukiwanie luk i wymaganych aktualizacji* lub rzadziej. Podczas konfigurowania terminarza zadania *Zainstaluj aktualizacje Windows Update* należy pamiętać, że dla tego zadania konieczne jest zdefiniowanie listy aktualizacji za każdym razem przed uruchomieniem tego zadania.

Jeśli konfigurujesz terminarz uruchamiania zadań, upewnij się, że zadanie instalacji aktualizacji zostanie uruchomione po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

5 **Zatwierdzanie i odrzucanie aktualizacji oprogramowania (opcjonalne)**

Jeśli utworzyłeś zadanie Zainstaluj wymagane aktualizacje i napraw luki, możesz określić reguły instalacji aktualizacji we właściwościach zadania. Jeśli utworzyłeś zadanie Zainstaluj aktualizacje Windows Update, pomiń ten krok.

Dla każdej reguły możesz zdefiniować aktualizacje do zainstalowania w zależności od stanu aktualizacji: *Nie zdefiniowano*, *Zatwierdzono* lub *Odrzucono*. Na przykład, możesz utworzyć określone zadanie dla serwerów i ustawić regułę dla tego zadania, aby zezwolić na instalację tylko aktualizacji Windows Update i tylko tych, które posiadają stan *Zatwierdzono*. Po ręcznym ustawieniu stanu *Zatwierdzono* dla tych aktualizacji, które chcesz zainstalować. W tym przypadku aktualizacje Windows Update, które posiadają stan *Nie zdefiniowano* lub *Odrzucono*, nie będą zainstalowane na serwerach, które określiłeś w zadaniu.

Używanie stanu *Zatwierdzone* do zarządzania instalacją aktualizacji jest wystarczające dla małej ilości uaktualnień. Aby zainstalować kilka aktualizacji, użyj reguł, które możesz skonfigurować w zadaniu *Zainstaluj wymagane aktualizacje i napraw luki*. Zalecane jest ustawienie stanu *Zatwierdzone* tylko dla tych określonych aktualizacji, które nie spełniają kryteriów określonych w regułach. Jeśli ręcznie zatwierdzisz dużą liczbę aktualizacji, wydajność Serwera administracyjnego ulegnie zmniejszeniu i może doprowadzić do przeciążenia Serwera administracyjnego.

Domyślnie pobrane aktualizacje oprogramowania posiadają stan *Niezdefiniowane*. Możesz zmienić stan na *Zatwierdzono* lub *Odrzucono* na liście **Aktualizacje oprogramowania** list (**Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**).

Dostępne instrukcje:

- Konsola administracyjna: Zatwierdzanie i odrzucanie aktualizacji oprogramowania
- Kaspersky Security Center Web Console: Zatwierdzanie i odrzucanie aktualizacji oprogramowania innych firm

6 **Konfigurowanie Serwera administracyjnego do pracy jako serwer Windows Server Update Services (WSUS) (opcjonalne)**

Domyślnie, aktualizacje Windows Update są pobierane na zarządzane urządzenia z serwerów Microsoft. Możesz zmienić to ustawienie, żeby używać Serwera administracyjnego jako serwera WSUS. W tym przypadku Serwer administracyjny synchronizuje dane aktualizacji z Windows Update w określonej częstotliwości i dostarcza aktualizacje w trybie scentralizowanym do Windows Update na urządzeniach w sieci.

Aby użyć Serwera administracyjnego jako serwera WSUS, utwórz zadanie Wykonaj synchronizację Windows Update i zaznacz pole **Użyj Serwera administracyjnego jako serwera WSUS** w zasadzie Agenta sieciowego.

Dostępne instrukcje:

- Konsola administracyjna: Synchronizowanie aktualizacji z Windows Update z Serwerem administracyjnym, Konfigurowanie aktualizacji systemu Windows w zasadzie Agenta sieciowego
- Kaspersky Security Center Web Console: Tworzenie zadania synchronizacji Windows Update

7. **Uruchamianie zadania instalacji aktualizacji**

   Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Zainstaluj aktualizacje Windows Update*. Jeśli uruchamiasz te zadania, aktualizacje są pobierane i instalowane na zarządzanych urządzeniach. Po zakończeniu zadania, upewnij się, że na liście zadań posiada stan *Zakończone pomyślnie*.

8. **Utwórz raport dotyczący wyników instalacji aktualizacji oprogramowania firm trzecich (opcjonalne)**

   Aby wyświetlić szczegółowe statystyki dotyczące instalacji aktualizacji, utwórz **Raport z wynikami instalacji aktualizacji oprogramowania firm trzecich**.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie i przeglądanie raportu
   - Kaspersky Security Center Web Console: Tworzenie i przeglądanie raportu

Wyniki

Jeśli utworzyłeś i skonfigurowałeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, aktualizacje są automatycznie instalowane na zarządzanych urządzeniach. Jeśli nowe aktualizacje zostaną pobrane do repozytorium Serwera administracyjnego, Kaspersky Security Center sprawdzi, czy spełniają kryteria określone w regułach aktualizacji. Wszystkie nowe aktualizacje, które spełniają kryteria, zostaną zainstalowane automatycznie przy kolejnym uruchomieniu zadania.

Jeśli utworzyłeś zadanie *Zainstaluj aktualizacje Windows Update*, instalowane są tylko te aktualizacje określone we właściwościach zadania *Zainstaluj aktualizacje Windows Update*. W przyszłości, jeśli będziesz chciał zainstalować nowe aktualizacje pobrane do repozytorium Serwera administracyjnego, będziesz musiał dodać wymagane aktualizacje do listy aktualizacji w istniejącym zadaniu lub utworzyć nowe zadanie *Zainstaluj aktualizacje Windows Update*.

Przeglądanie informacji o dostępnych aktualizacjach aplikacji innych firm

W celu przejrzenia listy aktualizacji dostępnych dla aplikacji firm trzecich, zainstalowanych na urządzeniach klienckich:

W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.

W obszarze roboczym folderu możesz przejrzeć listę aktualizacji dostępnych dla aplikacji zainstalowanych na urządzeniach.

W celu przejrzenia właściwości aktualizacji,

W obszarze roboczym folderu **Aktualizacje oprogramowania**, z menu kontekstowego aktualizacji wybierz **Właściwości**.

W oknie właściwości aktualizacji można przeglądać następujące informacje:

- W sekcji **Ogólne** możesz wyświetlić **Stan zatwierdzenia aktualizacji**:
  - **Nie zdefiniowano** — aktualizacja jest dostępna na liście aktualizacji, ale nie została zatwierdzona do instalacji.
  - **Zatwierdzono** — aktualizacja jest dostępna na liście aktualizacji i zatwierdzona do instalacji.
  - **Odrzucono** — instalacja aktualizacji została odrzucona.
- W sekcji **Atrybuty** możesz zobaczyć wartości pola **Zainstalowana automatycznie**:
  - Ta wartość **Automatycznie** jest wyświetlana, jeśli zadanie *Zainstaluj wymagane aktualizacje i napraw luki* może zainstalować aktualizacje dla aplikacji. Zadanie automatycznie instaluje nowe aktualizacje z adresu internetowego dostarczonego przez dostawcę oprogramowania innej firmy.
  - Ta wartość **Ręcznie** jest wyświetlana, jeśli Kaspersky Security Center nie może automatycznie zainstalować aktualizacji dla aplikacji. Aktualizacje można zainstalować ręcznie.

  To pole **Zainstalowana automatycznie** nie jest wyświetlane w przypadku aktualizacji aplikacji Windows.
- Listę urządzeń klienckich, dla których przeznaczona jest aktualizacja.
- Listę komponentów systemu (wymagania wstępne), które należy zainstalować przed aktualizacjami (jeśli istnieją).
- Luki w oprogramowaniu, które aktualizacja wyeliminuje.

Zatwierdzanie i odrzucanie aktualizacji oprogramowania

Ustawienia zadania instalacji aktualizacji mogą wymagać zatwierdzenia aktualizacji, które mają zostać zainstalowane. Możesz zatwierdzić uaktualnienia, które muszą zostać zainstalowane, oraz odrzucić uaktualnienia, które nie muszą zostać zainstalowane.

Na przykład, możesz chcieć najpierw sprawdzić instalację aktualizacji w środowisku testowym i upewnić się, że nie wpływają negatywnie na działanie urządzeń, a następnie zezwolić na instalację tylko tych aktualizacji na urządzeniach klienckich.

Używanie stanu *Zatwierdzone* do zarządzania instalacją aktualizacji firm trzecich jest wystarczające dla małej ilości uaktualnień. Aby zainstalować kilka aktualizacji innych firm, użyj reguł, które możesz skonfigurować w zadaniu *Zainstaluj wymagane aktualizacje i napraw luki*. Zalecane jest ustawienie stanu *Zatwierdzone* tylko dla tych określonych aktualizacji, które nie spełniają kryteriów określonych w regułach. Jeśli ręcznie zatwierdzisz dużą liczbę aktualizacji, wydajność Serwera administracyjnego ulegnie zmniejszeniu i może doprowadzić do przeciążenia Serwera administracyjnego.

W celu zatwierdzenia lub odrzucenia jednej lub kilku aktualizacji:

1. W drzewie konsoli wybierz węzeł **Zaawansowane → Zarządzanie aplikacjami → Aktualizacje oprogramowania**.
2. W obszarze roboczym folderu **Aktualizacje oprogramowania** kliknij przycisk **Odśwież** w prawym górnym rogu. Zostanie wyświetlona lista uaktualnień.
3. Wybierz uaktualnienia, które chcesz zatwierdzić lub odrzucić.

   W prawej części obszaru roboczego pojawi się okno z informacjami dla wybranych obiektów.

4. Z listy rozwijalnej **Stan zatwierdzenia aktualizacji** wybierz **Zatwierdzono**, aby zatwierdzić wybrane aktualizacje, lub **Odrzucono**, aby odrzucić wybrane aktualizacje.

   Domyślna wartość to **Nie zdefiniowano**.

Aktualizacje, dla których ustawiłeś stan **Zatwierdzono**, są umieszczane w kolejce do instalacji.

Aktualizacje, których ustawiony stan **Odrzucono**, są odinstalowywane (jeśli to możliwe) ze wszystkich urządzeń, na których były wcześniej zainstalowane. Dodatkowo, nie zostaną one zainstalowane na innych urządzeniach w przyszłości.

Niektórych uaktualnień dla aplikacji firmy Kaspersky nie można odinstalować. Jeśli ich ustawiony stan to **Odrzucono**, Kaspersky Security Center nie odinstaluje tych uaktualnień z urządzeń, na których były wcześniej zainstalowane. Jednakże te uaktualnienia nigdy nie zostaną zainstalowane na innych urządzeniach w przyszłości. Jeśli nie można odinstalować aktualizacji dla aplikacji Kaspersky, ta informacja zostanie wyświetlona w oknie właściwości aktualizacji: w panelu **Sekcje** wybierz **Ogólne**, a w obszarze roboczym ta informacja pojawi się w sekcji **Wymagania instalacyjne**. Jeśli ustawisz stan **Odrzucono** dla aktualizacji oprogramowania firm trzecich, te aktualizacje nie zostaną zainstalowane na urządzeniach, dla których planowane było ich zainstalowanie, ale jeszcze nie zostały zainstalowane. Uaktualnienia pozostaną na urządzeniach, na których zostały już zainstalowane. Jeśli musisz je usunąć, możesz je usunąć ręcznie lokalnie.

Synchronizacja aktualizacji z Windows Update z Serwerem administracyjnym

Jeśli w oknie **Ustawienia zarządzania aktualizacjami** kreatora wstępnej konfiguracji wybrano **Użyj Serwera administracyjnego jako serwera WSUS**, zadanie synchronizacji Windows Update zostanie utworzone automatycznie. Zadanie można uruchomić w folderze **Zadania**. Funkcja aktualizacji oprogramowania Microsoft jest dostępna tylko po pomyślnym zakończeniu zadania **Wykonaj synchronizację Windows Update**.

Aktualizacje oprogramowania Microsoft mogą przekraczać 10 GB. Upewnij się, że baza danych Serwera administracyjnego jest w stanie pomieścić takie woluminy; w przeciwnym razie zadanie **Wykonaj synchronizację Windows Update** zakończy się niepowodzeniem. Baza danych Microsoft SQL Express nie jest obsługiwana dla zadania **Wykonaj synchronizację Windows Update**.

Zadanie **Wykonaj synchronizację Windows Update** pobiera tylko metadane z serwerów Microsoft. Jeśli sieć nie wykorzystuje serwera WSUS, każde urządzenie klienckie pobiera aktualizacje Microsoft niezależnie z zewnętrznych serwerów.

W celu utworzenia zadania synchronizacji Windows Updates z Serwerem administracyjnym:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.

2. Kliknij przycisk **Akcje dodatkowe** i z listy rozwijalnej wybierz **Konfiguruj synchronizację z usługą Windows Update**.

   Kreator tworzy zadanie **Wykonaj synchronizację Windows Update** wyświetlane w folderze **Zadania**.

   Zostanie uruchomiony kreator tworzenia zadania pobierania danych Centrum aktualizacji systemu Windows. Postępuj zgodnie z instrukcjami kreatora.

Zadanie synchronizacji Windows Update możesz również utworzyć w folderze **Zadania**, klikając **Utwórz zadanie**.

Microsoft regularnie usuwa przestarzałe aktualizacje z serwerów firmy, więc liczba bieżących aktualizacji zawsze mieści się pomiędzy 200 000, a 300 000. Aby zmniejszyć wykorzystanie miejsca na dysku i rozmiar bazy danych, Kaspersky Security Center usuwa nieaktualne aktualizacje, których nie ma już na serwerach aktualizacji firmy Microsoft.

Podczas wykonywania zadania **Wykonaj synchronizację Windows Update** aplikacja pobiera listę bieżących aktualizacji z serwera aktualizacji Microsoft. Następnie, Kaspersky Security Center tworzy listę aktualizacji, które są przestarzałe. Przy kolejnym uruchomieniu zadania **Wyszukiwanie luk i wymaganych aktualizacji** program Kaspersky Security Center oznaczy wszystkie przestarzałe aktualizacje i ustawi dla nich czas usunięcia. Przy kolejnym uruchomieniu zadania **Wykonaj synchronizację Windows Update** wszystkie aktualizacje, które zostały oznaczone do usunięcia 30 dni wcześniej, zostaną usunięte. Kaspersky Security Center sprawdza także obecność przestarzałych aktualizacji, które zostały oznaczone do usunięcia ponad 180 dni temu, a następnie usuwa te starsze aktualizacje.

Jeśli zadanie **Wykonaj synchronizację Windows Update** zostanie zakończone, a przestarzałe aktualizacje zostaną usunięte, baza danych może wciąż posiadać kody skrótów odnoszące się do plików usuniętych aktualizacji, a także odpowiednie pliki w plikach %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (jeśli zostały pobrane wcześniej). Możesz uruchomić zadanie **Konserwacja Serwera administracyjnego**, aby usunąć te przestarzałe wpisy z bazy danych oraz odpowiednich plików.

Krok 1. Określanie, czy zmniejszyć ruch sieciowy

Jeśli Kaspersky Security Center synchronizuje aktualizacje z Microsoft Windows Update Servers, informacje o wszystkich plikach są zapisywane w bazie danych Serwera administracyjnego. Wszystkie pliki niezbędne dla aktualizacji zostają także pobrane na dysk podczas interakcji z Windows Update Agent. Kaspersky Security Center zapisuje informacje o plikach aktualizacji ekspresowej w bazie danych i pobiera je, gdy jest to konieczne. Pobranie plików aktualizacji ekspresowej prowadzi do zmniejszenia wolnego miejsca na dysku.

Aby uniknąć zmniejszenia ilości wolnego miejsca na dysku oraz zmniejszyć ruch sieciowy, możesz wyłączyć opcję **Pobierz ekspresowe pliki instalacyjne**.

Jeśli ta opcja jest zaznaczona, pliki aktualizacji ekspresowej są pobierane podczas wykonywania zadania. Domyślnie ta opcja nie jest zaznaczona.

Krok 2. Aplikacje

W tej sekcji możesz wybrać aplikacje, dla których zostaną pobrane uaktualnienia.

Jeśli pole **Wszystkie aplikacje** jest zaznaczone, uaktualnienia będą pobierane dla wszystkich istniejących aplikacji, a także dla wszystkich aplikacji, które mogą zostać wydane w przyszłości.

Domyślnie zaznaczone jest pole **Wszystkie aplikacje**.

Krok 3. Kategorie uaktualnień

W tej sekcji możesz wybrać kategorie uaktualnień, które będą pobierane na Serwer administracyjny.

Jeśli pole **Wszystkie kategorie** jest zaznaczone, uaktualnienia będą pobierane dla wszystkich istniejących kategorii uaktualnień, a także dla wszystkich kategorii, które mogą pojawić się w przyszłości.

Domyślnie zaznaczone jest pole **Wszystkie kategorie**.

Krok 4. Języki aktualizacji

W tym oknie możesz wybrać wersję językową aktualizacji, które są pobierane na Serwer administracyjny. Wybierz jedną z następujących opcji pobierania wersji językowych aktualizacji:

- **Pobierz wszystkie języki, wraz z nowymi**

  Jeśli ta opcja jest zaznaczona, na Serwer administracyjny zostaną pobrane wszystkie wersje językowe aktualizacji. Domyślnie opcja ta jest zaznaczona.

- **Pobierz wybrane języki**

  Jeśli ta opcja jest zaznaczona, z listy wersji językowych możesz wybrać te, które powinny zostać pobrane na Serwer administracyjny.

Krok 5. Wybieranie konta do uruchamiania zadania

W oknie **Wybieranie konta do uruchomienia zadania** możesz określić, które konto ma być używane podczas uruchamiania zadania. Wybierz jedną z następujących opcji:

- **Konto domyślne**

  Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

  Domyślnie opcja ta jest zaznaczona.

- **Określ konto**

  Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

  - **Konto**

    Konto, z poziomu którego zadanie jest uruchamiane.

  - **Hasło**

    Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

Krok 6. Konfigurowanie terminarza uruchamiania zadania

W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- **Zaplanowane uruchomienie:**

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - **Co N godzin**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

- **Co N dni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

  Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N tygodni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

  Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

- **Co N minut**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

  Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Raz**

  Zadanie zostanie uruchomione raz, w określonym dniu i o określonej godzinie (domyślnie w dniu utworzenia zadania).

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

Krok 7. Definiowanie nazwy zadania

W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych (`"*<>?\:|`). Wartość domyślna to *Wykonaj synchronizację Windows Update*.

Krok 8. Kończenie tworzenia zadania

W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zakończyć pracę kreatora.

Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Nowo utworzone zadanie synchronizacji Windows Update pojawi się na liście zadań, w folderze **Zadania**.

Ręczne instalowanie uaktualnień na urządzeniach

Jeśli na stronie **Ustawienia zarządzania aktualizacjami** kreatora wstępnej konfiguracji wybrano **Wyszukaj i zainstaluj wymagane aktualizacje**, zadanie *instalacji wymaganych aktualizacji i napraw luk* zostanie utworzone automatycznie. Zadanie można uruchomić lub zatrzymać w folderze **Zarządzane urządzenia**, na zakładce **Zadania**.

Jeśli w kreatorze wstępnej konfiguracji wybrano **Wyszukaj wymagane aktualizacje**, możesz zainstalować aktualizacje oprogramowania na urządzeniach klienckich poprzez zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.

Możesz wykonać jedną z następujących czynności:

- Utworzyć zadanie instalowania aktualizacji.
- Dodać regułę instalowania aktualizacji do istniejącego zadania instalowania aktualizacji.
- W ustawieniach istniejącego zadania instalacji aktualizacji skonfiguruj testową instalację aktualizacji.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Instalowanie aktualizacji poprzez utworzenie zadania instalacji

Możesz wykonać jedną z następujących czynności:

- Utworzyć zadanie instalowania pewnych aktualizacji.
- Wybierz aktualizację i utwórz zadanie jej instalowania i podobnych aktualizacji.

W celu zainstalowania określonych aktualizacji:

1. W folderze **Zaawansowane → Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.
2. W obszarze roboczym wybierz aktualizacje, które chcesz zainstalować.
3. Wykonaj jedną z poniższych czynności:
   - Prawym klawiszem myszy kliknij wybrane aktualizacje na liście, a następnie wybierz **Zainstaluj aktualizację → Nowe zadanie**.
   - Kliknij odnośnik **Zainstaluj aktualizację (utwórz zadanie)** w oknie z informacjami dla wybranych aktualizacji.

4. Dokonaj wyboru w wyświetlonym oknie z pytaniem o zainstalowanie wszystkich poprzednich aktualizacji aplikacji. Kliknij **Tak**, jeśli wyrażasz zgodę na instalację kolejnych wersji aplikacji, jeśli jest to wymagane do zainstalowania wybranych aktualizacji. Kliknij **Nie**, jeśli chcesz aktualizować aplikację w sposób prosty, bez instalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

   Zostanie uruchomiony kreator tworzenia zadania naprawy luk oraz instalacji aktualizacji. Postępuj zgodnie z krokami kreatora.

5. W oknie **Wybieranie sposobu ponownego uruchomienia systemu operacyjnego** wybierz działanie, jakie zostanie wykonane, gdy system operacyjny na urządzeniach klienckich musi zostać uruchomiony ponownie po działaniu:

   - **Nie uruchamiaj ponownie urządzenia**

     Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

   - **Uruchom urządzenie ponownie**

     Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

   - **Pytaj użytkownika o akcję**

     Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

     Domyślnie opcja ta jest zaznaczona.

     - **Ponawiaj pytanie co (min)**

       Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

       Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

       Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

     - **Uruchom ponownie po (min)**

       Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

       Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

   - **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

     Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

Domyślnie opcja ta jest wyłączona.

6. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- **Zaplanowane uruchomienie:**

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - **Co N godzin**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

  - **Co N dni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

    Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Co N tygodni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

    Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

  - **Co N minut**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

    Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

  - **Codziennie (czas letni nie jest obsługiwany)**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

    Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

    Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

  - **Co tydzień**

    Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

- Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
- Kliknij ikonę sortowania, aby posortować zadania według nazwy.

  Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
- Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

7. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

8. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

   Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu działania kreatora, zadanie **Zainstaluj wymagane aktualizacje i napraw luki** pojawi się w folderze **Zadania**.

We właściwościach zadania *instalacji wymaganych aktualizacj* i naprawy luk można zezwolić na automatyczną instalację komponentów systemu (wymagania wstępne) przed instalacją aktualizacji. Jeśli ta opcja jest włączona, wszystkie wymagane komponenty systemu zostaną zainstalowane przed aktualizacją. Lista wymaganych komponentów znajduje się we właściwościach aktualizacji.

We właściwościach zadania *instalacji wymaganych aktualizacji* i naprawy luk można zezwolić na instalację aktualizacji, co spowoduje zaktualizowanie aplikacji do nowej wersji.

Jeśli w ustawieniach zadania znajdują się reguły instalacji aktualizacji firm trzecich, Serwer administracyjny pobierze wszystkie odpowiednie aktualizacje ze stron internetowych producentów. Aktualizacje są zapisywane w repozytorium Serwera administracyjnego, a następnie są rozsyłane i instalowane na urządzeniach, na których powinny zostać zastosowane.

Jeśli w ustawieniach zadania znajdują się reguły instalacji aktualizacji Microsoft, a Serwer administracyjny pełni rolę serwera WSUS, Serwer administracyjny pobierze wszystkie niezbędne aktualizacje do repozytorium, a następnie roześle je na zarządzane urządzenia. Jeśli sieć nie wykorzystuje serwera WSUS, każde urządzenie klienckie pobiera aktualizacje Microsoft niezależnie z zewnętrznych serwerów.

W celu zainstalowania określonej aktualizacji i jej podobnych:

1. W folderze **Zaawansowane → Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.

2. W obszarze roboczym wybierz aktualizację, którą chcesz zainstalować.

3. Kliknij przycisk **Uruchom Kreatora instalacji aktualizacji**.

   Zostanie uruchomiony kreator instalacji aktualizacji.

   > Funkcje Kreator naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

   Postępuj zgodnie z krokami kreatora.

4. W oknie **Wyszukaj istniejące zadania instalacji aktualizacji** określ następujące ustawienia:

   - **Wyszukaj zadania, które instalują tę aktualizację**

     Jeśli ta opcja jest włączona, kreator instalacji aktualizacji wyszukuje istniejące zadania, które instalują wybraną aktualizację.

     Jeśli ta opcja jest wyłączona lub wyszukiwanie nie znajdzie stosowanych zadań, kreator instalacji aktualizacji wyświetli pytanie o utworzenie reguły lub zadania instalacji aktualizacji.

     Domyślnie opcja ta jest włączona.

   - **Zatwierdź instalację aktualizacji**

     Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

     Domyślnie opcja ta jest wyłączona.

5. Jeśli wybierzesz wyszukiwanie istniejących zadań instalacji aktualizacji i wyszukiwanie znajdzie zadania, możesz przejrzeć właściwości tych zadań lub uruchomić je ręcznie. Dalsze działania nie są wymagane.

   W przeciwnym razie kliknij przycisk **Nowe zadanie instalacji aktualizacji**.

6. Wybierz typ reguły instalacji, która ma zostać dodana do nowego zadania, a następnie kliknij przycisk **Zakończ**.

7. Dokonaj wyboru w wyświetlonym oknie z pytaniem o zainstalowanie wszystkich poprzednich aktualizacji aplikacji. Kliknij **Tak**, jeśli wyrażasz zgodę na instalację kolejnych wersji aplikacji, jeśli jest to wymagane do zainstalowania wybranych aktualizacji. Kliknij **Nie**, jeśli chcesz aktualizować aplikację w sposób prosty, bez instalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

   Zostanie uruchomiony kreator tworzenia zadania naprawy luk oraz instalacji aktualizacji. Postępuj zgodnie z krokami kreatora.

8. W oknie **Wybieranie sposobu ponownego uruchomienia systemu operacyjnego** wybierz działanie, jakie zostanie wykonane, gdy system operacyjny na urządzeniach klienckich musi zostać uruchomiony ponownie po działaniu:

   - **Nie uruchamiaj ponownie urządzenia**

     Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

   - **Uruchom urządzenie ponownie**

     Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

   - **Pytaj użytkownika o akcję**

     Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

     Domyślnie opcja ta jest zaznaczona.

     - **Ponawiaj pytanie co (min)**

       Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

       Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

       Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

     - **Uruchom ponownie po (min)**

       Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

       Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

9. W oknie **Wybierz urządzenia, do których zostanie przypisane zadanie** wybierz jedną z następujących opcji:

   - **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**

     Zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

     Na przykład, możesz chcieć użyć tej opcji w zadaniu instalowania Agenta sieciowego na nieprzypisanych urządzeniach.

   - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

     Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

     Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

   - **Przypisz zadanie do wyboru urządzeń**

     Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

     Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

10. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

    - **Zaplanowane uruchomienie:**

      Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

      - **Co N godzin**

        Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

        Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

      - **Co N dni**

        Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

        Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

      - **Co N tygodni**

        Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

        Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

      - **Co N minut**

        Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

        Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

      - **Codziennie (czas letni nie jest obsługiwany)**

        Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

        Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

        Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

      - **Co tydzień**

        Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

      - **Według dni tygodnia**

        Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

        Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

      - **Co miesiąc**

        Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

        W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie** (zaznaczone domyślnie)

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

11. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

12. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

    Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu działania kreatora, zadanie **Zainstaluj wymagane aktualizacje i napraw luki** jest tworzone i wyświetlane w folderze **Zadania**.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Aktualizacja do nowej wersji aplikacji może spowodować problemy z działaniem niektórych aplikacji na urządzeniach.

Instalowanie aktualizacji poprzez dodanie reguły do istniejącego zadania instalacji

W celu zainstalowania aktualizacji poprzez dodanie reguły do istniejącego zadania instalacji:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.

2. W obszarze roboczym wybierz aktualizację, którą chcesz zainstalować.

3. Kliknij przycisk **Uruchom Kreatora instalacji aktualizacji**.

   Zostanie uruchomiony kreator instalacji aktualizacji.

   > Funkcje Kreator naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

   Postępuj zgodnie z krokami kreatora.

4. W oknie **Wyszukaj istniejące zadania instalacji aktualizacji** określ następujące ustawienia:

   - **Wyszukaj zadania, które instalują tę aktualizację**

     Jeśli ta opcja jest włączona, kreator instalacji aktualizacji wyszukuje istniejące zadania, które instalują wybraną aktualizację.

     Jeśli ta opcja jest wyłączona lub wyszukiwanie nie znajdzie stosowanych zadań, kreator instalacji aktualizacji wyświetli pytanie o utworzenie reguły lub zadania instalacji aktualizacji.

     Domyślnie opcja ta jest włączona.

   - **Zatwierdź instalację aktualizacji**

     Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

     Domyślnie opcja ta jest wyłączona.

5. Jeśli wybierzesz wyszukiwanie istniejących zadań instalacji aktualizacji i wyszukiwanie znajdzie zadania, możesz przejrzeć właściwości tych zadań lub uruchomić je ręcznie. Dalsze działania nie są wymagane.

   W innej sytuacji kliknij przycisk **Dodaj regułę instalacji aktualizacji**.

6. Wybierz zadanie, do którego chcesz dodać regułę, a następnie kliknij przycisk **Dodaj regułę**.

   Możesz także przejrzeć właściwości istniejących zadań, uruchomić je ręcznie lub utworzyć nowe zadanie.

7. Wybierz typ reguły, która zostanie dodana do wybranego zadania, a następnie kliknij przycisk **Zakończ**.

8. Dokonaj wyboru w wyświetlonym oknie z pytaniem o zainstalowanie wszystkich poprzednich aktualizacji aplikacji. Kliknij **Tak**, jeśli wyrażasz zgodę na instalację kolejnych wersji aplikacji, jeśli jest to wymagane do zainstalowania wybranych aktualizacji. Kliknij **Nie**, jeśli chcesz aktualizować aplikację w sposób prosty, bez instalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

Nowa reguła instalacji aktualizacji zostanie dodana do istniejącego zadania **Instalacja wymaganych aktualizacji i naprawa luk**.

Konfigurowanie testowej instalacji aktualizacji

W celu skonfigurowania testowej instalacji aktualizacji:

1. W drzewie konsoli wybierz zadanie **Zainstaluj wymagane aktualizacje i napraw luki** znajdujące się w folderze **Zarządzane urządzenia**, na zakładce **Zadania**.

2. Z menu kontekstowego zadania wybierz **Właściwości**.

   Zostanie otwarte okno właściwości **Zainstaluj wymagane aktualizacje i napraw luki**.

3. W oknie właściwości zadania, w sekcji **Instalacja testowa** wybierz jedną z opcji dostępnych dla instalacji testowej:

   - **Nie skanuj**. Wybierz tę opcję, jeśli nie chcesz przeprowadzać testowej instalacji aktualizacji.

   - **Uruchom skanowanie na wybranych urządzeniach**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na wybranych urządzeniach. Kliknij przycisk **Dodaj** i wybierz urządzenia, na których chcesz przeprowadzić testową instalację aktualizacji.

   - **Uruchom skanowanie na urządzeniach w określonej grupie**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na grupach urządzeń. W polu **Określ grupę testową** określ grupę urządzeń, na których chcesz przeprowadzić instalację testową.

   - **Uruchom skanowanie na określonym procencie urządzeń**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na określonej liczbie urządzeń. W polu **Procentowy udział urządzeń testowych z wszystkich urządzeń docelowych** określ procentową ilość urządzeń, na których chcesz przeprowadzić testową instalację aktualizacji.

4. Po wybraniu dowolnej opcji, za wyjątkiem **Nie skanuj**, w polu **Czas na podjęcie decyzji, jeśli instalacja ma być kontynuowana, w godzinach** określ liczbę godzin, jaka powinna upłynąć od testowej instalacji aktualizacji do momentu uruchomienia instalacji aktualizacji na wszystkich urządzeniach.

Konfigurowanie aktualizacji systemu Windows w zasadzie Agenta sieciowego

W celu skonfigurowania aktualizacji systemu Windows w zasadzie Agenta sieciowego:

1. W drzewie konsoli wybierz **Zarządzane urządzenia**.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Wybierz zasadę Agenta sieciowego.

4. Z otwartego menu kontekstowego zasady wybierz **Właściwości**.

   Zostanie otwarte okno właściwości zasady Agenta sieciowego.

5. W panelu **Sekcje** wybierz **Aktualizacje oprogramowania i luki**.

6. Zaznacz opcję **Użyj Serwera administracyjnego jako serwera WSUS**, aby pobierać aktualizacje systemu Windows na Serwer administracyjny, a następnie rozsyłać je na urządzenia klienckie przy użyciu Agenta sieciowego.

   Jeśli ta opcja nie jest zaznaczona, aktualizacje systemu Windows nie są pobierane na Serwer administracyjny. W tym przypadku urządzenia klienckie pobierają aktualizacje systemu Windows bezpośrednio z serwerów firmy Microsoft.

7. Wybierz zestaw aktualizacji, które użytkownicy mogą zainstalować na swoich urządzeniach ręcznie, korzystając z Windows Update.

   Na urządzeniach działających pod kontrolą systemu Windows 10, jeśli usługa Windows Update już wykryła aktualizacje dla urządzenia, nowa opcja, którą wybierzesz w sekcji **Zezwalaj użytkownikom na zarządzanie instalowaniem aktualizacji Windows Update**, zostaną zastosowane dopiero po zainstalowaniu wykrytych aktualizacji.

   Wybierz element z listy rozwijalnej:

   - **Zezwalaj użytkownikom na instalację wszystkich dostępnych aktualizacji Windows Update**

     Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach.

     Wybierz tę opcję, jeśli nie chcesz uczestniczyć w instalacji aktualizacji.

     Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

   - **Zezwalaj użytkownikom na instalację wszystkich zatwierdzonych aktualizacji Windows Update**

     Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach i które zostały zatwierdzone przez Ciebie.

     Na przykład, możesz chcieć najpierw sprawdzić instalację aktualizacji w środowisku testowym i upewnić się, że nie wpływają negatywnie na działanie urządzeń, a następnie zezwolić na instalację tylko tych zatwierdzonych aktualizacji.

     Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

   - **Nie zezwalaj użytkownikom na instalowanie aktualizacji Windows Update**

     Użytkownicy nie mogą ręcznie zainstalować aktualizacji Microsoft Windows Update na swoich urządzeniach. Wszystkie stosowane aktualizacje są instalowane w sposób skonfigurowany przez Ciebie.

     Wybierz tę opcję, jeśli chcesz zarządzać instalacją aktualizacji w sposób scentralizowany.

     Na przykład, możesz chcieć zoptymalizować terminarz aktualizacji, aby sieć nie została przeciążona. Możesz skonfigurować terminarz aktualizacji po godzinach, aby nie przeszkadzały w pracy użytkowników.

8. Wybierz tryb szukania aktualizacji systemu Windows:

   - **Aktywny**

     Jeśli ta opcja jest zaznaczona, Serwer administracyjny z pomocą Agenta sieciowego przesyła żądanie z Agenta Windows Update na urządzeniu klienckim do źródła uaktualnień: Serwery Windows Update lub WSUS. Następnie Agent sieciowy przesyła informacje z usługi Windows Update Agent do Serwera administracyjnego.

     Opcja zaczyna działać tylko wtedy, gdy zaznaczona jest opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

     Domyślnie opcja ta jest zaznaczona.

   - **Pasywny**

     Jeżeli ta opcja jest zaznaczona, Agent sieciowy co jakiś czas przesyła informacje od Serwera administracyjnego dotyczące aktualizacji pobranych przy ostatniej synchronizacji agenta usługi Windows Update ze źródłem uaktualnień. Jeśli nie zostanie przeprowadzona synchronizacja agenta usługi Windows Update ze źródłem uaktualnień, informacje o aktualizacjach Serwera administracyjnego będą przestarzałe.

     Wybierz tę opcję, jeśli chcesz uzyskać aktualizacje z pamięci podręcznej źródła uaktualnień.

   - **Wyłączony**

     Jeśli ta opcja jest zaznaczona, Serwer administracyjny nie żąda informacji dotyczących aktualizacji.

     Wybierz tę opcję, gdy, na przykład, chcesz najpierw przetestować aktualizacje na swoim lokalnym urządzeniu.

9. Zaznacz opcję **Skanuj pliki wykonywalne w poszukiwaniu luk podczas ich uruchamiania**, jeśli chcesz skanować pliki wykonywalne w poszukiwaniu luk podczas uruchamiania plików.

10. Upewnij się, że edycja jest zablokowana dla wszystkich zmienionych ustawień. W przeciwnym razie zmiany nie mają zastosowania.

11. Kliknij **Zastosuj**.

Eliminowanie luk w oprogramowaniu innych firm

Ta sekcja opisuje funkcje Kaspersky Security Center, które dotyczą eliminowania luk w oprogramowaniu zainstalowanym na zarządzanych urządzeniach.

Scenariusz: Wyszukiwanie i usuwanie luk w oprogramowaniu firm trzecich

Ta sekcja zawiera scenariusz wyszukiwania i naprawiania luk na zarządzanych urządzeniach działających pod kontrolą systemu Windows. Możesz znaleźć i naprawić luki w oprogramowaniu w systemie operacyjnym oraz w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft.

Wymagania wstępne

- Kaspersky Security Center zostanie wdrożony w Twojej organizacji.
- W Twojej organizacji znajdują się zarządzane urządzenia działające pod kontrolą systemu Windows.
- Połączenie internetowe w przypadku Serwera administracyjnego jest wymagane, aby można było wykonywać następujące zadania:
  - Sporządzanie listy zalecanych poprawek dla luk w oprogramowaniu firmy Microsoft. Lista jest tworzona i regularnie aktualizowana przez specjalistów z Kaspersky.
  - Naprawianie luk w oprogramowaniu firm trzecich innym niż oprogramowanie firmy Microsoft.

Etapy

Wyszukiwanie i naprawianie luk w oprogramowaniu odbywa się w etapach:

1. **Skanowanie luk w oprogramowaniu zainstalowanym na zarządzanych urządzeniach**

   Aby odszukać luki w oprogramowaniu zainstalowanym na zarządzanych urządzeniach, uruchom zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Kaspersky Security Center pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania.

   Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Jeśli nie uruchamiałeś kreatora, uruchom go teraz lub utwórz zadanie ręcznie.

   Dostępne instrukcje:

   - Konsola administracyjna: Skanowanie aplikacji w poszukiwaniu luk, Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
   - Kaspersky Security Center Web Console: Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji, Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

2. **Analizowanie listy wykrytych luk w oprogramowaniu**

   Przejrzyj listę **Luki w oprogramowaniu** i zdecyduj, które luki mają zostać naprawione. Aby przejrzeć szczegółowe informacje o każdej luce, kliknij nazwę luki na liście. Dla każdej luki na liście możesz także przejrzeć statystyki dotyczące luki na zarządzanych urządzeniach.

   Dostępne instrukcje:

   - Konsola administracyjna: Przeglądanie informacji o lukach w oprogramowaniu, Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach
   - Kaspersky Security Center Web Console: Przeglądanie informacji o lukach w oprogramowaniu, Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach

3. **Konfigurowanie naprawy luk**

   Jeśli luki w oprogramowaniu zostaną wykryte, możesz naprawić luki w oprogramowaniu na zarządzanych urządzeniach, korzystając z zadania *Zainstaluj wymagane aktualizacje i napraw luki* lub zadania *Napraw luki*.

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do aktualizacji i naprawy luk w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft, zainstalowanym na zarządzanych urządzeniach. To zadanie umożliwia zainstalowanie kilku aktualizacji i naprawę kilku luk zgodnie z pewnymi regułami. Pamiętaj, że to zadanie może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami. Aby naprawić luki w oprogramowaniu, zadanie *Zainstaluj wymagane aktualizacje i napraw luki* używa zalecanych aktualizacji oprogramowania.

Zadanie *Napraw luki* nie wymaga opcji licencjonowania dla funkcji Zarządzanie lukami i poprawkami. Aby użyć tego zadania, należy ręcznie określić poprawki użytkownika dla luk w programach innych firm, wymienionych w ustawieniach zadania. Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla programów innych firm.

Możesz uruchomić Kreator naprawiania luk, który tworzy jedno z tych zadań automatycznie, lub możesz utworzyć jedno z tych zadań ręcznie.

Dostępne instrukcje:

- Konsola administracyjna: Wybieranie poprawek użytkownika dla luk w programach innych firm, Naprawianie luk w aplikacjach
- Kaspersky Security Center Web Console: Wybieranie poprawek użytkownika dla luk w programach innych firm, Naprawianie luk w programach innych firm, Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki

4 Konfigurowanie terminarza zadań

Aby upewnić się, że lista luk jest zawsze aktualna, skonfiguruj zadanie *Wyszukiwanie luk i wymaganych aktualizacji* tak, aby było uruchamiane automatycznie od czasu do czasu. Zalecana przeciętna częstotliwość uruchamiania to raz na tydzień.

Jeśli utworzyłeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz skonfigurować terminarz tak, aby zadanie było uruchamiane z tą samą częstotliwością co zadanie *Wyszukiwanie luk i wymaganych aktualizacji* lub rzadziej. Podczas ustawiania terminarza zadania *Napraw luki* należy pamiętać, żeby wybrać poprawki dla oprogramowania Microsoft lub określić poprawki użytkownika dla oprogramowania innych firm za każdym razem przed rozpoczęciem zadania.

Jeśli konfigurujesz terminarz uruchamiania zadania, upewnij się, że zadanie naprawy luki zostanie uruchomione po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

5 Ignorowanie luk w oprogramowaniu (opcjonalne)

Jeśli chcesz, możesz zignorować luki w oprogramowaniu na wszystkich zarządzanych urządzeniach lub tylko na wybranych zarządzanych urządzeniach.

Dostępne instrukcje:

- Konsola administracyjna: Ignorowanie luk w oprogramowaniu
- Kaspersky Security Center Web Console: Ignorowanie luk w oprogramowaniu

6 Uruchamianie zadania naprawy luk

Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Napraw lukę*. Po zakończeniu zadania, upewnij się, że na liście zadań posiada stan *Zakończone pomyślnie*.

7 Utwórz raport dotyczący wyników naprawy luk w oprogramowaniu (opcjonalne)

Aby wyświetlić szczegółowe statystyki dotyczące naprawy luk, wygeneruj Raport o lukach. Raport wyświetla informacje o lukach w oprogramowaniu, które nie zostały naprawione. Dzięki temu możesz wiedzieć o wyszukiwaniu i naprawie luk w programach innych firm, w tym w oprogramowaniu firmy Microsoft, w swojej organizacji.

Dostępne instrukcje:

- Konsola administracyjna: Tworzenie i przeglądanie raportu
- Kaspersky Security Center Web Console: Tworzenie i przeglądanie raportu

8. **Sprawdzanie konfiguracji wyszukiwania i naprawy luk w programach innych firm**

   Upewnij się, że wykonałeś następujące czynności:

   - Uzyskałeś i przejrzałeś listę luk w oprogramowaniu na zarządzanych urządzeniach
   - Zignorowałeś luki w oprogramowaniu, jeśli chciałeś
   - Skonfigurowałeś zadanie naprawy luk
   - Skonfigurowałeś terminarz zadań wyszukiwania i naprawy luk w oprogramowaniu, aby były uruchamianie po kolei
   - Sprawdziłeś, czy zadanie naprawy luk w oprogramowaniu zostało uruchomione

Wyniki

Jeśli utworzyłeś i skonfigurowałeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, luki zostają naprawione na zarządzanych urządzeniach automatycznie. Jeśli zadanie zostaje uruchomione, zestawia listę dostępnych aktualizacji oprogramowania z regułami określonymi w ustawieniach zadania. Wszystkie aktualizacje oprogramowania, które spełniają kryteria w regułach, zostaną pobrane do repozytorium Serwera administracyjnego i zostaną zainstalowane w celu naprawy luk w oprogramowaniu.

Jeśli utworzyłeś zadanie *Napraw luki*, naprawione zostaną tylko luki w oprogramowaniu firmy Microsoft.

Informacje o wyszukiwaniu i eliminowaniu luk w oprogramowaniu

Kaspersky Security Center wykrywa i naprawia luki w oprogramowaniu na zarządzanych urządzeniach działających pod kontrolą systemów operacyjnych z rodziny Microsoft Windows. Luki są wykrywane w systemie operacyjnym i w oprogramowaniu innych firm, w tym w oprogramowaniu firmy Microsoft.

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), przy czym funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Wyszukiwanie luk w oprogramowaniu

Aby znaleźć luki w oprogramowaniu, Kaspersky Security Center wykorzystuje znaki charakterystyczne z bazy danych znanych zagrożeń. Ta baza danych jest tworzona przez specjalistów z Kaspersky. Zawiera informacje o lukach, takie jak opis luki, data wykrycia luki, priorytet luki. Szczegóły dotyczące luk w oprogramowaniu można znaleźć na stronie internetowej Kaspersky.

Kaspersky Security Center wykorzystuje zadanie *Wyszukiwanie luk i wymaganych aktualizacji* do wykrywania luk w oprogramowaniu.

W niektórych przypadkach luki w zabezpieczeniach wykryte w systemie operacyjnym Microsoft Windows można naprawić, korzystając z jednej z następujących metod:

- Instalowanie aktualizacji systemu operacyjnego.
- Aktualizacja systemu operacyjnego do nowszej wersji (na przykład z Windows 10 do Windows 11).

W tym scenariuszu Kaspersky Security Center wyświetla dwa wpisy dla tej samej luki w zabezpieczeniach.

Naprawianie luk w oprogramowaniu

Aby naprawić luki w oprogramowaniu, Kaspersky Security Center używa aktualizacji oprogramowania opublikowanych przez producentów oprogramowania. Metadane aktualizacji oprogramowania są pobierane z repozytorium Serwera administracyjnego w wyniku uruchomienia następującego zadania:

- *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. To zadanie jest przeznaczone do pobrania metadanych aktualizacji dla Kaspersky i oprogramowania firm trzecich. To zadanie jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Możesz ręcznie utworzyć zadanie Pobierz uaktualnienia do repozytorium Serwera administracyjnego.
- *Wykonaj synchronizację Windows Update*. To zadanie jest przeznaczone do pobrania metadanych aktualizacji dla oprogramowania firmy Microsoft.

Aktualizacje oprogramowania eliminujące luki mogą być w postaci pełnych pakietów dystrybucyjnych lub poprawek. Aktualizacje oprogramowania, które eliminują luki w oprogramowaniu, nazywane są *poprawkami*. *Zalecane poprawki* to takie poprawki, które są zalecane do zainstalowania przez specjalistów z Kaspersky. *Poprawki użytkownika* to takie poprawki, które są ręcznie określane do zainstalowania przez użytkowników. Aby zainstalować poprawkę użytkownika, należy utworzyć pakiet instalacyjny zawierający tę poprawkę.

Jeśli posiadasz licencję dla Kaspersky Security Center z funkcją Zarządzanie lukami i poprawkami, aby usunąć luki w oprogramowaniu, możesz użyć zadania *Zainstaluj wymagane aktualizacje i napraw luki*. To zadanie automatycznie eliminuje kilka luk poprzez zainstalowanie zalecanych poprawek. Dla tego zadania można ręcznie skonfigurować pewne reguły do naprawy kilku luk.

Jeśli nie posiadasz licencji dla Kaspersky Security Center z funkcją Zarządzanie lukami i poprawkami, aby usunąć luki w oprogramowaniu, możesz użyć zadania *Napraw luki*. Korzystając z tego zadania, możesz wyeliminować luki poprzez zainstalowanie zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla innych programów innych firm.

Ze względów bezpieczeństwa wszelkie aktualizacje oprogramowania innych firm, które instalujesz za pomocą funkcji Zarządzanie lukami i poprawkami, są automatycznie skanowane w poszukiwaniu szkodliwego oprogramowania przez technologie firmy Kaspersky. Technologie te są używane do automatycznego sprawdzania plików i obejmują skanowanie antywirusowe, analizę statyczną, analizę dynamiczną, analizę zachowania w środowisku sandbox i uczenie maszynowe.

Eksperci firmy Kaspersky nie przeprowadzają ręcznej analizy aktualizacji oprogramowania innych firm, które są instalowane przez funkcję Zarządzanie lukami i poprawkami. Ponadto eksperci z firmy Kaspersky nie wyszukują luk (znanych lub nieznanych) ani nieudokumentowanych funkcji w takich aktualizacjach, a także nie przeprowadzają innych rodzajów analizy aktualizacji innych, niż określone w powyższym akapicie.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Aby naprawić niektóre luki w oprogramowaniu, należy zaakceptować Umowę licencyjną użytkownika końcowego (EULA) dla instalowanego oprogramowania, jeśli wymagane jest zaakceptowanie Umowy licencyjnej. Jeśli odrzucisz Umowę licencyjną użytkownika końcowego, luka w oprogramowaniu nie zostanie wyeliminowana.

Przeglądanie informacji o lukach w oprogramowaniu

W celu przejrzenia listy luk wykrytych na urządzeniach klienckich:

W folderze **Zaawansowane → Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.

Strona wyświetla listę luk w aplikacjach wykrytych na zarządzanych urządzeniach.

W celu uzyskania informacji o wybranej luce:

Z menu kontekstowego luki wybierz **Właściwości**.

Zostanie otwarte okno właściwości luki, wyświetlające następujące informacje:

- Aplikacja, w której wykryto lukę.
- Lista urządzeń, na których wykryto lukę.
- Informacje dotyczące naprawy luki.

W celu wyświetlenia raportu o wszystkich wykrytych lukach:

W folderze **Luki w oprogramowaniu** kliknij odnośnik **Wyświetl raport o lukach**.

Zostanie utworzony raport o lukach w aplikacjach zainstalowanych na urządzeniach. Możesz wyświetlić ten raport w węźle z nazwą odpowiedniego Serwera administracyjnego, otwierając zakładkę **Raporty**.

Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach

Statystyki dla każdej luki w oprogramowaniu możesz przejrzeć na zarządzanych urządzeniach. Statystyki są przedstawiane w postaci wykresu. Wykres wyświetla liczbę urządzeń z następującymi stanami:

- *Zignorowano na: <liczba urządzeń>*. Stan jest przypisywany, jeśli we właściwościach luki ręcznie ustawiono opcję ignorowania luki.
- *Naprawiono na: <liczba urządzeń>*. Ten stan jest przypisywany, jeśli zadanie naprawy luki zostało zakończone pomyślnie.
- *Naprawa zaplanowana na: <liczba urządzeń>*. Stan jest przypisywany, jeśli utworzono zadanie naprawy luki, ale zadanie nie zostało jeszcze wykonane.
- *Zastosowano poprawkę na: <liczba urządzeń>*. Stan jest przypisywany, jeśli ręcznie wybrano aktualizację oprogramowania do naprawy luki, ale ta aktualizacja oprogramowania nie naprawiła luki.
- *Naprawa wymagana na: <liczba urządzeń>*. Ten stan jest przypisywany, jeśli luka została naprawiona tylko na niektórych zarządzanych urządzeniach i wymagana jest naprawa luki na większej liczbie zarządzanych urządzeń.

W celu sprawdzenia statystyk dotyczących luki na zarządzanych urządzeniach:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.

   Strona wyświetla listę luk w aplikacjach wykrytych na zarządzanych urządzeniach.

2. Wybierz lukę, dla której chcesz przejrzeć statystyki.

   W sekcji do pracy z wybranym obiektem wyświetlany jest wykres stanów luki. Kliknięcie stanu spowoduje otwarcie listy urządzeń, na których luka posiada wybrany stan.

Skanowanie aplikacji w poszukiwaniu luk

Jeśli skonfigurowano aplikację poprzez Kreator wstępnej konfiguracji, zadanie *Wykrywanie* luk zostanie utworzone automatycznie. Zadanie można zobaczyć w folderze **Zarządzane urządzenia**, na zakładce **Zadania**.

W celu utworzenia zadania wykrywania luk w aplikacjach zainstalowanych na urządzeniach klienckich:

1. W drzewie konsoli wybierz **Zaawansowane** → **Zarządzanie aplikacjami**, a następnie wybierz podfolder **Luki w oprogramowaniu**.
2. W obszarze roboczym wybierz **Akcje dodatkowe** → **Konfiguruj wykrywanie luk**.

   Jeśli zadanie wykrywania luk już istnieje, zostanie wyświetlona zakładka **Zadania** folderu **Zarządzane urządzenia** z wybranym istniejącym zadaniem. W przeciwnym razie zostanie uruchomiony Kreator tworzenia zadania Znajdź luki i wymagane aktualizacje. Postępuj zgodnie z krokami kreatora.

3. W oknie **Wybierz typ zadania** wybierz **Wyszukiwanie luk i wymaganych aktualizacji**.

4. W oknie **Ustawienia** określ ustawienia zadania w następujący sposób:

- **Wyszukaj luki i aktualizacje wymienione przez firmę Microsoft**

  Podczas wyszukiwania luk i aktualizacji program Kaspersky Security Center używa informacji o stosowanych aktualizacjach firmy Microsoft ze źródła uaktualnień Microsoft, które są dostępne w danym momencie.

  Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

  Informacje o opcjonalnych aktualizacjach Microsoft Windows nie są wysyłane do Serwera administracyjnego.

- **Połącz z serwerem aktualizacji, aby zaktualizować dane**

  Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem uaktualnień Microsoft. Następujące serwery mogą pełnić rolę źródeł aktualizacji Microsoft:

  - Serwer administracyjny Kaspersky Security Center (zapoznaj się z ustawieniami zasady Agenta sieciowego)
  - System Windows Server wdrożony w sieci Twojej organizacji wraz z programem Microsoft Windows Server Update Services (WSUS)
  - Serwery aktualizacji Microsoft

  Jeśli ta opcja jest włączona, agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem aktualizacji firmy Microsoft, aby odświeżyć informacje o stosowanych aktualizacjach Microsoft Windows.

  Jeśli ta opcja jest wyłączona, agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła aktualizacji firmy Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia.

  Nawiązywanie połączenia ze źródłem aktualizacji firmy Microsoft może zużywać dużo zasobów. Możesz chcieć wyłączyć tę opcję, jeśli ustawisz regularne nawiązywanie połączenia z tym źródłem uaktualnień w innym zadaniu lub we właściwościach zasady Agenta sieciowego, w sekcji **Aktualizacje oprogramowania i luki**. Jeśli nie chcesz wyłączyć tej opcji, następnie, aby zmniejszyć obciążenie Serwera, możesz skonfigurować terminarz zadania do losowego opóźnienia uruchomienia zadania w ciągu 360 minut.

  Domyślnie opcja ta jest włączona.

Kombinacja następujących opcji ustawień zasady Agenta sieciowego definiuje tryb uzyskiwania aktualizacji:

- Agent usługi Windows Update na zarządzanym urządzeniu łączy się z serwerem aktualizacji w celu pobierania aktualizacji tylko wtedy, gdy opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest włączona we właściwościach zadania *Wyszukiwanie luk i wymaganych aktualizacji*, a opcja **Tryb wyszukiwania aktualizacji systemu Windows** jest ustawiona na **Aktywny** w ustawieniach zasady Agenta sieciowego.

- Jeśli nie potrzebujesz, aby Agent sieciowy nawiązał połączenie ze źródłem aktualizacji systemu Microsoft Windows i pobrał aktualizacje podczas wykonywania zadania *skanowania w poszukiwaniu luk*, możesz ustawić opcję **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, a opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** musi pozostać włączona. Dzięki temu możesz zaoszczędzić zasoby i wykorzystać wcześniej pobrane aktualizacje systemu Windows do skanowania w poszukiwaniu luk w zabezpieczeniach. Możesz użyć trybu pasywnego, jeśli skonfigurujesz otrzymywanie aktualizacji systemu Microsoft Windows w inny sposób. Jeśli odbieranie aktualizacji systemu Microsoft Windows nie zostało skonfigurowane w inny sposób, nie należy ustawiać opcji **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, ponieważ w takim przypadku informacje o aktualizacjach nigdy nie zostaną odebrane.

- Bez względu na stan opcji **Połącz z serwerem aktualizacji, aby zaktualizować dane** (włączona lub wyłączona), jeśli opcja **Tryb wyszukiwania aktualizacji systemu Windows** zostanie ustawiona jako **Wyłączony**, Kaspersky Security Center nie żąda żadnych informacji o aktualizacjach.

- **Wyszukaj luki i aktualizacje innych firm wymienione przez firmę Kaspersky**

  Jeśli ta opcja jest włączona, Kaspersky Security Center wyszukuje luki i wymagane aktualizacje dla aplikacji firm trzecich (aplikacji producentów innych niż Kaspersky i Microsoft) w rejestrze systemu Windows i w folderach określonych pod **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**. Pełna lista obsługiwanych aplikacji firm trzecich jest zarządzana przez Kaspersky.

  Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie szuka luk i wymaganych uaktualnień dla aplikacji firm trzecich. Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft Windows i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

- **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**

  Foldery, w których Kaspersky Security Center wyszukuje aplikacje firm trzecich, które wymagają naprawienia luk i zainstalowania aktualizacji. Możesz użyć zmiennych systemowych.

  Określ foldery, w których zostaną zainstalowane aplikacje. Domyślnie, lista zawiera foldery systemowe, w których instalowana jest większość aplikacji.

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy zapisywanie plików śledzenia jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

5. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

   - **Zaplanowane uruchomienie:**

     Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

     - **Co N godzin**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

       Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

     - **Co N dni**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

       Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

     - **Co N tygodni**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

       Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

     - **Co N minut**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

       Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

     - **Codziennie (czas letni nie jest obsługiwany)**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

       Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

       Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

     - **Co tydzień**

       Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po pobraniu nowych uaktualnień do repozytorium**

  Zadanie jest uruchamiane po pobraniu uaktualnień do repozytorium. Na przykład, możesz użyć tego terminarza dla zadania wyszukiwania luk i wymaganych aktualizacji.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

6. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

7. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

   Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu działania kreatora, zadanie **Wyszukiwanie luk** i wymaganych aktualizacji pojawi się na liście zadań w folderze **Zarządzane urządzenia**, na zakładce **Zadania**.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Po zakończeniu zadania *Wyszukiwanie luk* i wymaganych aktualizacji, Serwer administracyjny wyświetla listę luk wykrytych w aplikacjach zainstalowanych na urządzeniu; wyświetla także wszystkie aktualizacje oprogramowania wymagane do wyeliminowania wykrytych luk.

Jeśli pojawi się błąd agenta usługi Windows Update 0x80240033 „Windows Update Agent error 80240033 ("License terms could not be downloaded.")" („pobranie warunków licencyjnych nie powiodło się"), możesz rozwiązać ten problem poprzez Rejestr systemu Windows.

Serwer administracyjny nie wyświetla listy wymaganych aktualizacji oprogramowania, jeśli uruchamiasz dwa zadania po kolei — zadanie *Wykonaj synchronizację Windows Update* ma wyłączoną opcję **Pobierz pliki instalacji ekspresowej**, a następnie zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Aby przejrzeć listę wymaganych aktualizacji oprogramowania, musisz ponownie uruchomić zadanie *Wyszukiwanie luk i wymaganych aktualizacji*.

Agent sieciowy otrzymuje informacje o wszelkich dostępnych aktualizacjach systemu Windows i aktualizacjach dla innych produktów Microsoft od Windows Update lub Serwera administracyjnego, gdy Serwer administracyjny pełni rolę serwera WSUS. Informacje są przesyłane, gdy aplikacje zostają uruchomione (jeśli jest to dostępne dla zasady) i przy każdym uruchomieniu zadania *Wyszukiwanie luk* i wymaganych aktualizacji na urządzeniach klienckich.

Naprawianie luk w aplikacjach

Jeśli na stronie **Ustawienia zarządzania aktualizacjami** kreatora wstępnej konfiguracji wybrano **Wyszukaj i zainstaluj wymagane aktualizacje**, zadanie *instalacji wymaganych aktualizacji i napraw luk* zostanie utworzone automatycznie. Zadanie jest wyświetlane w obszarze roboczym folderu **Zarządzane urządzenia**, na zakładce **Zadania**.

Jeśli jest inaczej, możesz wykonać jedną z następujących czynności:

- Utwórz zadanie naprawy luk poprzez zainstalowanie dostępnych uaktualnień.
- Dodaj regułę dla naprawy luk do istniejącego zadania naprawy luk.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Naprawianie luk poprzez utworzenie zadania naprawy luk

Możesz wykonać jedną z następujących czynności:

- Utwórz zadanie naprawy kilku luk, które spełniają określone reguły.
- Wybierz lukę i utwórz zadanie naprawy tej luki i podobnych luk.

W celu naprawy luk, które spełniają określone reguły:

1. W drzewie konsoli wybierz Serwer administracyjny na urządzeniach, których luki chcesz naprawić.
2. W menu **Widok** okna głównego aplikacji wybierz **Konfiguruj interfejs**.
3. W oknie, które zostanie otwarte, zaznacz pole wyboru **Wyświetl zarządzanie lukami i poprawkami**, a następnie kliknij przycisk **OK**.
4. W oknie z wiadomością aplikacji kliknij **OK**.
5. Uruchom ponownie Konsolę administracyjną, aby zmiany zostały zastosowane.
6. W drzewie konsoli wybierz folder **Zarządzane urządzenia**.
7. W obszarze roboczym wybierz zakładkę **Zadania**.
8. Kliknij przycisk **Utwórz zadanie**, aby uruchomić Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
9. W oknie **Wybierz typ zadania** wybierz **Zainstaluj wymagane aktualizacje i napraw luki**.

   Jeśli zadanie nie jest wyświetlane, sprawdź, czy Twoje konto ma uprawnienia **Odczyt**, **Modyfikuj** i **Wykonaj** dla obszaru funkcjonalnego **Zarządzanie systemem: Zarządzanie lukami w zabezpieczeniach i poprawkami**. Bez tych praw dostępu nie można utworzyć ani skonfigurować zadania *Zainstaluj wymagane aktualizacje i napraw luki*.
10. W oknie **Ustawienia** określ ustawienia zadania w następujący sposób:

    - **Określ reguły instalacji aktualizacji**

      Te reguły są stosowane do instalacji aktualizacji na urządzeniach klienckich. Jeśli reguły nie zostały określone, zadanie nie zostanie wykonane. Informacje dotyczące działań wykonywanych na regułach znajdziesz w sekcji Reguły instalacji aktualizacji.

    - **Uruchom instalację podczas ponownego uruchamiania lub wyłączania urządzenia**

      Jeśli ta opcja jest włączona, aktualizacje są instalowane po ponownym uruchomieniu lub zamknięciu urządzenia. W innym przypadku aktualizacje są instalowane zgodnie z terminarzem.

      Użyj tej opcji, jeśli instalowanie aktualizacji może wpłynąć na działanie urządzenia.

      Domyślnie opcja ta jest wyłączona.

    - **Zainstaluj wymagane ogólne składniki systemu**

      Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

Domyślnie opcja ta jest wyłączona.

- **Zezwól na instalację nowych wersji aplikacji podczas aktualizacji**

  Jeśli ta opcja jest włączona, aktualizacje są dozwolone, gdy powodują zainstalowanie nowej wersji aplikacji.

  Jeśli ta opcja jest wyłączona, aplikacja nie zostanie zaktualizowana. W takiej sytuacji możesz ręcznie zainstalować nowe wersje aplikacji lub użyć w tym celu innego zadania. Na przykład, możesz użyć tej opcji, jeśli struktura Twojej firmy nie jest obsługiwana przez nową wersję aplikacji lub jeśli chcesz sprawdzić aktualizację w infrastrukturze testowej.

  Domyślnie opcja ta jest włączona.

  > Aktualizowanie aplikacji może spowodować problemy z działaniem powiązanych aplikacji zainstalowanych na urządzeniach klienckich.

- **Pobierz aktualizacje na urządzenie, ale ich nie instaluj**

  Jeśli ta opcja jest włączona, aplikacja pobierze uaktualnienia na urządzenie, ale nie zainstaluje ich automatycznie. Możesz ręcznie zainstalować pobrane aktualizacje.

  Aktualizacje Microsoft są pobierane do folderu systemowego Windows. Aktualizacje aplikacji firm trzecich (aplikacje innych producentów niż Kaspersky i Microsoft) są pobierane do folderu określonego w polu **Pobierz uaktualnienia do**.

  Jeśli ta opcja jest wyłączona, aktualizacje są instalowane na urządzeniu automatycznie.

  Domyślnie opcja ta jest wyłączona.

  - **Pobierz uaktualnienia do**

    Ten folder jest używany do pobierania aktualizacji aplikacji innych firm (aplikacji innych producentów niż Kaspersky i Microsoft).

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy zapisywanie plików śledzenia jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

  - **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

    Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

11. W oknie **Wybieranie sposobu ponownego uruchomienia systemu operacyjnego** wybierz działanie, jakie zostanie wykonane, gdy system operacyjny na urządzeniach klienckich musi zostać uruchomiony ponownie po działaniu:

    - **Nie uruchamiaj ponownie urządzenia**

      Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

    - **Uruchom urządzenie ponownie**

      Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

    - **Pytaj użytkownika o akcję**

      Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

      Domyślnie opcja ta jest zaznaczona.

      - **Ponawiaj pytanie co (min)**

        Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

        Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

        Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

      - **Uruchom ponownie po (min)**

        Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

        Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    - **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

      Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

      Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

      Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

      Domyślnie opcja ta jest wyłączona.

12. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- **Zaplanowane uruchomienie:**

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - **Co N godzin**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

  - **Co N dni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

    Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Co N tygodni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

    Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

  - **Co N minut**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

    Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

  - **Codziennie (czas letni nie jest obsługiwany)**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

    Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

    Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

  - **Co tydzień**

    Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

  - **Według dni tygodnia**

    Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

    Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

  - **Co miesiąc**

    Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

    W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

13. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

14. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

    Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu działania kreatora, zadanie **Zainstaluj wymagane aktualizacje i napraw luki** jest tworzone i wyświetlane w folderze **Zadania**.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Jeśli wyniki zadania zawierają błąd agenta usługi Windows Update 0x80240033 „Windows Update Agent error 80240033 ("License terms could not be downloaded.")" („pobranie warunków licencyjnych nie powiodło się"), możesz rozwiązać ten problem poprzez Rejestr systemu Windows.

W celu naprawy określonej luki i jej podobnych:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.

2. Wybierz lukę, którą chcesz naprawić.

3. Kliknij przycisk **Uruchom kreatora naprawiania luk**.

   Zostanie uruchomiony Kreator naprawiania luk.

   > Funkcje kreatora naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

   Postępuj zgodnie z krokami kreatora.

4. W oknie **Wyszukaj istniejące zadania naprawiania luk** określ następujące parametry:

   - **Pokaż tylko zadania naprawiające tę lukę**

     Jeśli ta opcja jest wyłączona, Kreator naprawiania luk wyszukuje istniejące zadania, które naprawiają wybraną lukę.

     Jeśli ta opcja jest wyłączona lub wyszukiwanie nie znajdzie stosowanych zadań, Kreator naprawiania luk wyświetli pytanie o utworzenie reguły lub zadania naprawy luki.

     Domyślnie opcja ta jest włączona.

   - **Akceptuj aktualizacje, które naprawiają tę lukę**

     Instalacja aktualizacji, które naprawiają lukę, zostanie zaakceptowana. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

     Domyślnie opcja ta jest wyłączona.

5. Jeśli wybierzesz wyszukiwanie istniejących zadań naprawiania luk i wyszukiwanie znajdzie zadania, możesz przejrzeć właściwości tych zadań lub uruchomić je ręcznie. Dalsze działania nie są wymagane.

   W przeciwnym razie kliknij przycisk **Nowe zadanie naprawiania luk**.

6. Wybierz typ reguły naprawiania luki, która ma zostać dodana do nowego zadania, a następnie kliknij przycisk **Zakończ**.

7. Dokonaj wyboru w wyświetlonym oknie z pytaniem o zainstalowanie wszystkich poprzednich aktualizacji aplikacji. Kliknij **Tak**, jeśli wyrażasz zgodę na instalację kolejnych wersji aplikacji, jeśli jest to wymagane do zainstalowania wybranych aktualizacji. Kliknij **Nie**, jeśli chcesz aktualizować aplikację w sposób prosty, bez instalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

   Zostanie uruchomiony kreator tworzenia zadania naprawy luk oraz instalacji aktualizacji. Postępuj zgodnie z krokami kreatora.

8. W oknie **Wybieranie sposobu ponownego uruchomienia systemu operacyjnego** wybierz działanie, jakie zostanie wykonane, gdy system operacyjny na urządzeniach klienckich musi zostać uruchomiony ponownie po działaniu:

   - **Nie uruchamiaj ponownie urządzenia**

     Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

   - **Uruchom urządzenie ponownie**

     Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

   - **Pytaj użytkownika o akcję**

     Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

     Domyślnie opcja ta jest zaznaczona.

     - **Ponawiaj pytanie co (min)**

       Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

       Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

       Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

     - **Uruchom ponownie po (min)**

       Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

       Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

   - **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

     Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

     Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

     Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

     Domyślnie opcja ta jest wyłączona.

9. W oknie **Wybierz urządzenia, do których zostanie przypisane zadanie** wybierz jedną z następujących opcji:

   - **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**

     Zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

     Na przykład, możesz chcieć użyć tej opcji w zadaniu instalowania Agenta sieciowego na nieprzypisanych urządzeniach.

   - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

     Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

     Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

   - **Przypisz zadanie do wyboru urządzeń**

     Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

     Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

10. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

    - **Zaplanowane uruchomienie:**

      Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

      - **Co N godzin**

        Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

        Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

      - **Co N dni**

        Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

        Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N tygodni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

  Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

- **Co N minut**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

  Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

Można wybrać kilka dni tygodnia.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

11. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

12. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

    Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu działania kreatora, zadanie **Zainstaluj wymagane aktualizacje i napraw luki** jest tworzone i wyświetlane w folderze **Zadania**.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Naprawianie luk poprzez dodanie reguły do istniejącego zadania naprawiania luk

W celu naprawienia luki poprzez dodanie reguły do istniejącego zadania naprawiania luk:

1. W folderze **Zaawansowane → Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.

2. Wybierz lukę, którą chcesz naprawić.

3. Kliknij przycisk **Uruchom kreatora naprawiania luk**.

   Zostanie uruchomiony Kreator naprawiania luk.

   > Funkcje kreatora naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

   Postępuj zgodnie z krokami kreatora.

4. W oknie **Wyszukaj istniejące zadania naprawiania luk** określ następujące parametry:

   - **Pokaż tylko zadania naprawiające tę lukę**

     Jeśli ta opcja jest wyłączona, Kreator naprawiania luk wyszukuje istniejące zadania, które naprawiają wybraną lukę.

Jeśli ta opcja jest wyłączona lub wyszukiwanie nie znajdzie stosowanych zadań, Kreator naprawiania luk wyświetli pytanie o utworzenie reguły lub zadania naprawy luki.

Domyślnie opcja ta jest włączona.

- **Akceptuj aktualizacje, które naprawiają tę lukę**

  Instalacja aktualizacji, które naprawiają lukę, zostanie zaakceptowana. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

  Domyślnie opcja ta jest wyłączona.

5. Jeśli wybierzesz wyszukiwanie istniejących zadań naprawiania luk i wyszukiwanie znajdzie zadania, możesz przejrzeć właściwości tych zadań lub uruchomić je ręcznie. Dalsze działania nie są wymagane.

   W innym przypadku kliknij przycisk **Dodaj regułę naprawiania luk do istniejącego zadania**.

6. Wybierz zadanie, do którego chcesz dodać regułę, a następnie kliknij przycisk **Dodaj regułę**.

   Możesz także przejrzeć właściwości istniejących zadań, uruchomić je ręcznie lub utworzyć nowe zadanie.

7. Wybierz typ reguły, która zostanie dodana do wybranego zadania, a następnie kliknij przycisk **Zakończ**.

8. Dokonaj wyboru w wyświetlonym oknie z pytaniem o zainstalowanie wszystkich poprzednich aktualizacji aplikacji. Kliknij **Tak**, jeśli wyrażasz zgodę na instalację kolejnych wersji aplikacji, jeśli jest to wymagane do zainstalowania wybranych aktualizacji. Kliknij **Nie**, jeśli chcesz aktualizować aplikację w sposób prosty, bez instalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

Nowa reguła naprawiania luk zostanie dodana do istniejącego zadania **Instalacja wymaganych aktualizacji i naprawa luk**.

Naprawianie luk w odizolowanej sieci

W tej sekcji opisano kroki, które możesz podjąć, aby usunąć luki w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach podłączonych do serwerów administracyjnych bez dostępu do Internetu.

Scenariusz: Eliminowanie luk w oprogramowaniu innych firm w odizolowanej sieci

Możesz instalować aktualizacje i eliminować luki w oprogramowaniu innych firm zainstalowanym na zarządzanych urządzeniach w odizolowanej sieci. Takie sieci obejmują serwery administracyjne i podłączone do nich zarządzane urządzenia, które nie mają dostępu do Internetu. Aby naprawić luki w takiej sieci, potrzebujesz serwera administracyjnego połączonego z Internetem. Następnie będzie można pobierać poprawki z aktualizacjami przy użyciu serwera administracyjnego z dostępem do Internetu i przesyłać poprawki do odizolowanych serwerów administracyjnych.

Możesz pobrać aktualizacje oprogramowania innych firm wydane przez dostawców oprogramowania, ale nie możesz pobierać aktualizacji oprogramowania firmy Microsoft na odizolowanych serwerach administracyjnych przy użyciu Kaspersky Security Center.

Aby dowiedzieć się, jak działa proces naprawiania luk w odizolowanej sieci, zapoznaj się z opisem i schematem tego procesu.

Wymagania wstępne

Zanim zaczniesz, wykonaj następujące czynności:

1. Przydziel jedno urządzenie do łączenia się z internetem i pobierania poprawek. To urządzenie będzie liczone jako Serwer administracyjny z dostępem do internetu.
2. Zainstaluj Kaspersky Security Center, w wersji co najmniej 14, na następujących urządzeniach:
   - Przydzielone urządzenie, które będzie pełnić rolę serwera administracyjnego z dostępem do Internetu
   - Izolowane urządzenia, które będą działać jako izolowane od Internetu serwery administracyjne (zwane dalej odizolowanymi serwerami administracyjnymi)
3. Upewnij się, że każdy Serwer administracyjny ma: wystarczająco dużo miejsca na dysku do pobierania i przechowywania aktualizacji i poprawek.

Etapy

Instalowanie aktualizacji i eliminowanie luk w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach izolowanych serwerów administracyjnych obejmuje następujące etapy:

1. **Konfigurowanie serwera administracyjnego z dostępem do Internetu**

   Przygotuj swój Serwer administracyjny z dostępem do Internetu do obsługi żądań dotyczących wymaganych aktualizacji oprogramowania innych firm i pobierania poprawek.

2. **Konfigurowanie izolowanych Serwerów administracyjnych**

   Przygotuj odizolowane serwery administracyjne, dzięki czemu mogą tworzyć listy wymaganych aktualizacji i obsługiwać poprawki pobrane przez serwer administracyjny z dostępem do Internetu. Po skonfigurowaniu odizolowane serwery administracyjne nie próbują już pobierać poprawek z Internetu. Zamiast tego uzyskują aktualizacje przez poprawki.

3. **Przesyłanie poprawek i instalowanie aktualizacji na odizolowanych serwerach administracyjnych**

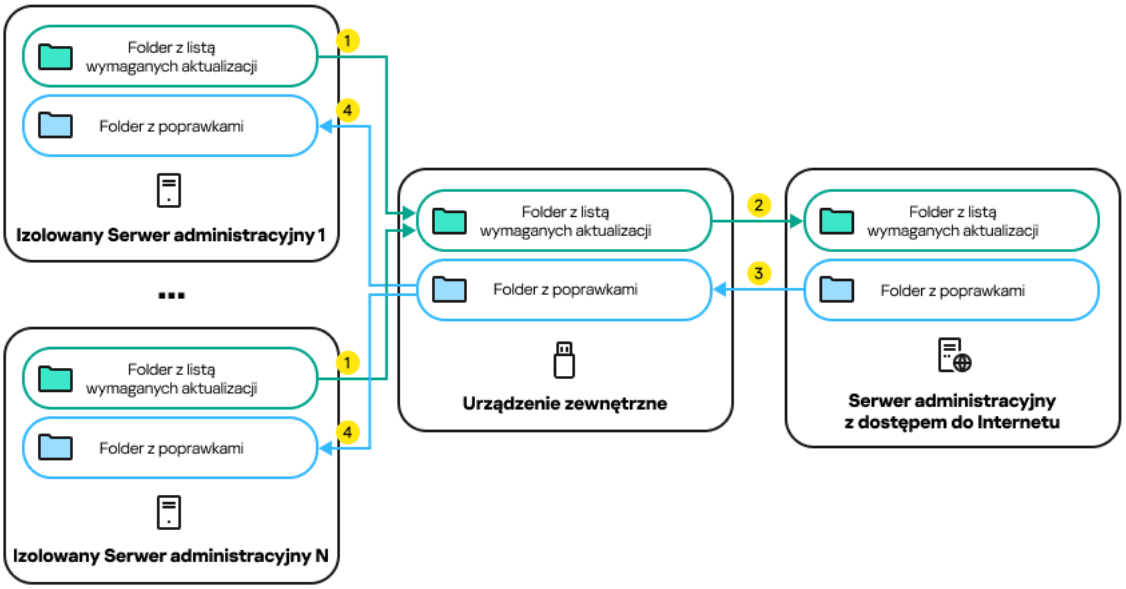
   Po zakończeniu konfigurowania serwerów administracyjnych możesz: przesyłać wymagane listy aktualizacji i poprawki pomiędzy serwerem administracyjnym z dostępem do Internetu a odizolowanymi serwerami administracyjnymi. Następnie aktualizacje z poprawek zostaną zainstalowane na zarządzanych urządzeniach przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki*.

Wyniki

W ten sposób uaktualnienia oprogramowania firm trzecich są przesyłane do odizolowanych serwerów administracyjnych i instalowane na podłączonych zarządzanych urządzeniach za pomocą Kaspersky Security Center. Wystarczy raz skonfigurować serwery administracyjne, a potem możesz otrzymywać aktualizacje tak często, jak potrzebujesz, na przykład raz lub kilka razy dziennie.

Eliminowanie luk w oprogramowaniu innych firm w odizolowanej sieci

Proces naprawiania luk w zabezpieczeniach oprogramowania firm trzecich w odizolowanej sieci jest przedstawiony na rysunku i opisany poniżej. Możesz okresowo powtarzać ten proces.



Proces przesyłania poprawek i lista wymaganych aktualizacji między serwerem administracyjnym z dostępem do Internetu a izolowanymi serwerami administracyjnymi

Każdy serwer administracyjny odizolowany od Internetu (zwany dalej izolowanym serwerem administracyjnym) generuje listę aktualizacji, które należy zainstalować na zarządzanych urządzeniach podłączonych do tego serwera administracyjnego. Lista wymaganych aktualizacji jest przechowywana w określonym folderze i przedstawia zestaw plików binarnych. Każdy plik ma nazwę zawierającą identyfikator poprawki z wymaganą aktualizacją. W rezultacie każdy plik na liście wskazuje konkretną poprawkę.

Używając zewnętrznego dysku, przenosisz listę wymaganych aktualizacji z izolowanego Serwera administracyjnego na przydzielony Serwer administracyjny z dostępem do Internetu. Następnie przydzielony Serwer administracyjny pobiera poprawki z Internetu i umieszcza je w osobnym folderze.

Po pobraniu wszystkich poprawek i umieszczeniu ich w specjalnym dla nich folderze, przenosisz je na każdy odizolowany Serwer administracyjny, z którego pobrałeś listę wymaganych uaktualnień. Poprawki zapisujesz do folderu utworzonego specjalnie dla nich na izolowanym Serwerze administracyjnym. W rezultacie zadanie *Zainstaluj wymagane aktualizacje i napraw luki* uruchamia poprawki i instaluje aktualizacje na zarządzanych urządzeniach izolowanych Serwerów administracyjnych.

Konfigurowanie serwera administracyjnego z dostępem do internetu w celu usunięcia luk w odizolowanej sieci

Aby przygotować się na usuwanie luk i przesyłanie poprawek w izolowanej sieci, najpierw skonfiguruj serwer administracyjny z dostępem do Internetu, a następnie skonfiguruj odizolowane serwery administracyjne.

W celu skonfigurowania serwera administracyjnego z dostępem do Internetu:

1. Utwórz dwa foldery na dysku, na którym zainstalowany jest serwer administracyjny:

   - Folder z listą wymaganych aktualizacji
   - Folder na poprawki

   Możesz nazwać te foldery tak, jak chcesz.

2. Przyznaj prawa dostępu do modyfikacji do grupy KLAdmins w utworzonych folderach, korzystając ze standardowych narzędzi administracyjnych systemu operacyjnego.

3. Użyj narzędzia klscflag, aby zapisać ścieżki do folderów we właściwościach Serwera administracyjnego.

   Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

4. Wpisz następujące polecenia w wierszu polecenia systemu Windows:

   - W celu ustawienia ścieżki do folderu dla poprawek:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<ścieżka do folderu>"`
   - W celu ustawienia ścieżki do folderu dla listy wymaganych aktualizacji:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<ścieżka do folderu>"`

   Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\<folder na poprawki>"`

5. Jeśli to konieczne, użyj narzędzia klscflag, aby określić, jak często Serwer administracyjny powinien sprawdzać nowe żądania poprawek:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <wartość w sekundach>`

   Domyślna wartość to 120 sekund.

   Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. Utwórz zadanie *Wyszukiwanie luk i wymaganych aktualizacji* aby uzyskać informacje o poprawkach oprogramowania innych firm zainstalowanych na zarządzanych urządzeniach, a następnie ustal harmonogram zadania.

7. Utwórz zadanie *Napraw luki* aby określić poprawki dla oprogramowania innych firm używane do naprawiania luk, a następnie ustaw harmonogram zadań.

   Uruchom zadanie ręcznie, jeśli chcesz, aby zostało uruchomione wcześniej niż jest to określone w harmonogramie zadań. Kolejność rozpoczynania zadań ma znaczenie. *Napraw luki* należy uruchomić po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

8. Uruchom ponownie usługę Serwera administracyjnego.

Teraz serwer administracyjny z dostępem do Internetu jest gotowy do pobierania i przesyłania aktualizacji do izolowanych serwerów administracyjnych. Zanim zaczniesz naprawiać luki, skonfiguruj izolowane serwery administracyjne.

Konfigurowanie izolowanych Serwerów administracyjnych w celu usunięcia luk w odizolowanej sieci

Po zakończeniu konfigurowania serwera administracyjnego z dostępem do internetu, przygotuj każdy odizolowany serwer administracyjny w Twojej sieci, abyś mógł: wyeliminować luki i zainstalować aktualizacje na zarządzanych urządzeniach podłączonych do izolowanych serwerów administracyjnych.

Aby skonfigurować izolowane serwery administracyjne, wykonaj następujące czynności na każdym serwerze administracyjnym:

1. Aktywuj klucz licencyjny dla funkcji Zarządzanie lukami i poprawkami (VAPM).
2. Utwórz dwa foldery na dysku, na którym zainstalowany jest serwer administracyjny:
   - Folder, w którym pojawi się lista wymaganych aktualizacji
   - Folder na poprawki

   Możesz nazwać te foldery tak, jak chcesz.
3. Przyznaj *uprawnienia do modyfikacji* do grupy KL Admins w utworzonych folderach, korzystając ze standardowych narzędzi administracyjnych systemu operacyjnego.
4. Użyj narzędzia klscflag, aby zapisać ścieżki do folderów we właściwościach Serwera administracyjnego.

   Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
5. Wpisz następujące polecenia w wierszu polecenia systemu Windows:
   - W celu ustawienia ścieżki do folderu dla poprawek:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<ścieżka do folderu>"`
   - W celu ustawienia ścieżki do folderu dla listy wymaganych aktualizacji:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<ścieżka do folderu>"`

   Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\<folder na poprawki>"`
6. Jeśli to konieczne, użyj narzędzia klscflag, aby określić, jak często izolowany serwer administracyjny powinien sprawdzać dostępność nowych poprawek:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <wartość w sekundach>`

   Domyślna wartość to 120 sekund.

   Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`
7. Jeśli to konieczne, użyj narzędzia klscflag, aby obliczyć skróty SHA256 poprawek:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   Jeśli wprowadzisz to polecenie, możesz się upewnić, że poprawki nie zostały zmodyfikowane podczas przesyłania na izolowany Serwer administracyjny oraz że otrzymano prawidłowe poprawki zawierające wymagane aktualizacje.

Domyślnie, Kaspersky Security Center nie oblicza skrótów SHA256 poprawek. Jeśli włączysz tę opcję, po odebraniu przez izolowany serwer administracyjny poprawek, Kaspersky Security Center oblicza ich skróty i porównuje uzyskane wartości ze skrótami przechowywanymi w bazie danych serwera administracyjnego. Jeśli obliczony skrót nie zgadza się ze skrótem w bazie danych, pojawia się błąd i trzeba zastąpić nieprawidłowe poprawki.

8. Utwórz zadanie *Wyszukiwanie luk i wymaganych aktualizacji* aby uzyskać informacje o poprawkach oprogramowania innych firm zainstalowanych na zarządzanych urządzeniach, a następnie ustal harmonogram zadania.

9. Utwórz zadanie *Napraw luki* aby określić poprawki dla oprogramowania innych firm używane do naprawiania luk, a następnie ustaw harmonogram zadań.

   Uruchom zadanie ręcznie, jeśli chcesz, aby zostało uruchomione wcześniej niż jest to określone w harmonogramie zadań. Kolejność rozpoczynania zadań ma znaczenie. *Napraw luki* należy uruchomić po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

10. Uruchom ponownie usługę Serwera administracyjnego.

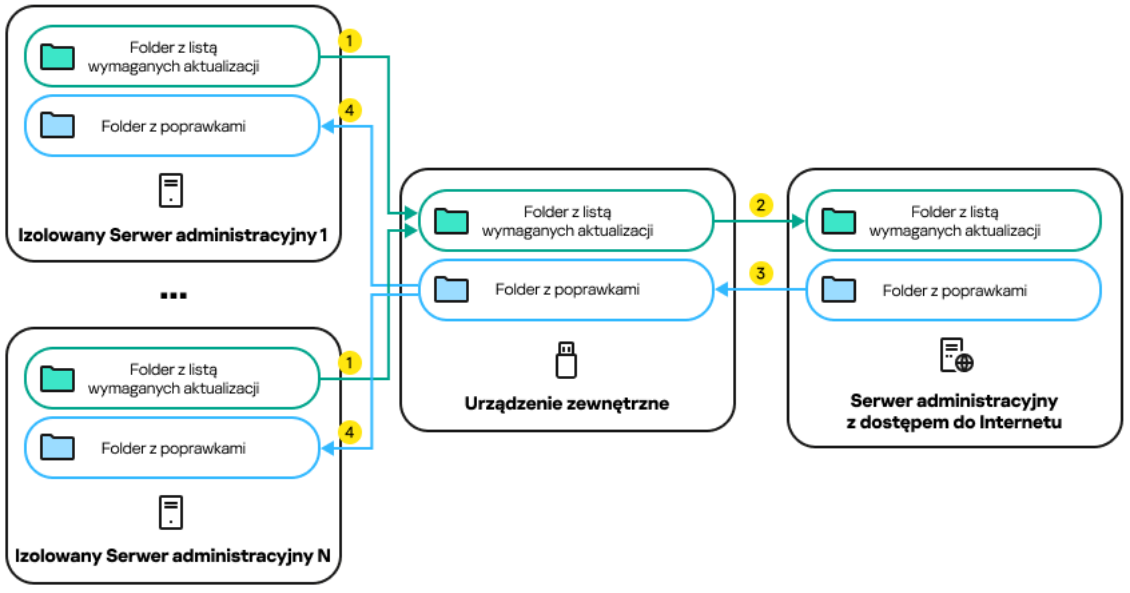
Po skonfigurowaniu wszystkich serwerów administracyjnych możesz: zarządzać poprawkami i listami wymaganych aktualizacji oraz eliminować luki w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach w odizolowanej sieci.

Przesyłanie poprawek i instalowanie aktualizacji w odizolowanej sieci

Po zakończeniu konfigurowania serwerów administracyjnych możesz przesyłać poprawki zawierające wymagane aktualizacje z serwera administracyjnego z dostępem do Internetu na izolowane serwery administracyjne. Możesz przesyłać i instalować aktualizacje tak często, jak potrzebujesz, na przykład, raz lub kilka razy dziennie.

Do przesyłania poprawek i listy wymaganych uaktualnień między Serwerami administracyjnymi potrzebny jest dysk zewnętrzny, taki jak dysk wymienny. Dlatego upewnij się, że na dysku zewnętrznym jest wystarczająco dużo miejsca do pobierania i przechowywania poprawek.

Proces przesyłania poprawek oraz lista wymaganych aktualizacji są wyświetlane na rysunku i opisane poniżej:



Proces przesyłania poprawek i lista wymaganych aktualizacji między serwerem administracyjnym z dostępem do Internetu a izolowanymi serwerami administracyjnymi

W celu zainstalowania aktualizacji i usunięcia luk na zarządzanych urządzeniach podłączonych do izolowanych Serwerów administracyjnych:

1. Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, jeśli nie zostało jeszcze uruchomione.
2. Podłącz dysk zewnętrzny do dowolnego izolowanego Serwera administracyjnego.
3. Utwórz dwa foldery na dysku zewnętrznym: jeden na listę wymaganych aktualizacji, a drugi na poprawki. Możesz nazwać te foldery tak, jak chcesz.

   Jeśli wcześniej utworzono foldery, wyczyść je.
4. Skopiuj listę wymaganych aktualizacji z każdego izolowanego Serwera administracyjnego i wklej tę listę do folderu z listą wymaganych aktualizacji na dysku zewnętrznym.

   W rezultacie wszystkie listy uzyskane ze wszystkich izolowanych serwerów administracyjnych łączysz w jeden folder. Folder ten powinien zawierać pliki binarne z identyfikatorami poprawek wymaganych dla wszystkich izolowanych serwerów administracyjnych.
5. Podłącz dysk zewnętrzny do Serwera administracyjnego z dostępem do Internetu.
6. Skopiuj listę wymaganych aktualizacji z dysku zewnętrznego i wklej tę listę do folderu listy wymaganych aktualizacji na Serwerze administracyjnym z dostępem do Internetu.

   Wszystkie wymagane poprawki są automatycznie pobierane z Internetu do folderu łatek na Serwerze administracyjnym. To może potrwać kilka godzin.
7. Upewnij się, że wszystkie wymagane poprawki zostały pobrane. W tym celu możesz wykonać jedną z następujących czynności:

   - Sprawdź folder w poszukiwaniu poprawek na Serwerze administracyjnym z dostępem do internetu. Wszystkie poprawki, które zostały określone na liście wymaganych aktualizacji, należy pobrać do odpowiedniego folderu. Jest to wygodniejsze, jeśli wymagana jest niewielka liczba poprawek.
   - Przygotuj specjalny skrypt, na przykład, skrypt powłoki. Jeśli otrzymasz dużą liczbę poprawek, trudno będzie samodzielnie sprawdzić, czy wszystkie poprawki zostały pobrane. W takich przypadkach lepiej zautomatyzować sprawdzanie.
8. Skopiuj poprawki z Serwera administracyjnego z dostępem do Internetu i wklej je do odpowiedniego folderu na dysku zewnętrznym.
9. Prześlij poprawki do każdego izolowanego Serwera administracyjnego. Umieść poprawki w specjalnym folderze.

W rezultacie każdy izolowany serwer administracyjny tworzy aktualną listę aktualizacji i poprawek wymaganych dla zarządzanych urządzeń podłączonych do bieżącego serwera administracyjnego. Po otrzymaniu przez serwer administracyjny z dostępem do Internetu listy wymaganych aktualizacji, serwer administracyjny pobiera poprawki z aktualizacjami z Internetu. Gdy te poprawki pojawią się na odizolowanych serwerach administracyjnych, zadanie *Zainstaluj wymagane aktualizacje i napraw luki* obsługuje poprawki. Aktualizacje są instalowane na zarządzanych urządzeniach, a luki w zabezpieczeniach oprogramowania innych firm są naprawiane.

Gdy uruchomione jest zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, nie uruchamiaj ponownie urządzenia serwera administracyjnego ani nie uruchamiaj zadania *Kopia zapasowa danych Serwera administracyjnego* (spowoduje to również ponowne uruchomienie). W rezultacie zadanie *Zainstaluj wymagane aktualizacje i napraw luki* zostanie przerwane, a aktualizacje nie zostaną zainstalowane. W takim przypadku musisz zrestartować to zadanie ręcznie lub poczekać na uruchomienie zadania zgodnie ze skonfigurowanym harmonogramem.

Wyłączanie możliwości przesyłania poprawek i instalowania aktualizacji w odizolowanej sieci

Można wyłączyć przesyłanie poprawek na izolowanych serwerach administracyjnych, na przykład, jeśli zdecydowano się usunąć jeden lub więcej serwerów z odizolowanej sieci. W ten sposób możesz zmniejszyć liczbę poprawek i czas ich pobierania.

W celu wyłączenia możliwości przekazania poprawek na izolowanych serwerach administracyjnych:

1. Jeśli chcesz wyizolować wszystkie serwery administracyjne, we właściwościach serwera administracyjnego z dostępem do Internetu usuń ścieżki do folderów z poprawkami oraz listę wymaganych aktualizacji. Jeśli chcesz, aby niektóre serwery administracyjne znajdowały się w odizolowanej sieci, pomiń ten krok.

   Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Wpisz następujące polecenia w wierszu polecenia:

   - W celu usunięcia ścieżki do folderu dla poprawek:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - W celu usunięcia ścieżki do folderu dla listy wymaganych aktualizacji:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. Uruchom ponownie usługę serwera administracyjnego, jeśli usunięto ścieżki do folderów na tym serwerze administracyjnym.

3. We właściwościach każdego serwera administracyjnego, który chcesz wyłączyć z izolacji, usuń ścieżki do folderów z poprawkami oraz listę wymaganych aktualizacji.

   Wpisz następujące polecenia w wierszu polecenia systemu Windows, korzystając z uprawnień administratora:

   - W celu usunięcia ścieżki do folderu dla poprawek:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - W celu usunięcia ścieżki do folderu dla listy wymaganych aktualizacji:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. Uruchom ponownie każdy serwer administracyjny, z którego usunięto ścieżki do folderów.

W rezultacie, jeśli zmieniono konfigurację serwera administracyjnego z dostępem do Internetu, nie będziesz już otrzymywać poprawek za pośrednictwem Kaspersky Security Center. Jeżeli zmieniono konfigurację tylko niektórych odizolowanych serwerów administracyjnych, np. usuwając niektóre z nich z izolowanej sieci, otrzymasz poprawki tylko dla pozostałych izolowanych serwerów administracyjnych.

Jeśli chcesz w przyszłości rozpocząć eliminowanie luk w zabezpieczeniach na wyłączonych izolowanych serwerach administracyjnych, musisz skonfigurować te serwery i serwer z dostępem do Internetu jeszcze raz.

Ignorowanie luk w oprogramowaniu

Możesz zignorować luki w oprogramowaniu, które mają zostać naprawione. Przyczyny zignorowania luk w oprogramowaniu mogą być, na przykład, następujące:

- Nie uważasz luki w oprogramowaniu za krytyczną dla swojej organizacji.
- Rozumiesz, poprawka luki w oprogramowaniu może uszkodzić dane związane z oprogramowaniem, które wymagało naprawy luki.
- Jesteś pewien, że luka w oprogramowaniu nie jest niebezpieczna dla sieci w Twojej organizacji, ponieważ używasz innych środków ochrony swoich zarządzanych urządzeń.

Możesz zignorować lukę w oprogramowaniu na wszystkich zarządzanych urządzeniach lub tylko na wybranych zarządzanych urządzeniach.

W celu zignorowania luki w oprogramowaniu na wszystkich zarządzanych urządzeniach:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.

   Obszar roboczy folderu wyświetla listę luk w aplikacjach, wykrytych na urządzeniach przez zainstalowanego na nich Agenta sieciowego.

2. Wybierz lukę, którą chcesz zignorować.

3. Z menu kontekstowego luki wybierz **Właściwości**.

   Zostanie otwarte okno właściwości luki.

4. W sekcji **Ogólne** wybierz opcję **Ignoruj lukę**.

5. Kliknij **OK**.

   Okno właściwości luki w oprogramowaniu zostanie zamknięte.

Luka w oprogramowaniu zostanie zignorowana na wszystkich zarządzanych urządzeniach.

W celu zignorowania luki w oprogramowaniu na wybranym zarządzanym urządzeniu:

1. Otwórz okno właściwości wybranego zarządzanego urządzenia i wybierz sekcję **Luki w oprogramowaniu**.

2. Wybierz lukę w oprogramowaniu.

3. Zignoruj wybraną lukę.

Luka w oprogramowaniu zostanie zignorowana na wybranym urządzeniu.

Zignorowana luka w oprogramowaniu nie zostanie naprawiona po zakończeniu wykonywania zadania *Napraw luki* lub zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Możesz wykluczyć zignorowane luki w oprogramowaniu z listy luk z użyciem filtra.

Wybieranie poprawek użytkownika dla luk w programach innych firm

Aby użyć zadania *Napraw luki*, należy ręcznie określić aktualizacje oprogramowania do naprawy luk w programach innych firm, wymienionych w ustawieniach zadania. Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla innych programów innych firm. *Poprawki użytkownika* to aktualizacje oprogramowania do naprawy luk, które administrator ręcznie określa do zainstalowania.

W celu wybrania poprawek użytkownika dla luk w programach firm trzecich:

1. W folderze **Zaawansowane → Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.

   Obszar roboczy folderu wyświetla listę luk w aplikacjach, wykrytych na urządzeniach przez zainstalowanego na nich Agenta sieciowego.

2. Wybierz lukę, dla której chcesz określić poprawkę użytkownika.

3. Z menu kontekstowego luki wybierz **Właściwości**.

   Zostanie otwarte okno właściwości luki.

4. W sekcji **Poprawki użytkownika i inne poprawki** kliknij przycisk **Dodaj**.

   Zostanie wyświetlona lista dostępnych pakietów instalacyjnych. Lista wyświetlonych pakietów instalacyjnych odpowiada liście **Zdalna instalacja → Pakiety instalacyjne**. Jeśli nie utworzono pakietu instalacyjnego zawierającego poprawkę użytkownika dla wybranej luki, możesz utworzyć pakiet teraz, uruchamiając Kreator tworzenia nowego pakietu.

5. Wybierz pakiet (lub pakiety) instalacyjny zawierający poprawkę użytkownika (lub poprawki użytkownika) dla luki w oprogramowaniu innych firm.

6. Kliknij **OK**.

Zostaną określone pakiety instalacyjne zawierające poprawki użytkownika dla luki w oprogramowaniu. Jeśli zadanie jest uruchamiane *Napraw luki*, pakiet instalacyjny zostanie zainstalowany, a luka w oprogramowaniu zostanie wyeliminowana.

Reguły instalacji aktualizacji

Jeśli usuwasz luki w aplikacjach, musisz określić reguły instalacji aktualizacji. Te reguły określają aktualizacje do zainstalowania oraz luki do wyeliminowania.

Dokładne ustawienia zależą od tego, czy tworzysz regułę dla aktualizacji aplikacji firmy Microsoft, aplikacji firm trzecich (aplikacje stworzone przez producentów oprogramowania innych niż Kaspersky i Microsoft) lub wszystkich aplikacji. Podczas tworzenia reguł dla aplikacji firmy Microsoft lub aplikacji firm trzecich możesz wybrać określone aplikacje oraz wersje aplikacji, dla których chcesz zainstalować uaktualnienia. Podczas tworzenia reguły dla wszystkich aplikacji możesz wybrać określone uaktualnienia, które chcesz zainstalować, oraz luki, które chcesz wyeliminować poprzez zainstalowanie uaktualnień.

W celu utworzenia reguły dla uaktualnień wszystkich aplikacji:

1. Na stronie **Ustawienia** kreatora tworzenia nowego zadania kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Postępuj zgodnie z krokami kreatora.

2. W kroku **Typ reguły** wybierz **Reguła dla wszystkich aktualizacji**.

3. W kroku **Kryteria ogólne** użyj list rozwijalnych do określenia następujących ustawień:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.

     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.

     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aktualizacje** wybierz aktualizacje, które mają zostać zainstalowane:

   - **Zainstaluj wszystkie pasujące aktualizacje**

     Zainstaluj aktualizacje oprogramowania, które spełniają kryteria określone w kroku **Kryteria ogólne**. Ta opcja jest wybrana domyślnie.

   - **Zainstaluj tylko aktualizacje z listy**

     Instalowane są tylko te aktualizacje oprogramowania, które wybierzesz ręcznie z listy. Ta lista zawiera wszystkie dostępne aktualizacje oprogramowania.

     Na przykład, możesz wybrać określone aktualizacje w następujących przypadkach: aby sprawdzić ich instalację w środowisku testowym, aby zaktualizować tylko krytyczne aplikacje lub aby zaktualizować tylko określone aplikacje.

     - **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

       Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

       Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

Domyślnie opcja ta jest włączona.

5. W kroku **Luki** wybierz luki, które zostaną wyeliminowane poprzez zainstalowanie wybranych aktualizacji:

   - **Napraw wszystkie luki spełniające inne kryteria**

     Wyeliminuj wszystkie luki, które spełniają kryteria określone na stronie **Kryteria ogólne** kreatora. Ta opcja jest wybrana domyślnie.

   - **Napraw tylko luki z listy**

     Naprawione zostaną tylko te luki, które ręcznie wybierzesz z listy. Ta lista zawiera wszystkie wykryte luki.

     Na przykład, możesz wybrać określone luki w następujących przypadkach: aby sprawdzić ich eliminację w środowisku testowym, aby wyeliminować luki tylko w krytycznych aplikacjach lub aby wyeliminować luki tylko w określonych aplikacjach.

6. W kroku **Nazwa** określ nazwę dla reguły, którą tworzysz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie utworzona i wyświetlona w polu **Określ reguły instalacji aktualizacji** Kreatora tworzenia nowego zadania.

W celu utworzenia reguły dla aktualizacji aplikacji firmy Microsoft:

1. Na stronie **Ustawienia** kreatora tworzenia nowego zadania kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Postępuj zgodnie z krokami kreatora.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji systemu Windows**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.

     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.

     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

Domyślnie opcja ta jest wyłączona.

- **Napraw luki z priorytetem MSRC równym lub większym niż**

  Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

  Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

  Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

  Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Kategorie aktualizacji** wybierz kategorie aktualizacji, które mają zostać zainstalowane. Te kategorie są takie same, jak w Microsoft Update Catalog. Domyślnie, zaznaczone są wszystkie kategorie.

6. W kroku **Nazwa** określ nazwę dla reguły, którą tworzysz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie utworzona i wyświetlona w polu **Określ reguły instalacji aktualizacji** Kreatora tworzenia nowego zadania.

W celu utworzenia nowej reguły dla aktualizacji aplikacji firm trzecich:

1. Na stronie **Ustawienia** kreatora tworzenia nowego zadania kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Postępuj zgodnie z krokami kreatora.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji firm trzecich**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.

     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.

     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

- **Napraw luki z priorytetem równym lub większym niż**

  Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

  Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

  Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

  Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Nazwa** określ nazwę dla reguły, którą tworzysz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie utworzona i wyświetlona w polu **Określ reguły instalacji aktualizacji** Kreatora tworzenia nowego zadania.

Grupy aplikacji

Sekcja ta opisuje sposób zarządzania grupami aplikacji zainstalowanych na urządzeniach.

Tworzenie kategorii aplikacji

Kaspersky Security Center pozwala na tworzenie kategorii aplikacji zainstalowanych na urządzeniach.

Kategorie aplikacji można utworzyć w jeden z następujących sposobów:

- Administrator określa folder, z którego pliki wykonywalne zostały uwzględnione w wybranej kategorii.
- Administrator określa urządzenie, z którego pliki wykonywalne mają zostać uwzględnione w wybranej kategorii.
- Administrator ustawia kryteria, które zostaną użyte przy dodawaniu aplikacji do wybranej kategorii.

Po utworzeniu kategorii aplikacji, administrator może ustawić reguły dla tej kategorii. Reguły określają zachowanie aplikacji znajdującej się w danej kategorii. Na przykład, możesz zablokować lub zezwolić na uruchamianie aplikacji znajdujących się w kategorii.

Zarządzanie aplikacjami uruchomionymi na urządzeniach

Kaspersky Security Center umożliwia zarządzanie uruchamianiem aplikacji na urządzeniach w trybie listy zezwolonych. Więcej informacji można znaleźć w internetowym systemie pomocy dla Kaspersky Endpoint Security for Windows. W trakcie pracy w trybie listy zezwolonych, na wybranych urządzeniach możesz uruchamiać aplikacje tylko z określonych kategorii. Administrator może wyświetlić wyniki analizy statystycznej zastosowanej na regułach uruchamiania aplikacji na urządzeniach dla każdego użytkownika.

Inwentaryzacja oprogramowania zainstalowanego na urządzeniach

Kaspersky Security Center pozwala na przeprowadzanie inwentaryzacji oprogramowania na urządzeniach działających pod kontrolą systemu Windows i Linux. Agent sieciowy pobiera informacje o wszystkich aplikacjach zainstalowanych na urządzeniach. Informacje zebrane w trakcie inwentaryzacji są wyświetlane w obszarze roboczym folderu **Rejestr aplikacji**. Administrator może wyświetlić szczegółowe informacje o każdej aplikacji, łącznie z wersją i producentem.

Liczba plików wykonywalnych pobranych z jednego urządzenia nie może przekraczać 150 000. Po osiągnięciu tego limitu, Kaspersky Security Center nie będzie mógł otrzymywać nowych plików.

Zarządzanie grupą licencjonowanych aplikacji

Kaspersky Security Center pozwala na tworzenie grup licencjonowanych aplikacji. Grupa licencjonowanych aplikacji zawiera aplikacje spełniające kryteria ustalone przez administratora. Administrator może określić następujące kryteria dla grup licencjonowanych aplikacji:

- Nazwa aplikacji
- Wersja aplikacji
- Producent
- Znacznik aplikacji

Aplikacje spełniające jedno lub kilka kryteriów są automatycznie dodawane do grupy. Aby utworzyć grupę licencjonowanych aplikacji, musisz ustawić przynajmniej jedno kryterium dodawania aplikacji do takiej grupy.

Każda grupa licencjonowanych aplikacji posiada swój klucz licencyjny. Klucz licencyjny grupy licencjonowanych aplikacji określa maksymalną dozwoloną liczbę instalacji aplikacji wchodzących w skład tej grupy. Jeśli liczba instalacji przekroczyła ograniczenie ustawione przez klucz licencyjny, na Serwerze administracyjnym zostanie zarejestrowane zdarzenie informacyjne. Administrator może określić datę wygaśnięcia dla klucza licencyjnego. Po nadejściu tej daty, na Serwerze administracyjnym jest zapisywane zdarzenie informacyjne.

Przeglądanie informacji o plikach wykonywalnych

Kaspersky Security Center pobiera wszystkie informacje o plikach wykonywalnych, które były uruchamiane na urządzeniach od momentu zainstalowania na nich systemu operacyjnego. Zebrane informacje o plikach wykonywalnych są wyświetlane w oknie głównym aplikacji, w obszarze roboczym folderu **Pliki wykonywalne**.

Korzystanie z Kontroli aplikacji do zarządzania plikami wykonywalnymi

Możesz użyć komponentu Kontrola aplikacji, aby zezwolić lub zablokować uruchamianie plików wykonywalnych na urządzeniach użytkowników. Komponent Kontrola aplikacji obsługuje systemy operacyjne oparte na systemie Windows i Linux.

W systemach operacyjnych opartych na systemie Linux komponent Kontrola aplikacji jest dostępny od wersji Kaspersky Endpoint Security 11.2 for Linux. Komponent ten jest również dostępny w Kaspersky Embedded Systems Security for Windows w wersji 3.0 i nowszych.

Wymagania wstępne

- Kaspersky Security Center zostanie wdrożony w Twojej organizacji.
- Zasada Kaspersky Endpoint Security for Windows lub Kaspersky Endpoint Security for Linux została utworzona i jest aktywna.
- Zasada Kaspersky Embedded Systems Security for Windows lub Kaspersky Embedded Systems Security for Linux została utworzona i jest aktywna.

Etapy

Scenariusz korzystania z Kontroli aplikacji podzielony jest na etapy:

1. **Tworzenie i przeglądanie listy plików wykonywalnych na urządzeniach klienckich**

   Ten etap pomaga w odnalezieniu plików wykonywalnych, które znajdują się na zarządzanych urządzeniach. Przejrzyj listę plików wykonywalnych i porównaj ją z listami dozwolonych i zabronionych plików wykonywalnych. Ograniczenia dotyczące użycia plików wykonywalnych mogą być związane z polityką bezpieczeństwa informacji, obowiązującej w Twojej organizacji.

   Dostępne instrukcje:

   - Konsola administracyjna: Inwentaryzacja plików wykonywalnych
   - Kaspersky Security Center Web Console: Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

2. **Tworzenie kategorii dla plików wykonywalnych używanych w Twojej organizacji**

   Przeanalizuj listy plików wykonywalnych, przechowywanych na zarządzanych urządzeniach. Na podstawie analizy utwórz kategorie dla plików wykonywalnych. Zalecane jest utworzenie kategorii „Aplikacje do pracy", która obejmuje standardowy zestaw plików wykonywalnych używanych w Twojej organizacji. Jeśli różne grupy bezpieczeństwa używają własnych zestawów plików wykonywalnych w swojej pracy, oddzielna kategoria może zostać utworzona dla każdej grupy bezpieczeństwa.

Dostępne instrukcje:

- Konsola administracyjna: Tworzenie kategorii aplikacji z zawartością dodaną ręcznie, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranych urządzeń, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranego folderu.
- Kaspersky Security Center Web Console: Tworzenie kategorii aplikacji z zawartością dodaną ręcznie, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranych urządzeń, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranego folderu.

3. **Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security**

   Skonfiguruj komponent Kontrola aplikacji w zasadzie Kaspersky Endpoint Security, korzystając z kategorii aplikacji, które utworzono w poprzednim kroku.

   Dostępne instrukcje:

   - Konsola administracyjna: Konfigurowanie zarządzania uruchamianiem aplikacji na urządzeniach klienckich
   - Kaspersky Security Center Web Console: Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows

4. **Konfigurowanie Kontroli aplikacji w zasadzie aplikacji Kaspersky Embedded Systems Security**

   Skonfiguruj komponent Kontrola aplikacji w zasadach Kaspersky Embedded Systems Security for Windows, korzystając z kategorii, które utworzyłeś/-aś. Aby uzyskać więcej informacji na temat komponentu Kontrola aplikacji, zapoznaj się z Pomocą Kaspersky Embedded Systems Security for Windows lub Pomocą Kaspersky Embedded Systems Security for Linux.

   Jeśli używasz dużej liczby reguł, może wystąpić błąd podczas ładowania zasady. Maksymalny rozmiar żądania w bajtach można zwiększyć, korzystając z następujących poleceń:

   - W przypadku żądania JSON:

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
     ```

   - W przypadku żądania HTTP:

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
     ```

     Gdzie `<max_request_size>` to maksymalny rozmiar żądania w bajtach (na przykład `200000000`).

5. **Włączanie komponentu Kontrola aplikacji w trybie testowym**

   Aby zapewnić, że reguły Kontroli aplikacji nie będą blokowały plików wykonywalnych wymaganych do pracy użytkownika, zalecane jest włączenie testowania reguł Kontroli aplikacji i analizowanie ich działania po utworzeniu nowych reguł. Po włączeniu testowania, Kaspersky Endpoint Security for Windows lub Kaspersky Embedded Systems Security nie zablokuje plików wykonywalnych, których uruchamianie jest zablokowane przez reguły Kontroli aplikacji, ale zamiast tego wyśle powiadomienia o ich uruchomieniu do Serwera administracyjnego.

   Podczas testowania reguł Kontroli aplikacji zalecane jest wykonanie następujących działań:

   - Określenie okresu testowania. Okres testowania może wahać się od siedmiu dni do dwóch miesięcy.
   - Sprawdź zdarzenia wynikające z testowania działania Kontroli aplikacji.

   Wskazówki jak postępować dla Kaspersky Security Center Web Console: Konfigurowanie komponentu Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Windows. Postępuj zgodnie z tymi instrukcjami i włącz opcję **Tryb testowy** w procesie konfiguracji.

6. **Zmienianie ustawień kategorii komponentu Kontrola aplikacji**

Jeśli to konieczne, wprowadź zmiany w ustawieniach Kontroli aplikacji. W oparciu o wyniki testu, możesz dodać pliki wykonywalne związane ze zdarzeniami komponentu Kontrola aplikacji do kategorii z zawartością dodaną ręcznie.

Dostępne instrukcje:

- Konsola administracyjna: Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji
- Kaspersky Security Center Web Console: Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

7. **Stosowanie reguł Kontroli aplikacji w trybie działania**

   Po przetestowaniu reguł Kontroli aplikacji i zakończeniu konfiguracji kategorii możesz zastosować reguły Kontroli aplikacji w trybie działania.

   Wskazówki jak postępować dla Kaspersky Security Center Web Console: Konfigurowanie komponentu Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Windows. Postępuj zgodnie z tymi instrukcjami i wyłącz opcję **Tryb testowy** w procesie konfiguracji.

8. **Weryfikowanie konfiguracji Kontroli aplikacji**

   Upewnij się, że wykonałeś następujące czynności:

   - Utworzono kategorie dla plików wykonywalnych.
   - Skonfigurowano Kontrolę aplikacji przy użyciu kategorii.
   - Zastosowałeś reguły Kontroli aplikacji w trybie działania.

Wyniki

Po zakończeniu scenariusza uruchamianie plików wykonywalnych na zarządzanych urządzeniach jest kontrolowane. Użytkownicy mogą uruchamiać tylko te pliki wykonywalne, które są dozwolone w Twojej organizacji, a nie mogą uruchamiać plików wykonywalnych, które są zabronione w Twojej organizacji.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Pomoc Kaspersky Embedded Systems Security for Windows
- Pomoc Kaspersky Embedded Systems Security for Linux

Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

Listę plików wykonywalnych przechowywanych na urządzeniach klienckich można uzyskać w jeden z następujących sposobów:

- Włączenie powiadomień o uruchomieniu aplikacji w zasadach Kaspersky Endpoint Security.
- Tworzenie zadania inwentaryzacji.

Włączenie powiadomień o uruchomieniu aplikacji w zasadach Kaspersky Endpoint Security

Aby włączyć powiadomienia o uruchomieniu aplikacji:

1. Otwórz ustawienia zasad Kaspersky Endpoint Security, a następnie przejdź do **Ustawienia ogólne** → **Raporty i pliki danych**.
2. W grupie ustawień **Przesyłania danych do Serwera administracyjnego** zaznacz pole wyboru **Informacje o uruchomionych aplikacjach** i zapisz zmiany.

Gdy użytkownik próbuje uruchomić pliki wykonywalne, informacje o tych plikach są dodawane do listy plików wykonywalnych na urządzeniu klienckim. Kaspersky Endpoint Security wysyła te informacje do Agenta sieciowego, a następnie Agent sieciowy wysyła je do Serwera administracyjnego.

Tworzenie zadania inwentaryzacji

Funkcja inwentaryzacji plików wykonywalnych jest dostępna dla następujących aplikacji:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux w wersji 11.2 i nowszych
- Kaspersky Security for Virtualization 4.0 Light Agent i nowsze wersje

Możesz zmniejszyć obciążenie bazy danych, jednocześnie uzyskując informacje o zainstalowanych aplikacjach. Aby zaoszczędzić miejsce, uruchom zadanie inwentaryzacji na urządzeniach, na których jest zainstalowany standardowy zestaw oprogramowania. Preferowana liczba urządzeń to od 1 do 3.

Zdecydowanie nie zalecamy uruchamiania zadania inwentaryzacji w przypadku korzystania z następujących baz danych: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (wszystkie edycje).

W celu utworzenia zadania dla plików wykonywalnych na urządzeniach klienckich:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. W obszarze roboczym folderu **Zadania** kliknij przycisk **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W oknie **Wybierz typ zadania**, jako typ zadania wybierz **Kaspersky Endpoint Security**, a następnie, jako podtyp zadania wskaż **Inwentaryzacja** i kliknij **Dalej**.
4. Wykonaj pozostałe instrukcje kreatora.

   Po zakończeniu działania Kreatora tworzenia nowego zadania, zostaje utworzone i skonfigurowane zadanie **Inwentaryzacja**. Jeśli chcesz, możesz zmienić ustawienia dla utworzonego zadania. Nowo utworzone zadanie będzie wyświetlane na liście zadań. Jeśli chcesz, możesz zmienić ustawienia dla utworzonego zadania.

Szczegółowy opis zadania inwentaryzacji znajduje się w następujących Pomocach:

- Pomoc Kaspersky Endpoint Security for Windows
- Pomoc Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Po wykonaniu zadania **Inwentaryzacja**, zostaje utworzona lista plików wykonywalnych przechowywanych na zarządzanych urządzeniach i możesz przejrzeć listę.

Podczas inwentaryzacji mogą zostać wykryte pliki wykonywalne w następujących formatach (w zależności od opcji wybranej we właściwościach zadania inwentaryzacji): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR i HTML.

Przeglądanie listy plików wykonywalnych, przechowywanych na zarządzanych urządzeniach

W celu przejrzenia listy plików wykonywalnych przechowywanych na urządzeniach klienckich:

W drzewie konsoli przejdź do **Zaawansowane** → **Zarządzanie aplikacjami** → **Pliki wykonywalne**.

W razie potrzeby możesz przesłać plik wykonywalny z zarządzanego urządzenia do urządzenia, na którym zainstalowano Konsolę administracyjną.

Aby wysłać plik wykonywalny:

1. W drzewie konsoli przejdź do **Zaawansowane** → **Zarządzanie aplikacjami** → **Pliki wykonywalne**.
2. Kliknij odnośnik do pliku wykonywalnego, który chcesz wysłać do urządzenia z zainstalowaną Konsolą administracyjną.

3. W oknie, które zostanie otwarte, przejdź do sekcji **Urządzenia**, a następnie zaznacz pole wyboru zarządzanego urządzenia, z którego chcesz wysłać plik wykonywalny.

   Przed wysłaniem pliku wykonywalnego upewnij się, że zarządzane urządzenie ma bezpośrednie połączenie z Serwerem administracyjnym, zaznaczając pole **Nie odłączaj od Serwera administracyjnego**.

4. Kliknij przycisk **Wyślij**, wybierz folder docelowy i kliknij przycisk **OK**.

   Wybrany plik wykonywalny zostanie pobrany w celu dalszego wysłania do urządzenia, na którym zainstalowano Konsolę administracyjną.

Tworzenie kategorii aplikacji dla zasad Kaspersky Endpoint Security for Windows

Możesz utworzyć kategorie aplikacji dla zasad Kaspersky Endpoint Security for Windows z folderu **Kategorie aplikacji** i z okna **Właściwości** zasady Kaspersky Endpoint Security for Windows.

*W celu utworzenia kategorii aplikacji dla zasady Kaspersky Endpoint Security z folderu **Kategorie aplikacji**:*

1. W drzewie konsoli wybierz **Zaawansowane** → **Zarządzanie aplikacjami** → **Kategorie aplikacji**.
2. W obszarze roboczym folderu **Kategorie aplikacji** kliknij przycisk **Nowa kategoria**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii.
3. W oknie **Typ kategorii** wybierz typ kategorii użytkownika:

   - **Ręcznie dodana kategoria z zawartością**. Określ kryteria, które będą używane do przypisywania plików wykonywalnych do tworzonej kategorii.
   - **Automatycznie dodana kategoria z zawartością**. Określ folder, z którego pliki wykonywalne zostaną automatycznie przypisane do utworzonej kategorii.

     Podczas tworzenia kategorii z zawartością dodaną automatycznie aplikacja przeprowadza inwentaryzację następujących typów plików: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX i SCR.

   - **Kategoria zawierająca pliki wykonywalne z wybranych urządzeń**. Określ urządzenie, którego pliki wykonywalne muszą być automatycznie przypisane do tej kategorii.
4. Postępuj zgodnie z instrukcjami kreatora.

   Jeśli kreator zakończy działanie, zostanie utworzona niestandardowa kategoria aplikacji. Nowo utworzone kategorie można przeglądać, korzystając z listy kategorii w obszarze roboczym folderu **Kategorie aplikacji**.

Jeśli chcesz wyeksportować kategorię aplikacji do pliku KLC, kliknij prawym przyciskiem myszy nazwę kategorii, wybierz z menu opcję **Eksportuj**, a następnie w otwartym oknie podaj nazwę pliku i kliknij przycisk **Zapisz**.

Możesz także utworzyć kategorię aplikacji z poziomu folderu **Zasady**.

*W celu utworzenia kategorii aplikacji z poziomu okna **Właściwości** zasady Kaspersky Endpoint Security for Windows:*

1. Z drzewa konsoli wybierz folder **Zasady**.
2. W obszarze roboczym folderu **Zasady** wybierz zasadę Kaspersky Endpoint Security, dla której chcesz utworzyć kategorię.
3. Kliknij go prawym klawiszem myszy i wybierz **Właściwości**.
4. W oknie **Właściwości**, które zostanie otwarte, w lewym panelu **Sekcje** wybierz **Kontrola zabezpieczeń → Kontrola aplikacji**.
5. W sekcji **Kontrola aplikacji**, na listach rozwijalnych **Tryb kontroli** i **Akcja** dokonaj wyboru dla listy zezwolonych i listy zablokowanych, a następnie kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Reguła Kontroli aplikacji** zawierające listę kategorii.
6. Kliknij przycisk **Utwórz nową**.
7. Wprowadź nazwę nowej kategorii i kliknij **OK**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii.
8. W oknie **Typ kategorii** wybierz typ kategorii użytkownika:

   - **Ręcznie dodana kategoria z zawartością**. Określ kryteria, które będą używane do przypisywania plików wykonywalnych do tworzonej kategorii.
   - **Automatycznie dodana kategoria z zawartością**. Określ folder, z którego pliki wykonywalne zostaną automatycznie przypisane do utworzonej kategorii.

     > Podczas tworzenia kategorii z zawartością dodaną automatycznie aplikacja przeprowadza inwentaryzację następujących typów plików: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX i SCR.

   - **Kategoria zawierająca pliki wykonywalne z wybranych urządzeń**. Określ urządzenie, którego pliki wykonywalne muszą być automatycznie przypisane do tej kategorii.
9. Postępuj zgodnie z instrukcjami kreatora.

Jeśli kreator zakończy działanie, zostanie utworzona niestandardowa kategoria aplikacji. Możesz przeglądać nowo utworzone kategorie na liście kategorii.

Kategorie aplikacji są używane przez komponent Kontrola aplikacji znajdujący się w Kaspersky Endpoint Security for Windows. Kontrola aplikacji umożliwia administratorowi nałożenie ograniczeń na uruchamianie aplikacji na urządzeniach klienckich—na przykład, ograniczając uruchamianie aplikacji z określonej kategorii.

Tworzenie kategorii aplikacji z zawartością dodaną ręcznie

Możesz określić zestaw kryteriów jako szablon plików wykonywalnych, dla których chcesz zezwolić na lub zablokować uruchamianie w Twojej organizacji. W oparciu o pliki wykonywalne odpowiadające kryteriom, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii aplikacji z zawartością dodaną ręcznie:

1. W drzewie konsoli, w folderze **Zaawansowane** → **Zarządzanie aplikacjami** wybierz podfolder **Kategorie aplikacji**.

2. Kliknij przycisk **Nowa kategoria**.

   Zostanie uruchomiony **Kreator tworzenia nowej kategorii**. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Na stronie kreatora **Typ kategorii** wybierz opcję **Kategoria z zawartością dodaną ręcznie jako typ kategorii użytkownika**.

4. Na stronie kreatora **Wprowadź nazwę kategorii aplikacji** wprowadź nową nazwę kategorii aplikacji.

5. W kroku **Konfiguracja warunków włączania aplikacji do kategorii** conditions for inclusion of applications in categories kliknij przycisk **Dodaj**.

6. Na liście rozwijalnej określ odpowiednie ustawienia:

   - **Z listy plików wykonywalnych**

     Jeśli ta opcja jest zaznaczona, możesz wskazać na liście plików wykonywalnych na urządzeniu klienckim te aplikacje, które chcesz dodać do kategorii.

   - **Z właściwości pliku**

     Jeżeli ta opcja jest zaznaczona, możesz określić szczegółowe dane dla plików wykonywalnych, które zostaną dodane do kategorii użytkownika dla aplikacji.

   - **Metadane z plików w folderze**

     Określ folder na urządzeniu klienckim, w którym znajdują się pliki wykonywalne. Metadane w plikach wykonywalnych, które znajdują się w określonym folderze, zostaną wysłane do Serwera administracyjnego. Pliki wykonywalne, które zawierają te same metadane, zostaną dodane do kategorii użytkownika.

   - **Sumy kontrolne plików znajdujących się w folderze**

     Jeżeli ta opcja jest zaznaczona, możesz wybrać lub utworzyć folder na urządzeniu klienckim. Suma kontrola MD5 plików, które znajdują się w określonym folderze, zostanie wysłana do Serwera administracyjnego. Aplikacje, które mają tę samą sumę kontrolną co pliki w określonym folderze, zostaną dodane do kategorii aplikacji użytkownika.

   - **Certyfikaty dla plików z folderu**

     Jeżeli ta opcja jest zaznaczona, możesz wskazać folder na urządzeniu klienckim, który zawiera pliki wykonywalne podpisane przez certyfikat. Certyfikaty plików wykonywalnych są do odczytu i zostają dodane do warunków kategorii. Pliki wykonywalne, które zostały podpisane zgodnie z określonymi certyfikatami, zostaną dodane do kategorii użytkownika.

     Informacje o certyfikatach można wyodrębnić tylko z plików wykonywalnych w formacie PE (.exe, .dll, .sys).

- **Metadane plików instalatora MSI**

  Jeśli ta opcja jest zaznaczona, możesz określić plik instalatora MSI jako warunek dodania aplikacji do kategorii użytkownika. Metadane instalatora aplikacji zostaną przesłane do Serwera administracyjnego. Aplikacje, dla których metadane instalatora są takie same jak dla określonego instalatora MSI, zostaną dodane do kategorii użytkownika dla aplikacji.

- **Sumy kontrolne plików z instalatora MSI aplikacji**

  Jeśli ta opcja jest zaznaczona, możesz określić plik instalatora MSI jako warunek dodania aplikacji do kategorii użytkownika. Suma kontrolna plików instalatora aplikacji zostanie przesłana do Serwera administracyjnego. Aplikacje, dla których suma kontrolna pliku instalatora MSI jest taka sama, jak określona suma kontrolna, zostają dodane do kategorii aplikacji użytkownika.

- **Z kategorii KL**

  Jeśli ta opcja jest zaznaczona, możesz określić kategorię aplikacji Kaspersky jako warunek dodania aplikacji do kategorii użytkownika. Aplikacje z określonej kategorii Kaspersky zostaną dodane do kategorii użytkownika dla aplikacji.

- **Określ ścieżkę do aplikacji (maski są obsługiwane)**

  Jeżeli ta opcja zostanie zaznaczona, możesz określić ścieżkę do pliku lub folderu na urządzeniu klienckim zawierający pliki wykonywalne, które zostaną dodane do kategorii użytkownika dla aplikacji. Można użyć wyrażeń regularnych, takich jak *C:\path_to_exe**, na przykład: *C:\Program Files\Internet Explorer**.

- **Wybierz certyfikat z repozytorium**

  Jeśli ta opcja jest zaznaczona, możesz określić certyfikaty z repozytorium. Warunek kategorii obejmuje tylko pliki wykonywalne podpisane określonym certyfikatem.

  Certyfikaty są dodawane do repozytorium, jeśli utworzono i uruchomiono zadanie inwentaryzacji lub zaznaczono pole wyboru **Informacje o uruchomionych aplikacjach** w profilu Kaspersky Endpoint Security. Możesz wykonać obie czynności.

  > Informacje o certyfikatach można wyodrębnić tylko z plików wykonywalnych w formacie PE (.exe, .dll, .sys).

- **Typ dysku**

  Jeżeli ta opcja jest zaznaczona, możesz określić typ nośnika (dowolny dysk lub dysk wymienny), na którym aplikacja jest uruchomiona. Aplikacje, które były uruchomione na wybranym typie urządzenia, zostaną dodane do kategorii użytkownika dla aplikacji.

7. Na stronie kreatora **Tworzenie kategorii aplikacji** kliknij przycisk **Zakończ**.

> Kaspersky Security Center zarządza tylko metadanymi z cyfrowo podpisanych plików. Nie można utworzyć kategorii w oparciu o metadane z plików, które nie zawierają podpisu cyfrowego.

Po zakończeniu działania kreatora, zostanie utworzona kategoria aplikacji użytkownika z zawartością dodaną ręcznie. Nowo utworzoną kategorię można przejrzeć, korzystając z list kategorii w obszarze roboczym folderu **Kategorie aplikacji**.

Jeśli chcesz wyeksportować kategorię aplikacji do pliku KLC, kliknij prawym przyciskiem myszy nazwę kategorii, wybierz z menu opcję **Eksportuj**, a następnie w otwartym oknie podaj nazwę pliku i kliknij przycisk **Zapisz**.

Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń

Możesz użyć plików wykonywalnych z wybranych urządzeń jako szablonu plików wykonywalnych, które chcesz zablokować lub na które chcesz zezwolić. W oparciu o pliki wykonywalne z wybranych urządzeń, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

Aby pobrać listę plików wykonywalnych z urządzeń:

1. Upewnij się, że została utworzona i jest aktywna zasada Kaspersky Endpoint Security for Windows lub Kaspersky Endpoint Security for Linux. Włącz komponent Kontrola aplikacji w zasadzie.
2. Uzyskaj listę plików wykonywalnych przechowywanych na urządzeniach klienckich.

W celu utworzenia kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń:

1. W drzewie konsoli, w folderze **Zaawansowane** → **Zarządzanie aplikacjami** wybierz podfolder **Kategorie aplikacji**.
2. Kliknij przycisk **Nowa kategoria**.

   Zostanie uruchomiony **Kreator tworzenia nowej kategorii**. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Na stronie kreatora **Typ kategorii** wybierz **kategorię, która zawiera pliki wykonywalne z wybranych urządzeń** jako typ kategorii użytkownika.
4. Na stronie kreatora **Wprowadź nazwę kategorii aplikacji** wprowadź nową nazwę kategorii aplikacji.
5. Na stronie kreatora **Ustawienia** kliknij przycisk **Dodaj**.
6. Wybierz urządzenie lub urządzenia, których pliki wykonywalne zostaną użyte do utworzenia kategorii aplikacji.
7. Określ następujące ustawienia:

   - **Algorytm obliczania wartości sumy kontrolnej**

     W zależności od wersji aplikacji zabezpieczającej, zainstalowanej na urządzeniach w sieci, musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w tej kategorii. Informacje o wartościach sumy kontrolnej obliczonych przez funkcje skrótu są przechowywane w bazie danych Serwera administracyjnego.

     SHA256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono luk, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje obsługują obliczanie SHA256. Obliczanie funkcji skrótu MD5 jest obsługiwane przez wszystkie wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w kategorii:

- Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowanych w Twojej sieci to Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowsze wersje, zaznacz pole **SHA256**. Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Może to spowodować błędy w działaniu aplikacji zabezpieczającej. W takim przypadku można użyć kryptograficznej funkcji skrótu MD5 dla plików kategorii.

- Jeśli w Twojej sieci są zainstalowane wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, wybierz **Suma kontrolna MD5**. Nie można dodać kategorii, która została utworzona na podstawie kryterium sumy kontrolnej MD5 pliku wykonywalnego dla Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowszych wersji. W takim przypadku można użyć kryptograficznej funkcji skrótu SHA256 dla plików kategorii.

Jeśli różne urządzenia w Twojej sieci używają zarówno wcześniejszych, jak i nowszych wersji Kaspersky Endpoint Security 10, zaznacz zarówno pole **SHA256**, jak i pole wyboru skrótu **Suma kontrolna MD5**.

Pole **Oblicz SHA256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje)** jest zaznaczone domyślnie.

Pole **Przelicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane w wersjach starszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** jest odznaczone domyślnie.

- **Synchronizuj dane z repozytorium Serwera administracyjnego**

  Wybierz tę opcję, jeśli chcesz, żeby Serwer administracyjny okresowo sprawdzał zmiany w określonym folderze (lub folderach).

  Domyślnie opcja ta jest wyłączona.

  Jeśli włączysz tę opcję, określ przedział czasu (w godzinach), aby sprawdzić zmiany w określonym folderze (folderach). Domyślnie przedział czasu skanowania wynosi 24 godziny.

8. W oknie kreatora **Filtr** ogólne określ następujące ustawienia:

- **Typ pliku**

  W tej sekcji możesz określić typ pliku, który jest używany do tworzenia kategorii aplikacji.

  Wszystkie pliki. Wszystkie pliki są brane pod uwagę podczas tworzenia kategorii. Domyślnie opcja ta jest zaznaczona.

  Tylko pliki spoza kategorii aplikacji. Tylko pliki poza kategoriami aplikacji są brane pod uwagę podczas tworzenia kategorii.

- **Foldery**

  W tej sekcji możesz określić, które foldery z wybranego urządzenia (urządzeń) zawierają pliki używane do tworzenia kategorii aplikacji.

  Wszystkie foldery. Wszystkie foldery są brane pod uwagę podczas tworzenia kategorii. Domyślnie opcja ta jest zaznaczona.

  Określony folder. Tylko określony folder jest brany pod uwagę podczas tworzenia kategorii. Jeśli wybierzesz tę opcję, musisz określić ścieżkę do folderu.

9. Na stronie kreatora **Tworzenie kategorii aplikacji** kliknij przycisk **Zakończ**.

Po zakończeniu pracy kreatora tworzona jest kategoria aplikacji użytkownika. Nowo utworzoną kategorię można przejrzeć, korzystając z list kategorii w obszarze roboczym folderu **Kategorie aplikacji**.

Jeśli chcesz wyeksportować kategorię aplikacji do pliku KLC, kliknij prawym przyciskiem myszy nazwę kategorii, wybierz z menu opcję **Eksportuj**, a następnie w otwartym oknie podaj nazwę pliku i kliknij przycisk **Zapisz**.

Tworzenie kategorii aplikacji zawierającej pliki wykonywalne z określonego folderu

Możesz użyć plików wykonywalnych z wybranego folderu jako standardu plików wykonywalnych, które chcesz zablokować lub na które chcesz zezwolić w swojej organizacji. W oparciu o pliki wykonywalne z wybranego folderu, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii aplikacji, która zawiera pliki wykonywalne z określonego folderu:

1. W drzewie konsoli, w folderze **Zaawansowane** → **Zarządzanie aplikacjami** wybierz podfolder **Kategorie aplikacji**.

2. Kliknij przycisk **Nowa kategoria**.

   Zostanie uruchomiony **Kreator tworzenia nowej kategorii**. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Na stronie kreatora **Typ kategorii** wybierz **kategorię, która zawiera pliki wykonywalne z określonego folderu** jako typ kategorii użytkownika.

4. Na stronie kreatora **Wprowadź nazwę kategorii aplikacji** wprowadź nową nazwę kategorii aplikacji.

5. Na stronie kreatora **Folder repozytorium** kliknij przycisk **Przeglądaj**.

6. Określ folder, którego pliki wykonywalne zostaną użyte do utworzenia kategorii aplikacji.

7. Określ następujące ustawienia:

   - **Uwzględnij w tej kategorii biblioteki dołączane dynamicznie (DLL)**

     Kategoria aplikacji zawiera biblioteki dołączane dynamicznie (pliki w formacie DLL), a składnik Kontrola aplikacji rejestruje akcje takich bibliotek działających w systemie. Włączenie plików DLL do kategorii może obniżyć wydajność Kaspersky Security Center.

     Domyślnie pole to nie jest zaznaczone.

   - **Uwzględnij w tej kategorii dane skryptów**

     Kategoria aplikacji zawiera dane o skryptach, a skrypty nie są blokowane przez moduł Ochrona WWW. Włączenie danych skryptów do kategorii może obniżyć wydajność Kaspersky Security Center.

     Domyślnie pole to nie jest zaznaczone.

   - **Algorytm obliczania wartości sumy kontrolnej**: **Oblicz sumy SHA256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze) / Oblicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane przez starsze wersje niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

     W zależności od wersji aplikacji zabezpieczającej, zainstalowanej na urządzeniach w sieci, musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w tej kategorii. Informacje o wartościach sumy kontrolnej obliczonych przez funkcje skrótu są przechowywane w bazie danych Serwera administracyjnego.

SHA256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono luk, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje obsługują obliczanie SHA256. Obliczanie funkcji skrótu MD5 jest obsługiwane przez wszystkie wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w kategorii:

- Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowanych w Twojej sieci to Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowsze wersje, zaznacz pole **SHA256**. Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Może to spowodować błędy w działaniu aplikacji zabezpieczającej. W takim przypadku można użyć kryptograficznej funkcji skrótu MD5 dla plików kategorii.

- Jeśli w Twojej sieci są zainstalowane wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, wybierz **Suma kontrolna MD5**. Nie można dodać kategorii, która została utworzona na podstawie kryterium sumy kontrolnej MD5 pliku wykonywalnego dla Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowszych wersji. W takim przypadku można użyć kryptograficznej funkcji skrótu SHA256 dla plików kategorii.

Jeśli różne urządzenia w Twojej sieci używają zarówno wcześniejszych, jak i nowszych wersji Kaspersky Endpoint Security 10, zaznacz zarówno pole **SHA256**, jak i pole wyboru skrótu **Suma kontrolna MD5**.

Pole **Oblicz SHA256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje)** jest zaznaczone domyślnie.

Pole **Oblicz MD5 plików należących do tej kategorii (obsługiwane w wersjach starszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** jest odznaczone domyślnie.

- **Wymuś skanowanie folderu pod kątem zmian**

  Jeśli ta opcja jest włączona, aplikacja regularnie sprawdza folder dodawania zawartości kategorii na obecność zmian. Możesz określić częstotliwość skanowań (w godzinach) w polu wejściowym znajdującym się obok pola do zaznaczenia. Domyślnie przedział czasu między wymuszonymi skanowaniami wynosi 24 godziny.

  Jeśli ta opcja jest wyłączona, aplikacja nie wymusza skanowania folderu. Serwer podejmie próbę uzyskania dostępu do plików, jeśli zostały zmodyfikowane, dodane lub usunięte.

  Domyślnie opcja ta jest wyłączona.

8. Na stronie kreatora **Tworzenie kategorii aplikacji** kliknij przycisk **Zakończ**.

   Po zakończeniu pracy kreatora tworzona jest kategoria aplikacji użytkownika. Nowo utworzoną kategorię można przejrzeć, korzystając z list kategorii w obszarze roboczym folderu **Kategorie aplikacji**.

Jeśli chcesz wyeksportować kategorię aplikacji do pliku KLC, kliknij prawym przyciskiem myszy nazwę kategorii, wybierz z menu opcję **Eksportuj**, a następnie w otwartym oknie podaj nazwę pliku i kliknij przycisk **Zapisz**.

Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

Pliki wykonywalne związane ze zdarzeniami **Uruchamianie aplikacji jest zabronione** i **Uruchamianie aplikacji jest zabronione w trybie testowym** możesz dodać do istniejących kategorii aplikacji z zawartością dodaną ręcznie lub do nowej kategorii aplikacji.

W celu dodania plików wykonywalnych związanych ze zdarzeniami Kontroli aplikacji do kategorii aplikacji:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.

2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.

3. Na zakładce **Zdarzenia** wybierz żądane zdarzenia.

4. Z menu kontekstowego jednego z wybranych zdarzeń wybierz **Dodaj do kategorii**.

5. W otwartym oknie **Akcja na pliku wykonywalnym związanym ze zdarzeniem** określ odpowiednie ustawienia:

   Wybierz jeden z następujących elementów:

   - **Dodaj do nowej kategorii aplikacji**

     Wybierz tę opcję, jeśli chcesz utworzyć nową kategorię aplikacji.

     Kliknij przycisk **OK**, aby uruchomić kreatora nowej kategorii. Po zakończeniu działania kreatora, zostaje utworzona kategoria z określonymi ustawieniami.

     Domyślnie ta opcja nie jest zaznaczona.

   - **Dodaj do istniejącej kategorii aplikacji**

     Wybierz tę opcję, jeśli musisz dodać reguły do istniejącej kategorii aplikacji. Wybierz odpowiednią kategorię na liście kategorii aplikacji.

     Opcja ta jest wybrana domyślnie.

   W sekcji **Rodzaj reguły** wybierz jedno z następujących ustawień:

   - **Dodaj do kategorii**

     Wybierz tę opcję, jeśli musisz dodać reguły do warunków kategorii aplikacji.

     Opcja ta jest wybrana domyślnie.

   - **Reguły dodawania do wykluczeń**

     Wybierz tę opcję, jeśli chcesz dodać reguły do wykluczeń kategorii aplikacji.

   W sekcji **Rodzaj informacji o pliku** wybierz jedno z następujących ustawień:

   - **Szczegóły certyfikatu (lub hash SHA256 dla plików bez certyfikatu)**

     Pliki mogą być podpisane certyfikatem. Kilka plików może być podpisanych tym samym certyfikatem. Na przykład, różne wersje tej samej aplikacji mogą być podpisane tym samym certyfikatem lub kilka różnych aplikacji od tego samego producenta może być podpisanych tym samym certyfikatem. Jeśli wybierzesz certyfikat, kilka wersji aplikacji lub kilka aplikacji od tego samego producenta może zostać przydzielonych do kategorii.

     Każdy plik posiada swoją unikatową funkcję skrótu SHA256. Jeśli wybierzesz funkcję skrótu SHA256, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

     Wybierz tę opcję, jeśli chcesz dodać do reguł kategorii szczegóły certyfikatu pliku wykonywalnego (lub funkcję skrótu SHA256 dla plików bez certyfikatu).

     Domyślnie opcja ta jest zaznaczona.

   - **Szczegóły certyfikatu (pliki bez certyfikatu zostaną pominięte)**

     Pliki mogą być podpisane certyfikatem. Kilka plików może być podpisanych tym samym certyfikatem. Na przykład, różne wersje tej samej aplikacji mogą być podpisane tym samym certyfikatem lub kilka różnych aplikacji od tego samego producenta może być podpisanych tym samym certyfikatem. Jeśli wybierzesz certyfikat, kilka wersji aplikacji lub kilka aplikacji od tego samego producenta może zostać przydzielonych do kategorii.

Wybierz tę opcję, jeśli chcesz dodać szczegóły certyfikatu pliku wykonywalnego do reguł kategorii. Jeśli plik wykonywalny nie posiada certyfikatu, ten plik zostanie pominięty. Do kategorii nie zostaną dodane żadne informacje o tym pliku.

- **Tylko SHA256 (pliki bez sumy kontrolnej zostaną pominięte)**

  Każdy plik posiada swoją unikatową funkcję skrótu SHA256. Jeśli wybierzesz funkcję skrótu SHA256, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

  Wybierz tę opcję, jeśli chcesz dodać tylko szczegóły funkcji skrótu SHA256 pliku wykonywalnego.

- **Tylko MD5 (tryb wycofany, wyłącznie dla wersji Kaspersky Endpoint Security 10 Service Pack 1)**

  Każdy plik posiada swoją unikatową funkcję skrótu MD5. Jeśli wybierzesz funkcję skrótu MD5, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

  Wybierz tę opcję, jeśli chcesz dodać tylko szczegóły funkcji skrótu MD5 pliku wykonywalnego. Obliczanie funkcji skrótu MD5 jest obsługiwane w Kaspersky Endpoint Security 10 Service Pack 1 for Windows i późniejszych wersjach.

6. Kliknij **OK**.

Konfigurowanie zarządzania uruchamianiem aplikacji na urządzeniach klienckich

Kategoryzacja aplikacji pozwala na optymalizację zarządzania aplikacjami uruchomionymi na urządzeniach. Możesz utworzyć kategorię aplikacji i skonfigurować Kontrolę aplikacji dla zasady, aby uruchomić tylko aplikacje z określonej kategorii na urządzeniach, na których ta zasada jest stosowana. Na przykład, możesz utworzyć kategorię, która zawiera aplikacje nazwane *Aplikacja_1* oraz *Aplikacja_2*. Po dodaniu tej kategorii do zasady można uruchamiać tylko dwie aplikacje na urządzeniach, na których stosowana jest zasada: *Aplikacja_1* oraz *Aplikacja_2*. Jeśli użytkownik próbuje uruchomić aplikację, która nie została włączona do tej kategorii, na przykład *Aplikacja_3*, uruchomienie tej aplikacji zostaje zablokowane. Użytkownikowi jest wyświetlane powiadomienie informujące, że uruchamianie *Aplikacji_3* jest blokowane, zgodnie z regułą Kontroli aplikacji. Możesz tworzyć kategorie z zawartością dodaną automatycznie na podstawie różnych kryteriów z określonego folderu. W takim przypadku pliki są automatycznie dodawane do kategorii z określonego folderu. Pliki wykonywalne aplikacji są kopiowane do określonego folderu i przetwarzane automatycznie; ich metryki są dodawane do kategorii.

W celu skonfigurowania zarządzania uruchamianiem aplikacji na urządzeniach klienckich:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Kategorie aplikacji**.

2. W obszarze roboczym folderu **Kategorie aplikacji** utwórz kategorię aplikacji, którymi chcesz zarządzać podczas ich uruchamiania.

3. W folderze **Zarządzane urządzenia**, na zakładce **Zasady** kliknij przycisk **Nowa zasada**, aby utworzyć nową zasadę dla Kaspersky Endpoint Security for Windows, i postępuj zgodnie z instrukcjami kreatora.

   Jeśli taka zasada już istnieje, możesz pominąć ten krok. W ustawieniach tej zasady możesz skonfigurować zarządzanie uruchamianiem aplikacji w określonej kategorii. Nowo utworzona zasada jest wyświetlana w folderze **Zarządzane urządzenia**, na zakładce **Zasady**.

4. Z menu kontekstowego zasady dla Kaspersky Endpoint Security for Windows wybierz **Właściwości**.

   Zostanie otwarte okno właściwości zasady dla Kaspersky Endpoint Security for Windows.

5. W oknie właściwości zasady Kaspersky Endpoint Security for Windows, w sekcji **Kontrola zabezpieczeń** → **Kontrola aplikacji** zaznacz pole **Kontrola aplikacji**.

6. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Reguła Kontroli aplikacji**.

7. W oknie **Reguła Kontroli aplikacji**, z listy rozwijalnej **Kategoria** wybierz kategorię aplikacji, dla których stosowana będzie reguła uruchamiania. Skonfiguruj regułę uruchamiania dla określonej kategorii aplikacji.

   W przypadku Kaspersky Endpoint Security 10 Service Pack 2 i nowszych wersji, żadne kategorie nie są wyświetlane, jeśli zostały utworzone zgodnie z kryterium sumy kontrolnej MD5 pliku wykonywalnego.

   Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2. Może to spowodować błędy aplikacji.

   Szczegółowe instrukcje dotyczące konfiguracji reguł kontroli można znaleźć w internetowym systemie pomocy dla Kaspersky Endpoint Security for Windows.

8. Kliknij **OK**.

Aplikacje będą uruchamiane na urządzeniach znajdujących się w określonej kategorii zgodnie z regułą, którą utworzyłeś. Nowo utworzona reguła jest wyświetlana w oknie właściwości zasady Kaspersky Endpoint Security for Windows, w sekcji **Kontrola aplikacji**.

Wyświetlanie wyników analizy statycznej reguł uruchamiania zastosowanych na plikach wykonywalnych

W celu wyświetlenia informacji o plikach wykonywalnych, których użytkownicy nie mogą uruchamiać:

1. W folderze **Zarządzane urządzenia** drzewa konsoli wybierz zakładkę **Zasady**.

2. Z menu kontekstowego zasady dla Kaspersky Endpoint Security for Windows wybierz **Właściwości**.

   Zostanie otwarte okno właściwości zasady aplikacji.

3. Na panelu **Sekcje** wybierz **Kontrola zabezpieczeń**, a następnie wybierz podsekcję **Kontrola aplikacji**.

4. Kliknij przycisk **Analiza statyczna**.

   Zostanie otwarte okno **Analiza listy uprawnień dostępu**. W lewej części okna wyświetlana jest lista użytkowników oparta o dane Active Directory.

5. Wybierz użytkownika z listy.

   Prawa część okna wyświetla kategorie aplikacji przypisane do tego użytkownika.

6. Aby wyświetlić pliki wykonywalne, których użytkownik nie może uruchamiać, w oknie **Analiza listy uprawnień dostępu** kliknij przycisk **Wyświetl pliki**.

   Zostanie otwarte okno wyświetlające listę zabronionych plików wykonywalnych.

7. Aby wyświetlić listę plików wykonywalnych z kategorii, wybierz kategorię aplikacji i kliknij przycisk **Wyświetl pliki w kategorii**.

   Zostanie otwarte okno wyświetlające listę plików wykonywanych uwzględnionych w kategorii aplikacji.

Przeglądanie rejestru aplikacji

Kaspersky Security Center przeprowadza inwentaryzację wszystkich programów zainstalowanych na zarządzanych urządzeniach.

Agent sieciowy tworzy listę aplikacji zainstalowanych na urządzeniu Windows lub Linux, a następnie wysyła ją do Serwera administracyjnego. W przypadku urządzeń klienckich z systemem Windows Agent sieciowy otrzymuje większość informacji o zainstalowanych aplikacjach z rejestru systemu Windows. W przypadku urządzeń klienckich opartych na systemie Linux menedżery pakietów dostarczają Agentowi sieciowemu informacje o zainstalowanych aplikacjach.

W celu przeglądania rejestru aplikacji zainstalowanych na urządzeniach klienckich,

W folderze **Zaawansowane → Zarządzanie aplikacjami** w drzewie konsoli wybierz podfolder **Rejestr aplikacji**.

Obszar roboczy folderu **Rejestr aplikacji** wyświetla listę aplikacji zainstalowanych na urządzeniach klienckich i Serwerze administracyjnym.

Możesz wyświetlić szczegóły dowolnej aplikacji, otwierając jej menu kontekstowe i wybierając **Właściwości**. Okno właściwości aplikacji wyświetla szczegóły dotyczące aplikacji oraz informacje o jej plikach wykonywalnych, a także listę urządzeń, na których zainstalowano aplikację.

W menu kontekstowym dowolnej aplikacji na liście możesz:

- Dodać tę aplikację do kategorii aplikacji.
- Przypisać znacznik do aplikacji.
- Wyeksportować listę aplikacji do pliku CSV lub pliku TXT.
- Przeglądać właściwości aplikacji, na przykład, nazwę producenta, numer wersji, listę plików wykonywalnych, listę urządzeń, na których jest zainstalowana aplikacja, listę dostępnych aktualizacji oprogramowania lub listę wykrytych luk w oprogramowaniu.

Aby wyświetlić aplikacje spełniające określone kryteria, można użyć filtrowania w obszarze roboczym folderu **Rejestr aplikacji**.

W oknie właściwości wykrytego urządzenia, w sekcji **Rejestr aplikacji** możesz przejrzeć listę aplikacji zainstalowanych na urządzeniu.

Generowanie raportu dotyczącego zainstalowanych aplikacji

W obszarze roboczym **Rejestr aplikacji** możesz także kliknąć przycisk **Wyświetl raport o zainstalowanych aplikacjach**, aby wygenerować raport zawierający szczegółowe statystyki dotyczące zainstalowanych aplikacji, w tym liczbę urządzeń, na których każda aplikacja jest zainstalowana. Ten raport, który otwiera stronę **Raport o zainstalowanych aplikacjach**, zawiera informacje o aplikacjach firmy Kaspersky oraz o oprogramowaniu innych firm. Jeśli chcesz tylko informacji na temat aplikacji firmy Kaspersky, zainstalowanych na urządzeniach klienckich, z listy **Podsumowanie** wybierz AO Kaspersky Lab.

Również informacje o aplikacjach Kaspersky i oprogramowaniu firm trzecich zainstalowanych na urządzeniach podłączonych do podrzędnych i wirtualnych Serwerów administracyjnych są przechowywane w rejestrze aplikacji głównego Serwera administracyjnego. Po dodaniu danych z podrzędnych i wirtualnych Serwerów administracyjnych, kliknij przycisk **Wyświetl raport o zainstalowanych aplikacjach**, a na stronie **Raport o zainstalowanych aplikacjach**, która zostanie otwarta, będziesz mógł przejrzeć te informacje.

W celu dodania informacji z podrzędnych i wirtualnych Serwerów administracyjnych do raportu o zainstalowanych aplikacjach:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na zakładce **Raporty** wybierz **Raport o zainstalowanych aplikacjach**.
4. Z menu kontekstowego raportu wybierz **Właściwości**.

   Zostanie otwarte okno **Właściwości: Raport o zainstalowanych aplikacjach**.
5. W sekcji **Hierarchia Serwerów administracyjnych** zaznacz pole **Dołącz dane z podrzędnych i wirtualnych Serwerów administracyjnych**.
6. Kliknij **OK**.

Informacje z podrzędnych i wirtualnych Serwerów administracyjnych będą uwzględnione w **Raport o zainstalowanych aplikacjach**.

Zmienianie czasu uruchomienia inwentaryzacji oprogramowania

Kaspersky Security Center przeprowadza inwentaryzację wszystkich programów zainstalowanych na zarządzanych urządzeniach klienckich działających pod kontrolą systemu Windows.

Agent sieciowy tworzy listę aplikacji zainstalowanych na urządzeniu, a następnie wysyła ją do Serwera administracyjnego. Agent sieciowy automatycznie pobiera informacje o zainstalowanych aplikacjach z rejestru systemu Windows.

Aby zapisać zasoby urządzenia, domyślnie Agent sieciowy rozpoczyna pobieranie informacji o zainstalowanych aplikacjach 10 minut po uruchomieniu usługi Agenta sieciowego.

W celu zmiany czasu uruchomienia inwentaryzacji oprogramowania, który upłynie po uruchomieniu usługi Agenta sieciowego na urządzeniu:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Agent sieciowy (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).
2. Przejdź do gałęzi:

   - W systemach 32-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - W systemach 64-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF

3. Dla klucza KLINV_INV_COLLECTOR_START_DELAY_SEC ustaw żądaną wartość w sekundach.

   Domyślna wartość to 600 sekund.

4. Uruchom ponownie usługę Agenta sieciowego.

Czas uruchomienia inwentaryzacji oprogramowania, który upłynie po uruchomieniu usługi Agenta sieciowego, zostanie zmieniony.

Informacje o zarządzaniu kluczem licencyjnym dla aplikacji innych firm

Kaspersky Security Center umożliwia śledzenie użycia klucza licencyjnego przez aplikacje firm trzecich zainstalowane na zarządzanych urządzeniach. Lista aplikacji, dla których można śledzić użycie klucza licencyjnego, jest pobierana z rejestru aplikacji. Dla każdego klucza licencyjnego można określić i śledzić naruszenie następujących ograniczeń:

- Maksymalna liczba urządzeń, na których aplikacja korzystająca z tego klucza licencyjnego może zostać zainstalowana
- Data wygaśnięcia klucza licencyjnego

Kaspersky Security Center nie sprawdza, czy określiłeś prawdziwy klucz licencyjny. Możesz śledzić tylko określone przez siebie ograniczenia. Jeśli jedno z ograniczeń, które nakładasz na klucz licencyjny, zostanie naruszone, Serwer administracyjny zarejestruje zdarzenie informacyjne, ostrzeżenie lub błąd funkcjonalny.

Klucze licencyjne są powiązane z grupami aplikacji. Grupa aplikacji to grupa aplikacji innych firm, które łączysz na podstawie jednego lub kilku kryteriów. Aplikacje można definiować według nazwy aplikacji, jej wersji, producenta i znacznika. Aplikacja jest dodawana do grupy, jeśli przynajmniej jedno z kryteriów jest spełnione. Do każdej grupy aplikacji można przypisać kilka kluczy licencyjnych, ale każdy klucz licencyjny może być powiązany tylko z jedną grupą aplikacji.

Kolejnym narzędziem, którego można użyć do śledzenia użycia klucza licencyjnego, jest Raport o stanie dotyczącym grup licencjonowanych aplikacji. Ten raport zawiera informacje o aktualnym stanie grup licencjonowanych aplikacji, w tym:

- Liczba instalacji kluczy licencyjnych w każdej grupie aplikacji
- Liczba używanych kluczy licencyjnych i wolnych kluczy licencyjnych
- Szczegółowa lista licencjonowanych aplikacji zainstalowanych na zarządzanych urządzeniach

Narzędzia do zarządzania kluczami licencyjnymi aplikacji innych firm znajdują się w podfolderze **Wykorzystanie licencji firm trzecich** (**Zaawansowane →Zarządzanie aplikacjami →Wykorzystanie licencji firm trzecich**). W tym podfolderze można tworzyć grupy aplikacji, dodawać klucze licencyjne i generować Raport o statnach grup licencjonowanych aplikacji.

Narzędzia do zarządzania kluczami licencyjnymi aplikacji innych firm są dostępne tylko po włączeniu opcji Zarządzanie lukami i poprawkami w oknie **Konfiguruj interfejs**.

Tworzenie grup licencjonowanych aplikacji

W celu utworzenia grupy licencjonowanych aplikacji:

1. W folderze **Zaawansowane → Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Wykorzystanie licencji firm trzecich**.

2. Kliknij przycisk **Dodaj grupę licencjonowanych aplikacji**, aby uruchomić Kreator dodawania grupy licencjonowanych aplikacji.

   Zostanie uruchomiony Kreator dodawania grupy licencjonowanych aplikacji.

3. W kroku **Szczegóły grupy licencjonowanych aplikacji** określ, które aplikacje chcesz uwzględnić w grupie aplikacji:

   - **Nazwa grupy licencjonowanych aplikacji**

   - **Śledź naruszenia ograniczeń**

     Jeśli jedno z ograniczeń, które nakładasz na klucz licencyjny grupy aplikacji, zostanie naruszone, Serwer administracyjny zarejestruje zdarzenie informacyjne, ostrzeżenie lub błąd funkcjonalny:

     - Zdarzenie informacyjne: **Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony (wykorzystywanych jest więcej niż 95%)**

     - Ostrzeżenie: **Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony**

     - Błąd funkcjonalny: **Przekroczono limit instalacji dla jednej z grup licencjonowanych aplikacji**

       Zdarzenie jest rejestrowane tylko raz, gdy określony warunek zostanie spełniony. Następnym razem to samo zdarzenie można zarejestrować tylko wtedy, gdy liczba instalacji powróci do normalnego poziomu, po czym zdarzenie wystąpi ponownie. Nie można zarejestrować zdarzenia częściej niż raz na godzinę.

   - **Kryteria dodawania wykrytych aplikacji do tej grupy licencjonowanych aplikacji**

     Określ kryteria, aby zdefiniować aplikacje, które chcesz uwzględnić w grupie aplikacji. Aplikacje można definiować według nazwy aplikacji, jej wersji, producenta i znacznika. Musisz określić co najmniej jedno kryterium. Aplikacja jest dodawana do grupy, jeśli przynajmniej jedno z kryteriów jest spełnione.

4. W kroku **Wprowadź dane o istniejących kluczach licencyjnych** określ klucze licencyjne, które chcesz śledzić. Wybierz opcję **Kontroluj, jeśli limit licencji zostanie przekroczony**, a następnie dodaj klucze licencyjne:

   a. Kliknij przycisk **Dodaj**.

   b. Wybierz klucz licencyjny, który chcesz dodać, a następnie kliknij przycisk **OK**. Jeśli wymaganego klucza licencyjnego nie ma na liście, kliknij przycisk **Dodaj**, a następnie określ właściwości klucza licencyjnego.

5. W kroku **Dodaj grupę licencjonowanych aplikacji** kliknij przycisk **Zakończ**.

Grupa licencjonowanych aplikacji zostanie utworzona i wyświetlona w folderze **Wykorzystanie licencji firm trzecich**.

Zarządzanie kluczami licencyjnymi dla grup licencjonowanych aplikacji

W celu utworzenia klucza licencyjnego dla grupy licencjonowanych aplikacji:

1. W folderze **Zaawansowane → Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Wykorzystanie licencji firm trzecich**.

2. W obszarze roboczym folderu **Wykorzystanie licencji firm trzecich** kliknij przycisk **Zarządzaj kluczami licencjonowanych aplikacji**.

   Zostanie otwarte okno **Zarządzanie kluczami licencjonowanych aplikacji**.

3. W oknie **Zarządzanie kluczami licencjonowanych aplikacji** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Klucz licencyjny**.

4. W oknie **Klucz licencyjny** określ właściwości klucza licencyjnego i ograniczenia, jakie ten klucz licencyjny nakłada na grupę licencjonowanych aplikacji.

   - **Nazwa**. Nazwa klucza licencyjnego.
   - **Komentarz**. Komentarz dotyczący wybranego klucza licencyjnego.
   - **Ograniczenie**. Liczba urządzeń, na których aplikacja korzystająca z tego klucza licencyjnego może zostać zainstalowana.
   - **Utraci ważność**. Data wygaśnięcia klucza licencyjnego.

Utworzone klucze są wyświetlane w oknie **Zarządzanie kluczami licencjonowanych aplikacji**.

W celu zastosowania klucza licencyjnego do grupy licencjonowanych aplikacji:

1. W folderze **Zaawansowane → Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Wykorzystanie licencji firm trzecich**.

2. W folderze **Wykorzystanie licencji firm trzecich** wybierz grupę licencjonowanych aplikacji, dla której chcesz zastosować klucz licencyjny.

3. Z menu kontekstowego grupy licencjonowanych aplikacji wybierz polecenie **Właściwości**.

   Zostanie otwarte okno właściwości grupy licencjonowanych aplikacji.

4. W oknie właściwości grupy licencjonowanych aplikacji, w sekcji **Klucze licencyjne** wybierz **Kontroluj, jeśli limit licencji zostanie przekroczony**.

5. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Wybierz klucz licencyjny**.

6. W oknie **Wybierz klucz licencyjny** wybierz klucz licencyjny, który chcesz zastosować do grupy licencjonowanych aplikacji.

7. Kliknij **OK**.

Ograniczenia nałożone na grupę licencjonowanych aplikacji i określone w kluczu licencyjnym będą zastosowane do wybranej grupy licencjonowanych aplikacji.

Inwentaryzacja plików wykonywalnych

Możesz uzyskać listę plików wykonywalnych przechowywanych na zarządzanych urządzeniach. Aby przeprowadzić inwentaryzację plików wykonywalnych, należy utworzyć zadanie inwentaryzacji.

Funkcja inwentaryzacji plików wykonywalnych jest dostępna dla następujących aplikacji:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent i nowsze wersje

Liczba plików wykonywalnych pobranych z jednego urządzenia nie może przekraczać 150 000. Po osiągnięciu tego limitu, Kaspersky Security Center nie będzie mógł otrzymywać nowych plików.

Zanim zaczniesz, włącz powiadomienia o uruchamianiu aplikacji w zasadzie Kaspersky Endpoint Security oraz w zasadzie Agenta sieciowego, aby móc przesłać dane do Serwera administracyjnego.

Aby włączyć powiadomienia o uruchomieniu aplikacji:

- Otwórz ustawienia zasad Kaspersky Endpoint Security i wykonaj następujące czynności:
  1. Przejdź do **Ustawienia ogólne** → **Raporty i przechowywanie**.
  2. W sekcji **Transfer danych do Serwera administracyjnego** zaznacz pole **Informacje o uruchomionych aplikacjach**.
  3. Zapisz zmiany.
- Otwórz ustawienia zasad Agenta sieciowego i wykonaj następujące czynności:
  1. Przejdź do sekcji **Repozytoria**.
  2. Zaznacz pole wyboru **Szczegóły zainstalowanych aplikacji**.
  3. Zapisz zmiany.

W celu utworzenia zadania dla plików wykonywalnych na urządzeniach klienckich:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. W obszarze roboczym folderu **Zadania** kliknij przycisk **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.

3. W oknie **Wybierz typ zadania**, jako typ zadania wybierz **Kaspersky Endpoint Security**, a następnie, jako podtyp zadania wskaż **Inwentaryzacja** i kliknij **Dalej**.

4. Wykonaj pozostałe instrukcje kreatora.

   Po zakończeniu pracy kreatora zostanie utworzone zadanie inwentaryzacji dla Kaspersky Endpoint Security. Nowo utworzone zadanie będzie wyświetlane na liście zadań, w obszarze roboczym folderu **Zadania**.

Lista plików wykonywalnych, wykrytych na urządzeniach podczas inwentaryzacji, jest wyświetlana w obszarze roboczym folderu **Pliki wykonywalne**.

Podczas inwentaryzacji aplikacja wykrywa pliki wykonywalne w następujących formatach: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR oraz HTML.

Przeglądanie informacji o plikach wykonywalnych

W celu przejrzenia listy wszystkich plików wykonywalnych wykrytych na urządzeniach klienckich:

W folderze **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Pliki wykonywalne**.

Obszar roboczy folderu **Pliki wykonywalne** wyświetla listę plików wykonywalnych uruchomionych na urządzeniach, bądź też plików wykrytych podczas działania zadania inwentaryzacji programu Kaspersky Endpoint Security for Windows.

Aby wyświetlić szczegóły dotyczące plików wykonywalnych spełniających określone kryteria, możesz użyć filtrowania.

W celu przejrzenia właściwości pliku wykonywalnego:

Wybierając z menu kontekstowego pliku element **Właściwości**.

Zostanie otwarte okno wyświetlające informacje o pliku wykonywalnym oraz listę urządzeń, na których wykryto plik wykonywalny.

Monitorowanie i raportowanie

Ta sekcja opisuje możliwości monitorowania i raportowania Kaspersky Security Center. Te możliwości dają ogląd infrastruktury, stanów ochrony i statystyk.

Po zainstalowaniu programu Kaspersky Security Center lub podczas jego działania, możesz skonfigurować funkcje monitorowania i raportowania, aby najlepiej odpowiadały Twoim potrzebom.

- **Kolory wskaźnika**

  Konsola administracyjna umożliwia szybką ocenę bieżącego stanu Kaspersky Security Center i zarządzanych urządzeń poprzez sprawdzenie wskaźników przypominających sygnalizację świetlną.

- **Statystyki**

  Statystyki dotyczące stanu systemu ochrony i zarządzanych urządzeń są wyświetlane w panelach informacyjnych, które można dostosować.

- **Raporty**

  Raporty umożliwiają uzyskanie szczegółowych informacji liczbowych na temat ochrony sieci Twojej organizacji, zapisania tych informacji w pliku, wysłania ich w wiadomości e-mail oraz ich wydrukowania.

- **Zdarzenia**

  Wybory zdarzeń oferują widok ekranowy nazwanych zestawów zdarzeń, które są wybrane z bazy danych Serwera administracyjnego. Te zestawy zdarzeń są grupowane zgodnie z następującymi kategoriami:

  - Według istotności—**Zdarzenia krytyczne**, **Błędy funkcjonalne**, **Ostrzeżenia** i **Informacja o zdarzeniach**
  - Według czasu—**Ostatnie zdarzenia**
  - Według typu—**Żądania użytkownika** and **Zdarzenia audytu**

Możesz tworzyć i przeglądać wybory zdarzeń zdefiniowane przez użytkownika oparte na ustawieniach dostępnych do konfiguracji w interfejsie Kaspersky Security Center Web Console.

Scenariusz: Monitorowanie i raportowanie

Ta sekcja zawiera scenariusz konfigurowania funkcji monitorowania i raportowania w Kaspersky Security Center.

Wymagania wstępne

Po wdrożeniu Kaspersky Security Center w sieci organizacji, możesz uruchomić jej monitorowanie i wygenerować raporty dotyczące jej funkcjonowania.

Etapy

Monitorowanie i raportowanie w sieci organizacji odbywa się w etapach:

1. **Konfigurowanie przełączania stanów urządzeń**

   Zapoznaj się z ustawieniami, które definiują przypisywanie stanów urządzeń w zależności od określonych warunków. Zmieniając te ustawienia, możesz zmienić liczbę zdarzeń z poziomem istotności *Krytyczne* lub *Ostrzeżenie*.

   Podczas konfigurowania przełączania stanów urządzeń upewnij się, że nowe ustawienia nie kolidują z zasadami bezpieczeństwa informacji Twojej organizacji i że nie możesz reagować na ważne zdarzenia związane z bezpieczeństwem w sieci w Twojej organizacji w odpowiednim momencie.

2. **Konfigurowanie powiadomień o zdarzeniach występujących na urządzeniach klienckich**

   Skonfiguruj powiadamianie (poprzez e-mail, wiadomość SMS lub przez uruchomienie pliku wykonywalnego) o zdarzeniach na urządzeniach klienckich zgodnie z potrzebami Twojej organizacji.

3. **Zmiana reakcji ochrony sieci na zdarzenie Epidemia wirusa**

   Aby dostosować odpowiedź sieci na nowe zdarzenia, możesz zmienić określone wartości progowe we właściwościach Serwera administracyjnego. Możesz także utworzyć rygorystyczną zasadę, która zostanie aktywowana, lub utworzyć zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.

4. **Zarządzanie statystykami**

   Skonfiguruj wyświetlanie statystyk zgodnie z potrzebami Twojej organizacji.

5. **Sprawdzanie stanu ochrony sieci w swojej organizacji**

   W celu przejrzenia stanu ochrony sieci w Twojej organizacji możesz wykonać jedną z następujących czynności:

   - W obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Statystyki** otwórz zakładkę drugiego poziomu (stronę) **Stan ochrony** i przejrzyj panel informacyjny **Stan ochrony w czasie rzeczywistym**
   - Wygeneruj i sprawdź **Raport o stanie ochrony**
   - Wygeneruj i przejrzyj **Raport o błędach**

6. **Lokalizowanie urządzeń klienckich, które nie są chronione**

   Aby zlokalizować urządzenia klienckie, które nie są chronione, przejdź do obszaru roboczego węzła **Serwer administracyjny**, na zakładce **Statystyki** otwórz zakładkę drugiego poziomu (stronę) **Stan ochrony** i przejrzyj panel informacyjny **Historia wykrywania nowych urządzeń w sieci**. Możesz także wygenerować i przejrzeć **Raport wdrażania ochrony**.

7. **Sprawdzanie ochrony urządzeń klienckich**

   Aby sprawdzić ochronę urządzeń klienckich, przejdź do obszaru roboczego węzła **Serwer administracyjny**, na zakładce **Statystyki** otwórz zakładkę drugiego poziomu (stronę) **Wdrażanie** lub **Statystyki zagrożeń** i przejrzyj odpowiednie panele informacyjne. Możesz także uruchomić i przejrzeć wybór zdarzeń **Zdarzenia krytyczne**.

8. **Oszacowanie i ograniczenie nagromadzenia zdarzeń w bazie danych**

   Informacje o zdarzeniach występujących podczas działania zarządzanych aplikacji są przesyłane z urządzenia klienckiego i zapisywane w bazie danych Serwera administracyjnego. Aby zmniejszyć obciążenie na Serwerze administracyjnym, oszacuj i ogranicz maksymalną liczbę zdarzeń przechowywanych w bazie danych.

   Aby ocenić obciążenie bazy danych zdarzeniami, oblicz miejsce w bazie danych. Możesz także ograniczyć maksymalną liczbę zdarzeń, aby uniknąć przepełnienia bazy danych.

9. **Przeglądanie informacji o licencji**

   Aby przejrzeć informacje o licencji, przejdź do obszaru roboczego węzła **Serwer administracyjny**, na zakładce **Statystyki** otwórz zakładkę drugiego poziomu (stronę) **Wdrażanie** i przejrzyj panel informacyjny **Użycie kluczy licencyjnych**. Możesz także wygenerować i przejrzeć **Raport o użyciu kluczy licencyjnych**.

Wyniki

Po zakończeniu scenariusza zostaniesz poinformowany o ochronie sieci w swojej organizacji i tym samym będziesz mógł zaplanować działania związane z dalszą ochroną.

Monitorowanie koloru wskaźnika i rejestrowanych zdarzeń w Konsoli administracyjnej

Konsola administracyjna umożliwia szybką ocenę bieżącego stanu Kaspersky Security Center i zarządzanych urządzeń poprzez sprawdzenie wskaźników przypominających sygnalizację świetlną. Kolory wskaźnika są pokazywane w obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Monitorowanie**. Zakładka udostępnia sześć paneli informacyjnych z kolorowymi wskaźnikami i zarejestrowanymi zdarzeniami. Wskaźnik to kolorowy, pionowy pasek po lewej stronie panelu. Każdy panel ze wskaźnikiem odpowiada określonym zakresom funkcjonalnym Kaspersky Security Center (patrz tabela poniżej).

Kolory ikony wskaźnika w Konsoli administracyjnej

Nazwa panelu	Zakres funkcji
Wdrażanie	Instalacja Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci organizacji
Schemat zarządzania	Struktura grup administracyjnych. Skanowanie sieci. Reguły przenoszenia urządzeń
Ustawienia ochrony	Funkcjonalność aplikacji zabezpieczającej: stan ochrony, skanowanie w poszukiwaniu złośliwego oprogramowania
Aktualizuj	Uaktualnienia i łaty
Monitorowanie	Stan ochrony
Serwer administracyjny	Funkcje Serwera administracyjnego i właściwości

Każdy wskaźnik może przyjąć jeden z pięciu kolorów (patrz tabela poniżej). Kolor wskaźnika zależy od aktualnego stanu Kaspersky Security Center i zdarzeń, które zostały zarejestrowane.

Kolory zestawów

Stan	Kolor wskaźnika	Znaczenie koloru wskaźnika
Informacja	Zielony	Nie jest wymagana interwencja administratora.
Ostrzeżenie	Żółty	Wymagana jest interwencja administratora.
Krytyczny	Czerwony	Wystąpiły poważne problemy. W celu rozwiązania tych problemów wymagana jest interwencja administratora.
Informacja	Niebieski	Wydarzenia, które zostały zarejestrowane, nie są związane z potencjalnymi lub rzeczywistymi zagrożeniami dla bezpieczeństwa zarządzanych urządzeń.
Informacja	Szary	Szczegóły zdarzeń są niedostępne lub nie zostały jeszcze pobrane.

Celem administratora jest zachowanie zielonych kolorów wskaźników na wszystkich panelach informacyjnych, na zakładce **Monitorowanie**.

Panele informacyjne pokazują również zarejestrowane zdarzenia, które mają wpływ na kolory wskaźnika i stan Kaspersky Security Center (patrz tabela poniżej).

Nazwa, opis i kolory wskaźnika zarejestrowanych zdarzeń

Kolor wskaźnika	Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Opis
Czerwony	**Licencja utraciła ważność na %1 urządzeniach**	IDS_AK_STATUS_LIC_EXPAIRED	Tego typu zdarzenia mają miejsce, gdy licencja komercyjna wygasła. Raz dziennie Kaspersky Security Center sprawdza, czy licencja na urządzeniach wygasła. Po wygaśnięciu licencji komercyjnej Kaspersky Security Center zapewnia tylko podstawową funkcjonalność. Aby kontynuować korzystanie z Kaspersky Security Center, musisz odnowić swoją licencję komercyjną.

Kolor wskaźnika	Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Opis
Czerwony	**Aplikacja zabezpieczająca nie jest uruchomiona na %1 urządzeniach**	IDS_AK_STATUS_AV_NOT_RUNNING	Zdarzenia tego typu występują, gdy aplikacja zabezpieczająca zainstalowana na urządzeniu nie jest uruchomiona. Upewnij się, że Kaspersky Endpoint Security jest uruchomiony na urządzeniu.
Czerwony	**Ochrona jest wyłączona na %1 urządzeniach**	IDS_AK_STATUS_RTP_NOT_RUNNING	Zdarzenia tego typu występują, gdy aplikacja zabezpieczająca na urządzeniu jest wyłączona na dłużej niż określony przedział czasu. Sprawdź aktualny stan ochrony w czasie rzeczywistym na urządzeniu i upewnij się, że wszystkie potrzebne składniki ochrony są włączone.
Czerwony	**Na urządzeniach wykryto oprogramowanie zawierające luki**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Zdarzenia tego typu występują, gdy zadanie *Znajdź luki i wymagane aktualizacje* wykryje luki o priorytecie określonym w aplikacjach zainstalowanych na urządzeniu. Zobacz listę dostępnych aktualizacji w podfolderze **Aktualizacje oprogramowania** znajdującym się w folderze **Zarządzanie aplikacjami**. Ten folder zawiera listę aktualizacji pobranych przez Serwer administracyjny dla aplikacji Microsoft i innych producentów oprogramowania, które mogą być przesyłane na urządzenia. Po przejrzeniu informacji o dostępnych aktualizacjach, zainstaluj je na urządzeniu.
Czerwony	**Na Serwerze administracyjnym zostały zarejestrowane zdarzenia krytyczne**	IDS_AK_STATUS_EVENTS_OCCURED	Zdarzenia tego typu występują po wykryciu krytycznych zdarzeń Serwera administracyjnego. Sprawdź listę zdarzeń przechowywaną na Serwerze administracyjnym, a następnie napraw krytyczne zdarzenia jedno po drugim.
Czerwony	**W zdarzeniach na Serwerze administracyjnym zostały zarejestrowane błędy**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Zdarzenia tego typu występują, gdy po stronie Serwera administracyjnego są rejestrowane nieoczekiwane błędy. Sprawdź listę zdarzeń przechowywaną na Serwerze administracyjnym, a następnie napraw błędy jeden po drugim.
Czerwony	**Utracono połączenie z %1 urządzeniami**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Zdarzenia tego typu występują w przypadku utraty połączenia między Serwerem administracyjnym a urządzeniem. Wyświetl listę rozłączonych urządzeń i spróbuj połączyć je ponownie.
Czerwony	**%1 urządzeń od dłuższego czasu nie nawiązało połączenia z Serwerem administracyjnym**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Zdarzenia tego typu występują, gdy urządzenie nie nawiązało połączenia z Serwerem administracyjnym w określonym przedziale czasu, ponieważ urządzenie było wyłączone. Upewnij się, że urządzenie jest włączone i że Agent sieciowy jest uruchomiony.
Czerwony	**Liczba urządzeń posiadających stan inny niż OK: %1**	IDS_AK_STATUS_HOST_NOT_OK	Zdarzenia tego typu występują, gdy stan *OK* urządzenia podłączonego do Serwera administracyjnego zmienia się na *Krytyczny* lub *Ostrzeżenie*. Możesz rozwiązać problem za pomocą narzędzia do zdalnej diagnostyki Kaspersky Security Center.
Czerwony	**Bazy danych są nieaktualne na: %1 urządzeniach**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Zdarzenia tego typu występują, gdy antywirusowe bazy danych nie zostały zaktualizowane na urządzeniu w określonym przedziale czasu. Postępuj zgodnie z instrukcjami, aby zaktualizować bazy danych Kaspersky.

Kolor wskaźnika	Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Opis
Czerwony	**Urządzenia, na których wyszukiwanie aktualizacji systemu Windows nie było wykonywane od dłuższego czasu: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Zdarzenia tego typu występują, gdy zadanie *Wykonaj synchronizację usługi Windows Update* nie zostało uruchomione w określonym przedziale czasu. Postępuj zgodnie z instrukcjami, aby zsynchronizować aktualizacje z Windows Update z Serwerem administracyjnym.
Czerwony	**%1 – liczba wtyczek, które muszą zostać zainstalowane dla Kaspersky Security Center**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Zdarzenia tego typu występują, gdy zachodzi potrzeba zainstalowania dodatkowych wtyczek dla aplikacji Kaspersky. Pobierz i zainstaluj wymagane wtyczki administracyjne dla aplikacji Kaspersky ze strony Pomocy technicznej Kaspersky.

Praca z raportami, statystykami i powiadomieniami

Ta sekcja zawiera informacje dotyczące sposobów pracy z raportami, statystykami i wyborami zdarzeń i urządzeń w Kaspersky Security Center, jak również informacje o konfigurowaniu powiadomień Serwera administracyjnego.

Praca z raportami

Raporty w Kaspersky Security Center zawierają informacje o stanie zarządzanych urządzeń. Raporty są generowane na podstawie informacji przechowywanych na Serwerze administracyjnym. Możesz utworzyć raporty dla następujących typów obiektów:

- Dla wyborów urządzeń utworzonych zgodnie z określonymi ustawieniami.
- Dla grup administracyjnych.
- Dla określonych urządzeń należących do różnych grup administracyjnych.
- Dla wszystkich urządzeń w sieci (w raporcie rozsyłania).

Aplikacja oferuje kilka sztandarowych szablonów raportów. Możliwe jest utworzenie swoich własnych szablonów raportów. Raporty są wyświetlane w oknie głównym aplikacji, w folderze **Serwer administracyjny**.

Tworzenie szablonu raportu

W celu utworzenia szablonu raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Kliknij przycisk **Nowy szablon raportu**.

Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu pracy kreatora, nowo utworzony szablon raportu jest dodawany do wybranego folderu **Serwer administracyjny** drzewa konsoli. Możesz użyć tego szablonu do generowania i wyświetlania raportów.

Przeglądanie i edytowanie właściwości szablonu raportu

Możesz przeglądać i edytować podstawowe właściwości szablonu raportu, na przykład, nazwę szablonu raportu lub pola wyświetlane w raporcie.

W celu przejrzenia i edytowania właściwości szablonu raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportu wybierz żądany szablon raportu.
4. Z menu kontekstowego wybranego szablonu raportu wybierz **Właściwości**.

   Alternatywnie możesz w pierwszej kolejności wygenerować raport, a następnie kliknąć przycisk **Otwórz właściwości szablonu raportu** lub przycisk **Konfiguruj kolumny raportu**.
5. W otwartym oknie edytuj właściwości szablonu raportu. Właściwości każdego raportu mogą zawierać tylko pewne sekcje opisane poniżej.

   - **Sekcja Ogólne**:
     - Nazwa szablonu raportu
     - **Maksymalna liczba wyświetlanych wpisów**

       Jeśli ta opcja jest włączona, liczba wpisów wyświetlanych w tabeli ze szczegółowymi danymi raportu nie wynosi więcej niż określona wartość.

       Wpisy w raporcie są najpierw przechowywane zgodnie z regułami określonymi w sekcji **Pola → Pola szczegółów** właściwości szablonu raportu, a następnie przechowywane są tylko pierwsze wpisy wynikowe. Nagłówek tabeli ze szczegółowymi danymi raportu pokazuje wyświetloną liczbę wpisów oraz całkowitą dostępną liczbę wpisów, które odpowiadają ustawieniom innego szablonu raportu.

       Jeśli ta opcja jest wyłączona, tabela ze szczegółowymi danymi raportu wyświetla wszystkie dostępne wpisy. Nie jest zalecane wyłączenie tej opcji. Ograniczenie liczby wyświetlanych wpisów raportu zmniejsza obciążenie systemu zarządzania bazą danych (DBMS) i skraca czas wymagany do wygenerowania i eksportowania raportu. Niektóre z raportów zawierają zbyt wiele wpisów. W takiej sytuacji może być trudno przeczytać i przeanalizować je wszystkie. Dodatkowo, podczas tworzenia takiego raportu, na Twoim urządzeniu może zabraknąć pamięci, co w konsekwencji uniemożliwi przejrzenie raportu.

       Domyślnie opcja ta jest włączona. Domyślna wartość to 1000.
     - **Wersja do druku**

       Raport wyjściowy jest zoptymalizowany do drukowania: znaki spacji zostały dodane między niektórymi wartościami dla lepszej widoczności.

       Domyślnie opcja ta jest włączona.
   - Sekcja **Pola**

     Wybierz pola, które będą wyświetlane w raporcie, oraz kolejność tych pól, a także skonfiguruj, czy informacje w raporcie muszą być sortowane i filtrowane według każdego z pól.
   - Sekcja **Przedział czasu**

Zmodyfikuj okres dla raportu. Dostępne wartości wyglądają następująco:

- Między dwoma określonymi datami
- Od określonej daty do daty utworzenia raportu
- Od daty utworzenia raportu minus określona liczba dni do daty utworzenia raportu

- Sekcja **Grupa**, **Wybór urządzeń** lub **Urządzenia.**

  Zmień zestaw urządzeń klienckich, dla których tworzony jest raport. Tylko jedna z tych sekcji może być obecna, w zależności od ustawień określonych podczas tworzenia szablonu raportu.

- Sekcja **Ustawienia**.

  Zmień ustawienia raportu. Dokładny zestaw ustawień zależy od określonego raportu.

- Sekcja **Zabezpieczenia**. **Dziedzicz ustawienia od Serwera administracyjnego**

  Jeśli ta opcja jest włączona, ustawienia zabezpieczeń raportu są dziedziczone od Serwera administracyjnego.

  Jeśli ta opcja jest wyłączona, możesz skonfigurować ustawienia zabezpieczeń dla raportu. Możesz przypisać rolę do użytkownika lub grupy użytkowników lub przypisać uprawnienia do użytkownika lub grupy użytkowników, jak zastosowano do raportu.

  Domyślnie opcja ta jest włączona.

  > Sekcja **Zabezpieczenia** jest dostępna, jeśli w oknie ustawień interfejsu dostępne jest pole **Wyświetl sekcje ustawień zabezpieczeń**.

- Sekcja **Hierarchia Serwerów administracyjnych**:

  - **Dołącz dane z podrzędnych i wirtualnych Serwerów administracyjnych**

    Jeśli ta opcja jest włączona, raport zawiera informacje z podrzędnych i wirtualnych Serwerów administracyjnych, które podlegają Serwerowi administracyjnemu, dla którego utworzono szablon raportu.

    Wyłącz tę opcję, jeśli chcesz przejrzeć dane tylko z bieżącego Serwera administracyjnego.

    Domyślnie opcja ta jest włączona.

  - **Do poziomu zagnieżdżenia**

    Raport zawiera dane z podrzędnych i wirtualnych Serwerów administracyjnych, które znajdują się pod bieżącym Serwerem administracyjnym na poziomie zagnieżdżenia, który jest mniejszy niż lub równy określonej wartości.

    Domyślna wartość to 1. Możesz chcieć zmienić tę wartość, jeśli musisz zbierać informacje z podrzędnych Serwerów administracyjnych znajdujących się na niższych poziomach drzewa.

  - **Czas oczekiwania na dane (min)**

    Przed wygenerowaniem raportu, Serwer administracyjny, dla którego tworzony jest szablon raportu, oczekuje na dane z podrzędnych Serwerów administracyjnych przez określoną liczbę minut. Jeśli żadne dane nie są pobierane z podrzędnego Serwera administracyjnego pod koniec tego okresu, raport i tak zostanie uruchomiony. Zamiast rzeczywistych danych, raport wyświetla dane pobrane z pamięci podręcznej (jeśli opcja **Buforuj dane z podrzędnych Serwerów administracyjnych** jest włączona) lub **N/D** (nie jest dostępne) w innym przypadku.

    Domyślna wartość to 5 (minuty).

- **Buforuj dane z podrzędnych Serwerów administracyjnych**

  Podrzędne Serwery administracyjne regularnie przesyłają dane do Serwera administracyjnego, dla którego został utworzony szablon raportu. Przesłane dane są przechowywane w pamięci podręcznej.

  Jeśli podczas generowania raportu bieżący Serwer administracyjny nie może odbierać danych z podrzędnego Serwera administracyjnego, raport wyświetla dane pobrane z pamięci podręcznej. Wyświetlana jest także data przesłania danych do pamięci podręcznej.

  Włączenie tej opcji umożliwia przeglądanie informacji z podrzędnych Serwerów administracyjnych nawet wtedy, gdy aktualne dane nie mogą zostać pobrane. Jednakże wyświetlane dane mogą być przestarzałe.

  Domyślnie opcja ta jest wyłączona.

- **Częstotliwość aktualizacji pamięci podręcznej (godz.)**

  Podrzędne Serwery administracyjne regularnie przesyłają dane do Serwera administracyjnego, dla którego został utworzony szablon raportu. Możesz określić ten okres w godzinach. Jeśli określisz 0 godzin, dane są przesyłane tylko wtedy, gdy raport zostaje wygenerowany.

  Domyślna wartość to 0.

- **Prześlij szczegółowe informacje z podrzędnych Serwerów administracyjnych**

  W wygenerowanym raporcie tabela ze szczegółowymi danymi raportu zawiera dane z podrzędnych Serwerów administracyjnych Serwera administracyjnego, dla którego został utworzony szablon raportu.

  Włączenie tej opcji spowalnia tworzenie raportu i zwiększa ruch sieciowy między Serwerami administracyjnymi. Jednakże możesz przejrzeć wszystkie dane w jednym raporcie.

  Zamiast włączyć tę opcję, możesz chcieć przeanalizować szczegółowe dane raportu, aby wykryć wadliwy podrzędny Serwer administracyjny, a następnie wygenerować ten sam raport tylko dla tego wadliwego Serwera administracyjnego.

  Domyślnie opcja ta jest wyłączona.

Rozszerzony format filtra w szablonach raportu

W Kaspersky Security Center 15.1 możesz zastosować rozszerzony format filtra do szablonu raportu. Rozszerzony format filtra zapewnia większą elastyczność w porównaniu z domyślnym formatem. Możesz utworzyć złożone warunki filtrowania przy użyciu zestawu filtrów, które będą stosowane do raportu przy użyciu operatora logicznego LUB podczas tworzenia raportu w sposób opisany poniżej:

Filter[1](Field[1] AND Field[2]... AND Field[n]) OR Filter[2](Field[1] AND Field[2]... AND Field[n]) OR... Filter[n](Field[1] AND Field[2]... AND Field[n])

Dodatkowo, przy użyciu rozszerzonego formatu filtra możesz określić wartość przedziału czasu w odpowiednim formacie czasu (na przykład, korzystając z warunku „Przez ostatnie N dni") dla określonych pól w filtrze. Dostępność i zestaw warunków przedziału czasu zależy od typu szablonu raportu.

Konwertowanie filtra do rozszerzonego formatu

Format rozszerzonego filtra dla szablonów raportów jest obsługiwany tylko w Kaspersky Security Center 12 i nowszych wersjach. Po konwersji domyślnego filtra do rozszerzonego formatu, szablon raportu stanie się niekompatybilny z Serwerami administracyjnymi w Twojej sieci, w której znajdują się zainstalowane wcześniejsze wersje Kaspersky Security Center. Informacje z tych Serwerów administracyjnych nie zostaną odebrane dla raportu.

W celu przekonwertowania domyślnego filtra szablonu raportu do formatu rozszerzonego:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportu wybierz żądany szablon raportu.
4. Z menu kontekstowego wybranego szablonu raportu wybierz **Właściwości**.
5. W otwartym oknie właściwości wybierz sekcję **Pola**.
6. Na zakładce **Pola szczegółów** kliknij odnośnik **Konwertuj filtr**.
7. W otwartym oknie kliknij przycisk **OK**.

   Konwersja do rozszerzonego formatu filtra jest nieodwracalna dla szablonu raportu, do którego jest stosowana. Jeśli kliknąłeś odnośnik **Konwertuj filtr** przez przypadek, możesz anulować wprowadzone zmiany poprzez kliknięcie przycisku **Anuluj** w oknie właściwości szablonu raportu.

8. Aby zastosować wprowadzone zmiany, zamknij okno właściwości szablonu raportu, klikając przycisk **OK**.

   Jeśli okno właściwości szablonu raportu zostanie otwarte ponownie, zostanie wyświetlona nowo dostępna sekcja **Filtry**. W tej sekcji możesz skonfigurować rozszerzony filtr.

Konfigurowanie rozszerzonego filtra

W celu skonfigurowania rozszerzonego filtra we właściwościach szablonu raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportów wybierz szablon raportu, który wcześniej został przekonwertowany do formatu rozszerzonego filtra.
4. Z menu kontekstowego wybranego szablonu raportu wybierz **Właściwości**.
5. W otwartym oknie właściwości wybierz sekcję **Filtry**.

   Sekcja **Filtry** nie jest wyświetlana, jeśli szablon raportu nie został wcześniej przekonwertowany do formatu rozszerzonego filtra.

   W sekcji **Filtry** okna właściwości szablonu raportu możesz przejrzeć i zmodyfikować listę filtrów stosowanych do raportu. Każdy filtr na liście posiada unikatową nazwę i przedstawia zestaw filtrów dla odpowiednich pól w raporcie.

6. Otwórz okno ustawień filtra w jeden z następujących sposobów:

   - Aby utworzyć nowy filtr, kliknij przycisk **Dodaj**.
   - Aby zmodyfikować istniejący filtr, wybierz żądany filtr i kliknij przycisk **Modyfikuj**.

7. W otwartym oknie wybierz i określ wartości wymaganych pól filtra.
8. Aby zapisać wprowadzone zmiany i zamknąć okno, kliknij przycisk **OK**.

   Jeśli tworzysz nowy filtr, nazwa filtra musi zostać określona w polu **Nazwa filtra** przed kliknięciem przycisku **OK**.

9. Zamknij okno właściwości szablonu raportu, klikając przycisk **OK**.

   Rozszerzony filtr w szablonie raportu zostanie skonfigurowany. Teraz możesz tworzyć raporty, korzystając z szablonu raportu.

Tworzenie i przeglądanie raportu

W celu utworzenia i przejrzenia raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportu kliknij dwukrotnie żądany szablon raportu.

   Zostanie wyświetlony raport dla wybranego szablonu.

Raport wyświetla następujące dane:

- Nazwę i typ raportu, krótki opis i okres raportowania, a także informacje o grupie urządzeń, dla których generowany jest raport.
- Wykres graficzny przedstawiający najbardziej reprezentatywne dane raportu.
- Tabelę zbiorczą z wyliczonymi wskaźnikami raportu.
- Tabelę ze szczegółowymi danymi raportu.

Zapisywanie raportu

W celu zapisania utworzonego raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportu wybierz żądany szablon raportu.
4. Z menu kontekstowego wybranego szablonu raportu wybierz **Zapisz**.

Zostanie uruchomiony Kreator zapisywania raportu. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu pracy kreatora, zostanie otwarty folder, w którym znajduje się zapisany plik raportu.

Podczas zapisywania raportu jako plik XLS wszystkie powiązane obrazy, takie jak logo i datagram, są zapisywane jako osobne pliki.

Tworzenie zadania dostarczania raportu

Raporty mogą być wysyłane za pośrednictwem poczty elektronicznej. Dostarczanie raportów w Kaspersky Security Center jest wykonywane przez zadanie dostarczania raportów.

W celu utworzenia zadania dostarczenia jednego raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportu wybierz żądany szablon raportu.
4. Z menu kontekstowego wybranego szablonu raportu wybierz **Dostarcz raporty**.

   Zostanie uruchomiony Kreator tworzenia zadania dostarczania raportu. Postępuj zgodnie z instrukcjami kreatora.

W celu utworzenia zadania dostarczania kilku raportów:

1. Z drzewa konsoli, w węźle z nazwą żądanego Serwera administracyjnego wybierz folder **Zadania**.
2. W obszarze roboczym folderu **Zadania** kliknij przycisk **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   Nowo utworzone zadanie dostarczania raportów będzie wyświetlane w folderze **Zadania** drzewa konsoli.

Zadanie dostarczania raportu jest tworzone automatycznie, jeśli w trakcie instalacji Kaspersky Security Center określono ustawienia e-mail.

Krok 1. Wybieranie typu zadania

W oknie **Wybierz typ zadania**, na liście zadań jako typ zadania wybierz **Dostarcz raporty**.

Kliknij **Dalej**, aby przejść do kolejnego kroku.

Krok 2. Wybieranie typu raportu

W oknie **Wybierz typ raportu**, na liście szablonów tworzenia zadania wybierz typ raportu.

Kliknij **Dalej**, aby przejść do kolejnego kroku.

Krok 3. Działania podejmowane na raporcie

W oknie **Akcja stosowana wobec raportów** określ następujące ustawienia:

- **Wysyłaj raporty przy użyciu e-mail**

  Jeśli ta opcja jest włączona, aplikacja wyśle wygenerowane raporty za pośrednictwem poczty elektronicznej.

  Wysyłanie raportów w wiadomości e-mail można skonfigurować po kliknięciu odnośnika **Ustawienia powiadomień e-mail**. Odnośnik jest dostępny, jeśli ta opcja jest włączona.

  Jeśli ta opcja jest wyłączona, aplikacja zapisze raporty w folderze wskazanym do ich przechowywania.

  Domyślnie opcja ta jest wyłączona.

- **Zapisuj raporty w folderze współdzielonym**

  Jeśli ta opcja jest włączona, aplikacja zapisze raporty do folderu, który został określony w polu pod opcją do zaznaczenia. Aby zapisać raporty w folderze współdzielonym, określ ścieżkę UNC do folderu. W tym przypadku, w oknie **Wybieranie konta do uruchomienia zadania** musisz określić konto użytkownika i hasło dostępu do tego folderu.

  Jeśli ta opcja jest wyłączona, aplikacja nie zapisze raportów do folderu, a zamiast tego wyśle je za pośrednictwem poczty elektronicznej.

  Domyślnie opcja ta jest wyłączona.

- **Nadpisz starsze raporty tego samego typu**

  Jeśli ta opcja jest włączona, przy każdym uruchomieniu zadania nowy plik raportu nadpisze plik zapisany w folderze raportów przy poprzednim uruchomieniu zadania.

  Jeśli ta opcja jest wyłączona, pliki raportów nie będą nadpisywane. Nowy plik raportu jest przechowywany w folderze raportów przy każdym uruchomieniu zadania.

  To pole jest dostępne, jeśli zaznaczona jest opcja **Zapisz raport do folderu**.

  Domyślnie opcja ta jest wyłączona.

- **Określ konto, które ma mieć dostęp do folderu współdzielonego**

  Jeśli ta opcja jest włączona, możesz określić konto, z poziomu którego raport zostanie zapisany do folderu. Jeśli ścieżka UNC do folderu współdzielonego jest określona jako ustawienie **Zapisz raport w folderze** w oknie **Akcja stosowana wobec raportów**, musisz określić konto użytkownika i hasło dostępu do tego folderu.

  Jeśli ta opcja jest wyłączona, raport zostanie zapisany do folderu z poziomu konta Serwera administracyjnego.

  To pole jest dostępne, jeśli zaznaczona jest opcja **Zapisz raport do folderu**.

  Domyślnie opcja ta jest wyłączona.

Podczas zapisywania lub wysyłania raportu jako plik XLS wszystkie powiązane obrazy, takie jak logo i datagram, są zapisywane jako osobne pliki.

Kliknij **Dalej**, aby przejść do kolejnego kroku.

Krok 4. Wybieranie konta do uruchamiania zadania

W oknie **Wybieranie konta do uruchomienia zadania** możesz określić, które konto ma być używane podczas uruchamiania zadania. Wybierz jedną z następujących opcji:

- **Konto domyślne**

  Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

  Domyślnie opcja ta jest zaznaczona.

- **Określ konto**

  Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

  - **Konto**

    Konto, z poziomu którego zadanie jest uruchamiane.

  - **Hasło**

    Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

Kliknij **Dalej**, aby przejść do kolejnego kroku.

Krok 5. Konfigurowanie terminarza zadania

W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, zdefiniuj następujące ustawienia:

- **Zaplanowane uruchomienie:**

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - **Co N godzin**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

  - **Co N dni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

    Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Co N tygodni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

    Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

  - **Co N minut**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

    Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

  - **Codziennie (czas letni nie jest obsługiwany)**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

    Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

    Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

  - **Co tydzień**

    Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

  - **Według dni tygodnia**

    Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

    Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

- Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
- Kliknij ikonę sortowania, aby posortować zadania według nazwy.

  Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
- Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

Krok 6. Definiowanie nazwy zadania

W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych (`"*<>?\:|`).

Kliknij **Dalej**, aby przejść do kolejnego kroku.

Krok 7. Kończenie tworzenia zadania

W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zakończyć pracę kreatora.

Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Zarządzanie statystykami

Statystyki dotyczące stanu systemu ochrony i zarządzanych urządzeń są wyświetlane w panelach informacyjnych, które można dostosować. Statystyki są wyświetlane w obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Statystyki**. Zakładka zawiera kilka zakładek (stron) drugiego poziomu. Każda strona wyświetla panele informacyjne ze statystykami, a także odnośniki do nowości i innych materiałów z Kaspersky. Informacje statystyczne są wyświetlane na panelach informacyjnych jako tabela lub wykres (kołowy lub słupkowy). Dane w panelach informacyjnych są aktualizowane w trakcie działania aplikacji i odzwierciedlają bieżący stan aplikacji antywirusowej.

Możesz zmodyfikować zestaw zakładek drugiego poziomu na zakładce **Statystyki**, zmienić liczbę paneli informacyjnych na każdej zakładce oraz tryb wyświetlania danych w panelach informacyjnych.

*W celu dodania nowej zakładki drugiego poziomu z panelami informacyjnymi na zakładce **Statystyki**:*

1. Kliknij przycisk **Dostosuj widok** znajdujący się w prawym górnym rogu zakładki **Statystyki**.

   Zostanie otwarte okno właściwości statystyk. To okno zawiera listę zakładek, które są aktualnie wyświetlane na zakładce **Statystyki**. W tym oknie możesz zmienić kolejność wyświetlania stron na zakładce, dodać i usunąć strony, a także skonfigurować właściwości strony, klikając przycisk **Właściwości**.

2. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno właściwości nowej strony.

3. Skonfiguruj nową stronę:

   - W sekcji **Ogólne** określ nazwę strony.

   - W sekcji **Panele informacyjne** kliknij przycisk **Dodaj**, aby dodać panele informacyjne, które mają być wyświetlane na stronie.

     W sekcji **Panele informacyjne** kliknij przycisk **Właściwości**, aby skonfigurować właściwości dodanych paneli informacyjnych: nazwę, typ i wygląd wykresu na panelu oraz dane niezbędne do utworzenia wykresu.

4. Kliknij **OK**.

Strona z panelami informacyjnymi, które dodałeś, pojawi się na zakładce **Statystyki**. Kliknij ikonę ustawienia (⚙), aby natychmiast przejść do konfiguracji strony lub wybranego panelu informacyjnego na tej stronie.

Konfigurowanie powiadomień o zdarzeniach

Kaspersky Security Center umożliwia wybranie metody powiadamiania administratora o zdarzeniach występujących na urządzeniach klienckich oraz skonfigurowanie powiadomień:

- Poprzez e-mail. Po wystąpieniu zdarzenia, aplikacja wyśle powiadomienie na określone adresy e-mail. Możesz zmodyfikować treść powiadomienia.

- Za pośrednictwem wiadomości SMS. Po wystąpieniu zdarzenia, aplikacja wyśle powiadomienie na określone numery telefonu. Możesz skonfigurować wysyłanie powiadomień SMS poprzez bramkę pocztową.

- Poprzez uruchomienie pliku wykonywalnego. Po wystąpieniu zdarzenia na urządzeniu, na stacji roboczej administratora zostanie uruchomiony plik wykonywalny. Korzystając z pliku wykonywalnego, administrator może pobrać parametry dowolnego zdarzenia, które wystąpiło.

W celu skonfigurowania wysyłania powiadomień o zdarzeniach występujących na urządzeniach klienckich:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Kliknij odnośnik **Konfiguruj powiadomienia i eksportowanie zdarzeń** i z listy rozwijalnej wybierz wartość **Konfiguruj powiadomienia**.

   Spowoduje to otwarcie okna **Właściwości: Zdarzenia**.
4. W sekcji **Powiadamianie** wybierz metodę powiadamiania (poprzez e-mail, za pośrednictwem wiadomości SMS lub przez uruchomienie pliku wykonywalnego) i zdefiniuj ustawienia powiadomień:

   - **E-mail**

     Zakładka **E-mail** umożliwia skonfigurowanie wysyłania powiadomień o zdarzeniach za pośrednictwem poczty elektronicznej.

     W polu **Adresaci (adresy e-mail)** określ adresy e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami.

     W polu **Serwer SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

     - Adres IPv4 lub IPv6
     - Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
     - Nazwa DNS serwera SMTP

     W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

     Jeśli włączysz opcję **Użyj przeszukiwania DNS MX**, możesz użyć kilku wpisów MX adresów IP dla tej samej nazwy DNS serwera SMTP. Ta sama nazwa DNS może posiadać kilka wpisów MX z różnymi wartościami priorytetu odbierania wiadomości e-mail. Serwer administracyjny spróbuje wysłać powiadomienia e-mail do serwera SMTP w kolejności rosnącej priorytetów wpisów MX. Domyślnie opcja ta jest wyłączona.

     > Jeśli włączysz opcję **Użyj przeszukiwania DNS MX** i nie włączysz korzystania z ustawień TLS, zalecane jest użycie ustawień DNSSEC na urządzeniu serwerowym jako dodatkowego środka ochrony wysyłania powiadomień e-mail.

     Kliknij odnośnik **Ustawienia**, aby zdefiniować dodatkowe ustawienia powiadomień:

     - Nazwa podmiotu (nazwa podmiotu wiadomości e-mail)
     - Adres e-mail nadawcy
     - Ustawienia uwierzytelniania ESMTP

     Jeśli dla serwera SMTP włączono uwierzytelnianie ESMTP, do autoryzacji na serwerze SMTP należy określić konto.

     - Ustawienia TLS dla serwera SMTP:
       - **Nie korzystaj z TLS**

         Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.
       - **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.

- **Zawsze używaj TLS, sprawdź certyfikat serwera pod kątem ważności**

Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź certyfikat serwera pod kątem ważności**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

Możesz określić ustawienia TLS dla serwera SMTP:

- Odszukaj plik certyfikatu serwera SMTP:

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

- Odszukaj plik certyfikatu klienta:

Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

- Certyfikat X-509:

Musisz określić plik z certyfikatem oraz plik z kluczem prywatnym. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po załadowaniu obu plików należy określić hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

- Kontener pkcs12:

Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

Pole **Treść powiadomienia** zawiera standardowy tekst z informacjami dotyczącymi zdarzenia, który aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera dodatkowe parametry, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny. Istnieje możliwość zmodyfikowania treści wiadomości poprzez dodanie innych parametrów zastępczych z bardziej szczegółowymi danymi dotyczącymi zdarzenia. Lista dodatkowych parametrów jest dostępna po kliknięciu przycisku, znajdującego się z prawej strony pola.

Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%”.

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy poprawnie skonfigurowałeś powiadomienia. Aplikacja powinna wysłać powiadomienie testowe na adresy e-mail, które określiłeś.

- **SMS**

  Na zakładce **SMS** możesz skonfigurować wysyłanie powiadomień SMS o różnych zdarzeniach na telefon komórkowy. Wiadomości SMS są wysyłane poprzez bramkę pocztową.

  W polu **Odbiorcy (adresy e-mail)** określ adres e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami. Powiadomienia będą dostarczane na numery telefonów skojarzone z określonymi adresami e-mail.

  W polu **Serwery SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

  - Adres IPv4 lub IPv6
  - Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
  - Nazwa DNS serwera SMTP

  W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

  Kliknij odnośnik **Ustawienia**, aby zdefiniować dodatkowe ustawienia powiadomień:

  - Nazwa podmiotu (nazwa podmiotu wiadomości e-mail)
  - Adres e-mail nadawcy
  - Ustawienia uwierzytelniania ESMTP

  Jeśli to konieczne, jeśli dla serwera SMTP włączono uwierzytelnianie ESMTP, do autoryzacji na serwerze SMTP możesz określić konto.

  - Ustawienia TLS dla serwera SMTP

  Możesz wyłączyć korzystanie z TLS, użyć TLS, jeśli serwer SMTP obsługuje ten protokół lub możesz wymusić użycie tylko TLS. Jeśli zdecydujesz się używać tylko TLS, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Dodatkowo, jeśli wybierzesz używanie tylko TLS, możesz określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

  - Odszukaj plik certyfikatu serwera SMTP

  Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Kaspersky Security Center. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

  Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może zawierać pustą wartość, jeśli klucz prywatny nie zostanie zakodowane. Pole **Treść powiadomienia** zawiera standardowy tekst z informacjami o zdarzeniu, które aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera dodatkowe parametry, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny. Istnieje możliwość zmodyfikowania treści wiadomości poprzez dodanie innych parametrów zastępczych z bardziej szczegółowymi danymi dotyczącymi zdarzenia. Lista dodatkowych parametrów jest dostępna po kliknięciu przycisku, znajdującego się z prawej strony pola.

  Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%”.

  Kliknij odnośnik **Ustaw limit liczby powiadomień**, aby określić maksymalną liczbę powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

  Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy powiadomienia zostały skonfigurowane poprawnie. Aplikacja powinna wysłać powiadomienie testowe do określonych odbiorców.

- **Plik wykonywalny do uruchomienia**

  Jeśli wybrana jest ta metoda powiadamiania, w polu wejściowym określ aplikację, która zostanie uruchomiona, gdy wystąpi zdarzenie.

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Przycisk **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie na wskazany adres e-mail.

5. W polu **Treść powiadomienia** wprowadź tekst, który aplikacja wyśle po wystąpieniu zdarzenia.

   Możesz użyć listy rozwijanej znajdującej się na prawo od pola tekstowego, aby dodać dodatkowe ustawienia ze szczegółami zdarzenia (na przykład: opis zdarzenia lub czas wystąpienia).

   > Jeżeli tekst powiadomienia zawiera znak %, należy go określić dwukrotnie, aby umożliwić wysłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%".

6. Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy powiadomienia zostały skonfigurowane poprawnie.

   Aplikacja wysyła powiadomienie testowe do określonego użytkownika.

7. Kliknij **OK**, aby zachować zmiany.

Skonfigurowane ustawienia powiadamiania zostaną zastosowane do wszystkich zdarzeń występujących na urządzeniach klienckich.

Możesz zastąpić ustawienia powiadamiania dla pewnych zdarzeń w sekcji **Konfiguracja zdarzenia** ustawień Serwera administracyjnego, ustawień zasady lub ustawień aplikacji.

Tworzenie certyfikatu dla serwera SMTP

W celu utworzenia certyfikatu dla serwera SMTP:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Kliknij odnośnik **Konfiguruj powiadomienia i eksportowanie zdarzeń** i z listy rozwijalnej wybierz wartość **Konfiguruj powiadomienia**.

   Zostanie otwarte okno właściwości zdarzenia.

4. Na zakładce **E-mail** kliknij odnośnik **Ustawienia**, aby otworzyć okno **Ustawienia**.
5. W oknie **Ustawienia** kliknij odnośnik **Określ certyfikat**, aby otworzyć okno **Certyfikat do podpisu**.
6. W oknie **Certyfikat do podpisu** kliknij przycisk **Przeglądaj**.

   Zostanie otwarte okno **Certyfikat**.

7. Z listy rozwijalnej **Typ certyfikatu** wybierz typ certyfikatu - publiczny lub prywatny:

   - Jeśli wybrany jest certyfikat prywatny (**Kontener PKCS #12**), określ plik certyfikatu i hasło.
   - Jeśli wybrany jest certyfikat publiczny (**Certyfikat X.509**):

     a. Określ plik klucza prywatnego (z rozszerzeniem *.prk lub *.pem).

     b. Określ hasło dla klucza prywatnego.

     c. Określ plik klucza publicznego (z rozszerzeniem *.cer).

8. Kliknij **OK**.

Zostanie utworzony certyfikat dla serwera SMTP.

Wybory zdarzeń

Informacje o zdarzeniach, które wystąpiły w trakcie działania Kaspersky Security Center i zarządzanych aplikacji, są zapisywane w bazie danych Serwera Administracyjnego i w dzienniku systemu Microsoft Windows. Możesz przejrzeć informacje z bazy danych Serwera administracyjnego w obszarze roboczym węzła **Serwer Administracyjny**, na zakładce **Zdarzenia**.

Informacje na zakładce **Zdarzenia** są przedstawione pod postacią listy wyborów zdarzeń. Każdy wybór zawiera tylko zdarzenia określonego typu. Na przykład, wybór „Stan urządzenia jest Krytyczny" zawiera tylko wpisy dotyczące zmiany stanów urządzeń na „Krytyczny". Po zainstalowaniu aplikacji, zakładka **Zdarzenia** posiada kilka standardowych wyborów zdarzeń. Możesz tworzyć dodatkowe (niestandardowe) wybory zdarzeń lub eksportować informacje o zdarzeniach do pliku.

Przeglądanie wyboru zdarzeń

W celu przejrzenia wyboru zdarzeń:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Z listy rozwijalnej **Wybory zdarzeń** wybierz żądany wybór zdarzeń.

   Jeśli chcesz, żeby zdarzenia z tego wyboru były cały czas wyświetlane w obszarze roboczym, kliknij ikonę gwiazdki (☆) znajdującą się obok wyboru.

   Obszar roboczy będzie wyświetlał listę zdarzeń wybranego typu, przechowywanych na Serwerze administracyjnym.

Informacje przedstawione na liście zdarzeń mogą być sortowane (rosnąco lub malejąco) według dowolnej kolumny.

Dostosowywanie wyboru zdarzeń

W celu dostosowania wyboru zdarzeń:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Na zakładce **Zdarzenia** otwórz żądany wybór zdarzeń.
4. Kliknij przycisk **Właściwości wyboru**.

   W otwartym oknie właściwości wyboru zdarzeń możesz skonfigurować wybór zdarzeń.

Tworzenie kryterium wyboru zdarzenia

W celu utworzenia wyboru zdarzeń:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Kliknij przycisk **Utwórz wybór**.
4. W oknie **Nowy wybór zdarzeń**, które zostanie otwarte, wprowadź nazwę nowego wyboru i kliknij **OK**.

   Na liście rozwijalnej **Wybory zdarzeń** zostanie utworzony wybór pod nazwą, którą określiłeś.

Domyślnie utworzone kryterium wyboru zdarzeń zawiera wszystkie zdarzenia przechowywane na Serwerze administracyjnym. Aby wybór wyświetlał tylko żądane zdarzenia, należy go skonfigurować.

Eksportowanie wyboru zdarzeń do pliku tekstowego

W celu wyeksportowania wyboru zdarzeń do pliku tekstowego:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Kliknij przycisk **Import/Eksport**.
4. Z listy rozwijalnej wybierz **Eksportuj zdarzenia do pliku**.

   Zostanie uruchomiony Kreator eksportu zdarzeń. Postępuj zgodnie z instrukcjami kreatora.

Usuwanie zdarzeń z wyboru

W celu usunięcia zdarzeń z wyboru:

1. Z drzewa konsoli wybierz węzeł z nazwą odpowiedniego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Zaznacz zdarzenia, które chcesz usunąć, używając myszy bądź klawisza **Shift** lub **Ctrl**.
4. Usuń zaznaczone zdarzenia w jeden z następujących sposobów:
   - Wybierając **Usuń** z menu kontekstowego dowolnego z wybranych zdarzeń.

     Jeżeli z menu kontekstowego wybrałeś element **Usuń wszystkie**, wszystkie wyświetlone zdarzenia zostaną usunięte z wyboru, bez względu na to, które zaznaczyłeś.
   - Klikając odnośnik **Usuń zdarzenie** (jeśli wybrałeś jedno zdarzenie) lub **Usuń zdarzenia** (jeśli wybrałeś kilka zdarzeń) w oknie z informacjami dla tych zdarzeń.

Wybrane zdarzenia zostaną usunięte.

Dodawanie aplikacji do wykluczeń na żądanie użytkownika

Jeśli otrzymasz żądania użytkownika dotyczące odblokowania błędnie zablokowanych aplikacji, możesz utworzyć wykluczenie z reguł ochrony adaptacyjnej dla tych aplikacji. W konsekwencji aplikacje nie będą już blokowane na urządzeniach użytkowników. Możesz śledzić liczbę żądań użytkownika na zakładce **Monitorowanie** Serwera administracyjnego.

W celu dodania aplikacji zablokowanych przez Kaspersky Endpoint Security do wykluczeń według żądań użytkownika:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Z listy rozwijalnej **Wybory zdarzeń** wybierz **Żądania użytkownika**.
4. Kliknij prawym klawiszem myszy żądanie użytkownika (lub kilka żądań użytkownika) zawierające aplikacje, które chcesz dodać do wykluczeń, a następnie wybierz **Dodaj wykluczenie**.

   Zostanie uruchomiony kreator Dodawania wykluczenia. Postępuj zgodnie z jego instrukcjami.

Wybrane aplikacje zostaną wykluczone z listy **Wyzwalacze reguł w Trybie inteligentnego uczenia** (pod węzłem **Repozytoria** w drzewie konsoli) po kolejnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym i nie pojawi się już więcej na liście.

Wybory urządzeń

Informacje o stanie urządzeń są wyświetlane w folderze **Wybory urządzeń** drzewa konsoli.

Informacje w folderze **Wybory urządzeń** są wyświetlane jako lista wyborów urządzeń. Każdy wybór zawiera urządzenia, które spełniają określone warunki. Na przykład, wybór **Urządzenia ze stanem Krytyczny** zawiera tylko urządzenia posiadające stan *Krytyczny*. Po zainstalowaniu aplikacji, folder **Wybory urządzeń** posiada kilka standardowych wyborów. Możesz tworzyć dodatkowe (niestandardowe) wybory urządzeń, eksportować ustawienia wyboru do pliku lub tworzyć wybory zgodnie z ustawieniami zaimportowanymi z innego pliku.

Wyświetlanie wyboru urządzeń

W celu wyświetlenia wyboru urządzeń:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.
2. W obszarze roboczym folderu, z listy **Wybrane urządzenia** wybierz odpowiedni wybór urządzeń.
3. Kliknij przycisk **Uruchom wybrane**.
4. Kliknij zakładkę **Wyniki wyborów**.

W obszarze roboczym zostanie wyświetlona lista urządzeń, które spełniają kryteria wyboru.

Informacje przedstawione na liście urządzeń mogą być sortowane (rosnąco lub malejąco) według dowolnej kolumny.

Konfigurowanie kryteriów wyboru urządzeń

W celu skonfigurowania kryteriów wyboru urządzeń:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.
2. W obszarze roboczy kliknij zakładkę **Wybór**, a następnie kliknij odpowiedni wybór urządzeń na liście wyborów użytkownika.
3. Kliknij przycisk **Właściwości wyboru**.
4. W otwartym oknie właściwości określ następujące ustawienia:
   - Ogólne właściwości wyboru.
   - Warunki, jakie muszą zostać spełnione do uwzględnienia urządzeń w tym wyborze. Możesz skonfigurować warunki po wybraniu nazwy warunku i kliknięciu przycisku **Właściwości**.
   - Ustawienia zabezpieczeń.
5. Kliknij **OK**.

   Ustawienia zostaną zastosowane i zapisane.

Poniżej znajdują się opisy warunków przydzielania urządzeń do wyboru. Warunki są łączone przy użyciu operatora logicznego LUB: Wybór będzie zawierał urządzenia odpowiadające przynajmniej jednemu z wymienionych warunków.

Ogólne

W sekcji **Ogólne** możesz zmienić nazwę warunku wyboru oraz określić, czy ten warunek ma być odwrócony:

Odwróć warunek wyboru

Domyślnie opcja ta jest wyłączona.

Jeśli ta opcja jest włączona, określony warunek wyboru zostanie odwrócony. Wybór będzie zawierał wszystkie urządzenia, które nie spełniają warunku.

Poniższy przykład pokazuje logikę działania inwersji:

- **Warunek**: Na Twoim urządzeniu znajduje się system operacyjny z typem Linux i numerem kompilacji 00.0.000.
- **Warunek odwrócony**: Na urządzeniu znajduje się system operacyjny NIE z (typ Linux i numer kompilacji 00.0.000), co jest równoważne z następującym:

  Istnieje system operacyjny z typem NIE Linux LUB numerem kompilacji NIE 00.0.000.

W związku z tym wybór obejmie urządzenia z systemem operacyjnym, na przykład typu Windows i numerem kompilacji 00.0.000 lub typu Linux i dowolnym numerem kompilacji innym niż 00.0.000.

Sieć

W sekcji **Sieć** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich danymi sieciowymi:

- **Nazwa urządzenia lub adres IP**

  Nazwa sieciowa systemu Windows (nazwa NetBIOS) urządzenia lub adres IPv4 lub IPv6.

- **Domena Windows**

  Wyświetla wszystkie urządzenia znajdujące się w określonej domenie Windows.

- **Grupa administracyjna**

  Wyświetla urządzenia znajdujące się w określonej grupie administracyjnej.

- **Opis**

  Tekst wyświetlany w oknie właściwości urządzenia: pole **Opis** sekcji **Ogólne**.

  W celu opisania tekstu w polu **Opis** możesz użyć następujących znaków:

  - W słowie:

    - *****. Zastępuje dowolny wiersz dowolną liczbą znaków.

    Na przykład:

    Aby opisać słowa **Serwer** lub **Serwera**, możesz wpisać **Serwer***.

    - **?.** Zastępuje dowolny pojedynczy znak.

    Na przykład:

    Aby opisać słowa **Okno** lub **Okna**, możesz wpisać **Okn?**.

    Gwiazdka (*****) lub znak zapytania (**?**) nie mogą być używane jako pierwsze symbole wyszukiwanego słowa.

- W celu wyszukania kilku słów użyj:

  - Spacji. Wyświetla wszystkie urządzenia, których opisy zawierają dowolne z wymienionych słów.

  Na przykład:

  Aby odszukać frazę zawierającą słowa **Podrzędny** lub **Wirtualny**, wprowadź **Podrzędny Wirtualny** w tekście wyszukiwania.

  - **+**. Jeśli przed wyrazem wpisano znak „+”, wszystkie wyniki wyszukiwania będą zawierać ten wyraz.

  Na przykład:

  Aby odszukać frazę zawierającą zarówno **Podrzędny**, jak i **Wirtualny**, wprowadź **+Podrzędny+Wirtualny**.

  - **-**. Jeśli przed wyrazem wpisano znak „-”, żaden z wyników wyszukiwania nie będzie zawierać tego wyrazu.

  Na przykład:

  Aby odszukać frazę zawierającą **Podrzędny** i nie zawierającą **Wirtualny**, wprowadź **+Podrzędny-Wirtualny**.

  - **„<jakikolwiek tekst>”**. Tekst w cudzysłowach musi znajdować się w tekście.

  Na przykład:

  Aby odszukać frazę zawierającą kombinację słów **Podrzędny Serwer**, wprowadź **Podrzędny Serwer** w tekście wyszukiwania.

- **Zakres IP**

  Jeśli ta opcja jest włączona, możesz wprowadzić początkowy i końcowy adres IP z zakresu adresów IP, do którego muszą zostać włączone odpowiednie urządzenia.

  Domyślnie opcja ta jest wyłączona.

Znaczniki

W sekcji **Znaczniki** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o słowa kluczowe (znaczniki), które wcześniej zostały dodane do opisów zarządzanych urządzeń:

- **Zastosuj, jeśli co najmniej jeden określony znacznik jest zgodny**

  Jeśli ta opcja jest włączona, w wynikach wyszukiwania będą wyświetlane urządzenia z opisami, które zawierają przynajmniej jeden z wybranych znaczników.

  Jeśli ta opcja jest wyłączona, w wynikach wyszukiwania będą wyświetlane tylko urządzeni z opisami, które zawierają wszystkie wybrane znaczniki.

  Domyślnie opcja ta jest wyłączona.

- **Musi zawierać znacznik**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy zawierają wybrany znacznik. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

  Domyślnie opcja ta jest zaznaczona.

- **Nie może zawierać znacznika**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy nie zawierają wybranego znacznika. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

Active Directory

W sekcji **Active Directory** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o ich dane Active Directory:

- **Urządzenie znajduje się w jednostce organizacyjnej Active Directory**

  Jeśli ta opcja jest włączona, wybór będzie zawierał urządzenia z jednostki Active Directory określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

- **Uwzględnij podrzędne jednostki organizacyjne**

  Jeśli ta opcja jest włączona, wybór zawiera urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej domeny.

  Domyślnie opcja ta jest wyłączona.

- **Urządzenie należy do grupy Active Directory**

  Jeśli ta opcja jest włączona, wybór będzie zawierał komputery z grupy Active Directory określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

Aktywność sieciowa

W sekcji **Aktywność sieciowa** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich aktywnością sieciową:

- **Urządzenie jest punktem dystrybucji**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Wybór zawiera urządzenia pełniące role punktów dystrybucji.
  - **Nie**. Urządzenia pełniące role punktów dystrybucji nie będą uwzględniane w wyborze.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Nie odłączaj od Serwera administracyjnego**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Włączona**. Wybór będzie zawierał urządzenia, na których zaznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Wyłączona**. Wybór będzie zawierał urządzenia, na których odznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Przełączanie profilu połączenia**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Wybór będzie zawierał urządzenia, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie**. Wybór nie będzie zawierał urządzeń, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Ostatnie połączenie z Serwerem administracyjnym**

  To pole ustawia kryterium wyszukiwania urządzeń według godziny ostatniego połączenia z Serwerem administracyjnym.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego zostało nawiązane ostatnie połączenie pomiędzy Agentem sieciowym zainstalowanym na urządzeniu klienckim a Serwerem administracyjnym. Wybór będzie zawierał urządzenia mieszczące się w określonym przedziale czasu.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- **Nowe urządzenia odnalezione podczas skanowania sieci**

  Wyszukiwanie nowych urządzeń, które zostały wykryte podczas przeszukiwania sieci w przeciągu kilku ostatnich dni.

  Jeśli ta opcja jest włączona, wybór będzie zawierał nowe urządzenia wykryte podczas wykrywania urządzeń w czasie określonym w polu **Okres wykrywania (dni)**.

  Jeśli ta opcja jest wyłączona, wybór będzie zawierał wszystkie urządzenia wykryte podczas wykrywania urządzeń.

  Domyślnie opcja ta jest wyłączona.

- **Dostępność urządzenia**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie widoczne w sieci.
  - **Nie**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie niewidoczne w sieci.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

Aplikacja

W sekcji **Aplikacja** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o wybraną zarządzaną aplikację:

- **Nazwa aplikacji**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji Kaspersky.

  Lista zawiera tylko nazwy aplikacji z wtyczkami administracyjnymi zainstalowanych na stacji roboczej administratora.

  Jeśli żadna aplikacja nie została wybrana, kryterium nie będzie stosowane.

- **Wersja aplikacji**

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według numeru wersji aplikacji Kaspersky.

  Jeśli żaden numer wersji nie został określony, kryterium nie będzie stosowane.

- **Nazwa aktualizacji krytycznej**

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji lub numeru pakietu aktualizacyjnego.

  Jeśli pole będzie puste, kryterium nie będzie stosowane.

- **Ostatnia aktualizacja modułów**

  Ta opcja może zostać użyta do ustawienia kryterium wyszukiwania urządzeń według godziny ostatniej aktualizacji modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego została wykonana ostatnia aktualizacja modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- **Urządzenie jest zarządzane przez Kaspersky Security Center**

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić urządzenia zarządzane poprzez Kaspersky Security Center:

  - **Tak**. Aplikacja uwzględni w wyborze urządzenia zarządzane poprzez Kaspersky Security Center.
  - **Nie**. Aplikacja uwzględni w wyborze urządzenia, jeśli nie są one zarządzane przez Kaspersky Security Center.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Aplikacja zabezpieczająca jest zainstalowana**

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą:

  - **Tak**. Aplikacja uwzględni w wyborze wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą.
  - **Nie**. Aplikacja uwzględni w wyborze wszystkie urządzenia bez zainstalowanej aplikacji zabezpieczającej.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

System operacyjny

W sekcji **System operacyjny** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z typem systemu operacyjnego.

- **Wersja systemu operacyjnego**

  Jeśli pole jest zaznaczone, możesz wybrać system operacyjny z listy. Urządzenia, na których zainstalowany jest określony system operacyjny, są uwzględniane w wynikach wyszukiwania.

- **Typ systemu operacyjnego (bity)**

  Z listy rozwijalnej możesz wybrać architekturę swojego systemu operacyjnego, która określi sposób stosowania reguły przenoszenia do urządzenia (**Nieznany**, **x86**, **AMD64**, or **IA64**). Domyślnie, na liście nie wybrano żadnej opcji i tym samym nie zdefiniowano architektury systemu operacyjnego.

- **Wersja dodatku Service Pack systemu operacyjnego**

  W tym polu możesz określić wersję pakietu systemu operacyjnego (w formacie *X.Y*), która będzie określać sposób stosowania reguły przenoszenia do urządzenia. Domyślnie nie jest zdefiniowana żadna wartość.

- **Kompilacja systemu operacyjnego**

  > To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Numer kompilacji systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować wyszukiwanie wszystkich numerów kompilacji, za wyjątkiem określonego.

- **ID wersji systemu operacyjnego**

  > To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Identyfikator wydania systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy identyfikator wydania. Możesz także skonfigurować wyszukiwanie wszystkich numerów identyfikatorów wydania, za wyjątkiem określonego.

Stan urządzenia

W sekcji **Stan urządzenia** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o opis stanu urządzeń z zarządzanej aplikacji:

- **Stan urządzenia**

  Lista rozwijalna, z której możesz wybrać jeden ze stanów urządzenia: *OK*, *Krytyczny*, or *Ostrzeżenie*.

- **Opis stanu urządzenia**

  W tym polu możesz zaznaczyć pola obok warunków, które, jeśli są spełnione, spowodują przypisanie do urządzenia jednego z następujących stanów: *OK, Krytyczny* lub *Ostrzeżenie*.

- **Stan urządzenia zdefiniowany przez aplikację**

  Lista rozwijalna, z której możesz wybrać stan ochrony w czasie rzeczywistym. Urządzenia z określonymi stanami ochrony w czasie rzeczywistym są uwzględniane w wyborze.

Składniki ochrony

W sekcji **Składniki ochrony** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o ich stan ochrony:

- **Data opublikowania baz danych**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według daty opublikowania antywirusowej bazy danych. W polach do wprowadzania danych możesz określić przedział czasu, na podstawie którego wykonywane jest wyszukiwanie.

  Domyślnie opcja ta jest wyłączona.

- **Ostatnie skanowanie**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według czasu ostatniego skanowania w poszukiwaniu złośliwego oprogramowania. W polach wejściowych możesz określić przedział czasu, w trakcie którego zostało wykonane ostatnie skanowanie w poszukiwaniu złośliwego oprogramowania.

  Domyślnie opcja ta jest wyłączona.

- **Całkowita liczba wykrytych zagrożeń**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według liczby wykrytych wirusów. W polach wejściowych możesz określić niższe i wyższe wartości progowe liczby wykrytych wirusów.

  Domyślnie opcja ta jest wyłączona.

Rejestr aplikacji

W sekcji **Rejestr aplikacji** możesz skonfigurować kryteria wyszukiwania urządzeń na podstawie aplikacji na nich zainstalowanych:

- **Nazwa aplikacji**

  Lista rozwijalna, z której możesz wybrać aplikację. Urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Wersja aplikacji**

  Pole, w którym możesz określić wersję wybranej aplikacji.

- **Producent**

  Lista rozwijalna, z której możesz wybrać producenta aplikacji zainstalowanej na urządzeniu.

- **Stan aplikacji**

  Lista rozwijalna, z której możesz wybrać stan aplikacji (*Zainstalowana*, *Nie zainstalowana*). Urządzenia, na których określona aplikacja została zainstalowana lub nie została zainstalowana, w zależności od wybranego stanu, zostaną uwzględnione w wyborze.

- **Wyszukaj według aktualizacji**

  Jeśli ta opcja jest włączona, wyszukiwanie będzie się odbywać z użyciem szczegółów aktualizacji dla aplikacji zainstalowanych na odpowiednich urządzeniach. Po zaznaczeniu pola, pola **Nazwa aplikacji**, **Wersja aplikacji** i **Stan aplikacji** zostaną zmienione na **Nazwa aktualizacji**, **Wersja aktualizacji** i **Stan**.

  Domyślnie opcja ta jest wyłączona.

- **Nazwa niekompatybilnej aplikacji zabezpieczającej**

  Lista rozwijalna, z której możesz wybrać aplikacje zabezpieczające firm trzecich. Podczas wyszukiwania, urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Znacznik aplikacji**

  Z listy rozwijalnej możesz wybrać znacznik aplikacji. Wszystkie urządzenia, na których są zainstalowane aplikacje z wybranym znacznikiem w opisie, zostają uwzględnione w wyborze urządzeń.

- **Zastosuj do urządzeń bez określonych znaczników**

  Jeśli ta opcja jest włączona, wybór obejmuje urządzenia z opisami, które nie zawierają żadnego z wybranych znaczników.

  Jeśli ta opcja jest wyłączona, kryterium nie zostanie zastosowane.

  Domyślnie opcja ta jest wyłączona.

Rejestr sprzętu

W sekcji **Rejestr sprzętu** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o sprzęt na nich zainstalowany:

- **Urządzenie**

  Z listy rozwijalnej możesz wybrać typ jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- **Producent**

  Z listy rozwijalnej możesz wybrać nazwę producenta jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- **Nazwa urządzenia**

  Nazwa urządzenia w sieci Windows. Urządzenie z określoną nazwą zostanie uwzględniony w wyborze.

- **Opis**

  Opis urządzenia lub sprzętu. Urządzenia z opisem określonym w tym polu zostaną uwzględnione w wyborze.

  Opis urządzenia w dowolnym formacie może zostać wprowadzony w oknie właściwości tego urządzenia. Pole obsługuje wyszukiwanie pełnotekstowe.

- **Producent urządzenia**

  Nazwa producenta urządzenia. Urządzenia, które zostały wyprodukowane przez producenta określonego w tym polu, zostaną uwzględnione w wyborze.

  Nazwę producenta można wprowadzić w oknie właściwości urządzenia.

- **Numer seryjny**

  Cały sprzęt o numerze seryjnym określonym w tym polu zostanie uwzględniony w wyborze.

- **Numer ewidencyjny**

  Sprzęt o numerze inwentarzowym podanym w tym polu zostanie uwzględniony w wyborze.

- **Użytkownik**

  Cały sprzęt użytkownika określonego w tym polu zostanie uwzględniony w wyborze.

- **Lokalizacja**

  Lokalizacja urządzenia lub sprzętu (na przykład: w kwaterze głównej lub w oddziale firmy). Komputery lub inne urządzenia zainstalowane w lokalizacji określonej w tym polu zostaną uwzględnione w wyborze.

  Możesz opisać lokalizację urządzenia w dowolnym formacie w oknie właściwości tego urządzenia.

- **Częstotliwość procesora, w MHz**

  Zakres częstotliwości procesora. Urządzenia z procesorami odpowiadającymi zakresowi częstotliwości określonemu w tych polach (wszystkich) zostaną uwzględnione w wyborze.

- **Wirtualne rdzenie procesora**

  Zakres liczby wirtualnych rdzeni w procesorze. Urządzenia z pamięcią RAM odpowiadającą zakresowi określonemu w tych polach (wszystkich) zostaną uwzględnione w wyborze.

- **Pojemność dysku twardego, w GB**

  Zakres wartości rozmiaru dysku twardego urządzenia. Urządzenia z dyskami twardymi odpowiadającymi zakresowi określonemu w tych polach wejściowych (wszystkich) zostaną uwzględnione w wyborze.

- **Rozmiar pamięci RAM, w MB**

  Zakres wartości rozmiaru pamięci RAM urządzenia. Urządzenia z pamięcią RAM odpowiadającą zakresowi określonemu w tych polach wejściowych (wszystkich) zostaną uwzględnione w wyborze.

Maszyny wirtualne

W sekcji **Maszyny wirtualne** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w zależności od tego, czy są to maszyny wirtualne lub czy są one częścią Virtual Desktop Infrastructure (VDI):

- **Jest maszyną wirtualną**

  Z listy rozwijalnej możesz wybrać następujące opcje:

  - **Nieważne**.
  - **Nie**. Wyszukuje urządzenia, które nie są maszynami wirtualnymi.
  - **Tak**. Wyszukuje urządzenia, które są maszynami wirtualnymi.

- **Typ maszyny wirtualnej**

  Z listy rozwijalnej możesz wybrać producenta maszyny wirtualnej.

  Ta lista rozwijalna jest dostępna, jeśli wartość **Tak** lub **Nieważne** została wybrana na liście rozwijalnej **Jest maszyną wirtualną**.

- **Część Virtual Desktop Infrastructure**

  Z listy rozwijalnej możesz wybrać następujące opcje:

  - **Nieważne**.
  - **Nie**. Wyszukuje urządzenia, które nie są częścią Virtual Desktop Infrastructure.
  - **Tak**. Wyszukuje urządzenia, które są częścią Virtual Desktop Infrastructure (VDI).

Luki oraz aktualizacje

W sekcji **Luki oraz aktualizacje** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich źródłem Windows Update:

WUA został przełączony na Serwer administracyjny

Z listy rozwijalnej można wybrać jedną z następujących opcji wyszukiwania:

- **Tak**. Jeśli wybrano tę opcję, wyniki wyszukiwania będą uwzględniać urządzenia, które uzyskały aktualizacje poprzez Windows Update z Serwera administracyjnego.
- **Nie**. Jeśli wybrano tę opcję, wyniki będą uwzględniać urządzenia, które uzyskały aktualizacje za pośrednictwem Windows Update z innych źródeł.

Użytkownicy

W sekcji **Użytkownicy** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze według kont użytkowników, którzy logowali się do systemu operacyjnego.

- **Ostatni użytkownik zalogowany do systemu**

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik ostatnio logował się do systemu.

- **Użytkownik zalogowany do systemu co najmniej raz**

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik przynajmniej raz logował się do systemu.

Problemy mające wpływ na stan zarządzanych aplikacji

W sekcji **Problemy mające wpływ na stan zarządzanych aplikacji** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze według listy możliwych problemów wykrytych przez zarządzaną aplikację. Jeśli przynajmniej jeden problem, który wybrałeś, istnieje na urządzeniu, urządzenie zostanie uwzględnione w wyborze. Jeśli wybierzesz problem wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego problemu na wszystkich listach.

Opis stanu urządzenia

Możesz zaznaczyć opcje dla opisów stanów z zarządzanej aplikacji. Po odebraniu tych stanów, urządzenia zostaną uwzględnione w wyborze. Jeśli wybierzesz stan wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego stanu na wszystkich listach.

Stan komponentów w zarządzanych aplikacjach

W sekcji **Stan komponentów w zarządzanych aplikacjach** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o stany komponentów w zarządzanych aplikacjach:

- **Stan ochrony przed wyciekiem danych**

  Wyszukiwanie urządzeń według stanu Ochrona przed wyciekaniem danych (*Nieznana, Zatrzymano, Uruchamianie, Wstrzymana, Uruchamianie, Niepowodzenie*).

- **Stan ochrony serwerów współpracy**

  Wyszukiwanie urządzeń według stanu ochrony serwerów współpracy (*Nieznana*, *Zatrzymano*, *Uruchamianie, Wstrzymana*, *Uruchamianie*, *Niepowodzenie*).

- **Stan ochrony antywirusowej serwerów pocztowych**

  Wyszukiwanie urządzeń według stanu ochrony dla serwerów pocztowych (*Nieznana, Zatrzymano, Uruchamianie, Wstrzymana, Uruchamianie, Niepowodzenie*).

- **Stan czujnika Endpoint Sensor**

  Wyszukiwanie urządzeń według stanu komponentu Endpoint Sensor (*Nieznana, Zatrzymano, Uruchamianie, Wstrzymana, Uruchamianie, Niepowodzenie*).

Szyfrowanie

Algorytm szyfrowania

Algorytm blokowego szyfru symetrycznego AES (Advanced Encryption Standard). Z listy rozwijalnej możesz wybrać długość klucza szyfrowania (56-bitowy, 128-bitowy, 192-bitowy lub 256-bitowy).

Dostępne wartości: *AES56*, *AES128*, *AES192* i *AES256*.

Segmenty chmury

W sekcji **Segmenty chmury** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o ich odpowiednie segmenty chmury:

- **Urządzenie znajduje się w segmencie chmury**

  Jeśli ta opcja jest włączona, możesz kliknąć przycisk **Przeglądaj**, aby określić przeszukiwany segment.

  Jeśli włączono także opcję **Włączając obiekty potomne**, wyszukiwanie jest uruchamiane na wszystkich obiektach potomnych określonego segmentu.

  Wyniki wyszukiwania zawierają tylko urządzenia z wybranego segmentu.

- **Urządzenie wykryte przy pomocy API**

  Z listy rozwijalnej możesz wybrać, czy urządzenie jest wykrywane przez narzędzia API:

  - **AWS**. Urządzenie jest wykrywane przy pomocy AWS API, co oznacza, że urządzenie znajduje się w środowisku chmury AWS.

  - **Azure**. Urządzenie jest wykrywane przy pomocy Azure API, co oznacza, że urządzenie znajduje się w środowisku chmury Azure.

- **Google Cloud.** Urządzenie jest wykrywane przy pomocy Google API, co oznacza, że urządzenie znajduje się w środowisku Google Cloud.

- **Nie**. Urządzenie nie może zostać wykryte przy użyciu AWS, Azure lub Google API, co oznacza, że znajduje się poza środowiskiem chmury lub znajduje się w środowisku chmury, ale nie może zostać wykryte przy użyciu API.

- **Brak wartości**. Warunek nie ma zastosowania.

Składniki aplikacji

Ta sekcja zawiera listę komponentów tych aplikacji, które posiadają odpowiednie wtyczki administracyjne, zainstalowane w Konsoli administracyjnej.

W sekcji **Składniki aplikacji** możesz określić kryteria uwzględniania urządzeń w wyborze zgodnie ze stanami i numerami wersji komponentów, które odpowiadają wybranej aplikacji:

- **Stan**

  Wyszukiwanie urządzeń zgodnie ze stanem komponentu wysłanym przez aplikację do Serwera administracyjnego. Możesz wybrać jeden z następujących stanów: *Brak danych z urządzenia*, *Zatrzymane*, *Uruchamianie*, *Wstrzymane*, *Uruchomione*, *Błąd* lub *Nie zainstalowano*. Jeśli wybrany komponent aplikacji zainstalowanej na zarządzanym urządzeniu posiada określony stan, urządzenie jest uwzględniane w wyborze urządzeń.

  Stany wysłane przez aplikacje:

  - *Uruchamianie*—komponent jest właśnie w procesie inicjalizacji.

  - *Uruchomione*—komponent jest włączony i działa poprawnie.

  - *Wstrzymane*—komponent został zawieszony, na przykład, po wstrzymaniu przez użytkownika ochrony w zarządzanej aplikacji.

  - *Błąd*—podczas działania komponentu wystąpił błąd.

  - *Zatrzymane*—komponent jest wyłączony i nie działa w tym momencie.

  - *Nie zainstalowano*—użytkownik nie wybrał komponentu do zainstalowania podczas konfigurowania niestandardowej instalacji aplikacji.

  W przeciwieństwie do pozostałych stanów, stan *Brak danych z urządzenia* nie jest wysyłany przez aplikacje. Ta opcja pokazuje, że aplikacje nie posiadają informacji o wybranym stanie komponentu. Na przykład, to może mieć miejsce, gdy wybrany komponent nie należy do żadnej z aplikacji zainstalowanych na urządzeniu lub gdy urządzenie jest wyłączone.

- **Wersja**

  Wyszukiwanie urządzeń zgodnie z numerem wersji komponentu, który wybierasz na liście. Możesz wpisać numer wersji, na przykład `3.4.1.0`, a następnie określić, czy wybrany komponent musi posiadać równą, wcześniejszą lub nowszą wersję. Możesz także skonfigurować wyszukiwanie wszystkich wersji, za wyjątkiem określonej.

Eksportowanie ustawień wyboru urządzeń do pliku

W celu wyeksportowania ustawień wyboru urządzenia do pliku tekstowego:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.
2. W obszarze roboczym, na zakładce **Wybór** kliknij odpowiedni wybór urządzeń na liście wyborów użytkownika.

   Ustawienia mogą być eksportowane tylko z wyborów urządzeń utworzonych przez użytkownika.

3. Kliknij przycisk **Uruchom wybrane**.
4. Na zakładce **Wyniki wyborów** kliknij przycisk **Eksportuj ustawienia**.
5. W oknie **Zapisz jako**, które zostało otwarte, określ nazwę wyboru pliku eksportowania ustawień, wybierz folder, w którym zostanie zapisany, i kliknij przycisk **Zapisz**.

Ustawienia wyboru urządzenia zostaną zapisane do określonego pliku.

Tworzenie kryteriów wyboru urządzeń

W celu utworzenia kryterium wyboru urządzeń:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.
2. W obszarze roboczym folderu kliknij przycisk **Zaawansowane** i wybierz z listy rozwijalnej **Utwórz wybór**.
3. W oknie **Nowy wybór urządzeń**, które zostanie otwarte, wprowadź nazwę nowego wyboru i kliknij **OK**.

Nowy folder z podaną nazwą pojawi się w drzewie konsoli, w folderze **Wybory urządzeń**. Domyślnie nowy wybór urządzeń zawiera wszystkie urządzenia wchodzące w skład grup administracyjnych na Serwerze administracyjnym, na którym utworzono wybór. Aby wybór wyświetlał tylko żądane urządzenia, skonfiguruj wybór poprzez kliknięcie przycisku **Właściwości wyboru**.

Tworzenie wyboru urządzeń zgodnie z zaimportowanymi ustawieniami

W celu utworzenia wyboru urządzeń zgodnie z zaimportowanymi ustawieniami:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.
2. W obszarze roboczym folderu kliknij przycisk **Zaawansowane** i z listy rozwijalnej wybierz **Importuj wybór z pliku**.
3. W oknie, które zostanie otwarte, określ ścieżkę dostępu do pliku, z którego chcesz zaimportować ustawienia wyboru. Kliknij przycisk **Otwórz**.

   Wpis **Nowy wybór** jest tworzony w folderze **Wybory urządzeń**. Ustawienia nowego wyboru są importowane z określonego pliku.

Jeżeli w folderze **Wybory urządzeń** istnieje już wybór o nazwie **Nowy wybór**, do nazwy tworzonego wyboru zostanie dodany przyrostek numeryczny **(<kolejny numer seryjny>)**, na przykład: **(1)**, **(2)**.

Usuwanie urządzeń z grup administracyjnych w wyborze

Podczas pracy z wyborami urządzeń możesz usunąć urządzenia z grup administracyjnych bezpośrednio w tym wyborze, bez przełączania do grup administracyjnych, z których te urządzenia mają być usunięte.

W celu usunięcia urządzeń z grup administracyjnych:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.
2. Zaznacz urządzenia, które chcesz usunąć, używając klawisza **Shift** lub **Ctrl**.
3. Usuń zaznaczone urządzenia z grup administracyjnych w jeden z następujących sposobów:
   - Z menu kontekstowego jednego z zaznaczonych urządzeń wybierz **Usuń**
   - Kliknij przycisk **Wykonaj akcję** i z listy rozwijalnej wybierz wartość **Usuń z grupy**

   Wybrane urządzenia zostaną usunięte z odpowiednich grup administracyjnych.

Monitorowanie instalacji i dezinstalacji aplikacji

Możesz monitorować instalację lub dezinstalację określonych aplikacji na zarządzanych urządzeniach (na przykład, określonej przeglądarki). Aby użyć tej funkcji, możesz dodać aplikacje z Rejestru aplikacji do listy monitorowanych aplikacji. Jeśli monitorowana aplikacja jest instalowana lub dezinstalowana, Agent sieciowy publikuje odpowiednie zdarzenia: **Monitorowana aplikacja została zainstalowana** lub **Monitorowana aplikacja została odinstalowana**. Możesz monitorować te zdarzenia, korzystając z, na przykład, wyborów zdarzeń lub raportów.

Możesz monitorować te zdarzenia tylko wtedy, gdy są przechowywane w bazie danych Serwera administracyjnego.

W celu dodania aplikacji do listy monitorowanych aplikacji:

1. W folderze **Zaawansowane → Zarządzanie aplikacjami** w drzewie konsoli wybierz podfolder **Rejestr aplikacji**.
2. Nad listą aplikacji, która jest wyświetlana, kliknij przycisk **Pokaż okno właściwości rejestru aplikacji**.
3. W wyświetlonym oknie **Monitorowane aplikacje** kliknij przycisk **Dodaj**.
4. W wyświetlonym oknie **Wybierz nazwę aplikacji** wybierz aplikacje z Rejestru aplikacji, której instalację lub dezinstalację chcesz monitorować.
5. W oknie **Wybierz nazwę aplikacji** kliknij przycisk **OK**.

Po skonfigurowaniu listy monitorowanych aplikacji i zainstalowaniu lub odinstalowaniu zarządzanych urządzeń w swojej organizacji, możesz monitorować odpowiednie zdarzenia, na przykład, korzystać z wyboru zdarzeń Ostatnie zdarzenia.

Zdarzenia składników Kaspersky Security Center

Każdy komponent Kaspersky Security Center posiada swój zestaw typów zdarzeń. W tej sekcji wymienione są typy zdarzeń, które występują w Serwerze administracyjnym Kaspersky Security Center, Agencie sieciowym i serwerze iOS MDM. Typy zdarzeń, które występują w aplikacjach Kaspersky, nie zostały wymienione w tej sekcji.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Struktura danych opisu typu zdarzeń

Dla każdego typu zdarzenia dostarczone są następujące elementy: wyświetlana nazwa, identyfikator (ID), kod alfabetyczny, opis oraz domyślny czas przechowywania.

- **Nazwa wyświetlanego typu zdarzenia**. Ten tekst jest wyświetlany w Kaspersky Security Center, gdy konfigurujesz zdarzenia oraz podczas występowania zdarzeń.
- **ID typu zdarzenia**. Ten kod numeryczny jest używany, gdy przetwarzasz zdarzenia przy użyciu narzędzi firm trzecich do analizy zdarzeń.
- **Typ zdarzenia** (kod alfabetyczny). Ten kod jest używany, gdy przeglądasz i przetwarzasz zdarzenia, korzystając z widoków publicznych, dostępnych w bazie danych Kaspersky Security Center, a także podczas eksportowania zdarzeń do systemu SIEM.
- **Opis**. Ten tekst zawiera sytuacje, gdy zdarzenie wystąpi i co należy zrobić w takiej sytuacji.
- **Domyślny czas przechowywania**. To jest liczba dni, przez jaką zdarzenie jest przechowywane w bazie danych Serwera administracyjnego i jest wyświetlane na liście zdarzeń na Serwerze administracyjnym. Po upłynięciu tego czasu, zdarzenie jest usuwane. Jeśli wartość czasu przechowywania zdarzenia to 0, takie zdarzenia są wykrywane, ale nie są wyświetlane na liście zdarzeń na Serwerze administracyjnym. Jeśli skonfigurowałeś zapisywanie takich zdarzeń w dzienniku zdarzeń systemu operacyjnego, znajdziesz je tam.

Możesz zmienić czas przechowywania zdarzeń:

- Konsola administracyjna: Ustawianie czasu przechowywania dla zdarzenia
- Kaspersky Security Center Web Console: Ustawianie czasu przechowywania dla zdarzenia

Inne dane mogą zawierać następujące pola:

- **event_id**: unikatowa liczba zdarzeń w bazie danych, wygenerowana i przypisana automatycznie; nie mylić z **ID typu zdarzenia**.
- **task_id**: identyfikator zadania, które spowodowało wystąpienie zdarzenia (jeśli są jakiekolwiek)
- **severity**: jeden z następujących priorytetów (w kolejności rosnącej):

  0) Niepoprawny priorytet

  1) Informacja

  2) Ostrzeżenie

  3) Błąd

  4) Krytyczny

Zdarzenia Serwera administracyjnego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Serwera administracyjnego.

Zdarzenia krytyczne Serwera administracyjnego

Poniższa tabela wyświetla zdarzenia Serwera administracyjnego Kaspersky Security Center, które posiadają priorytet **Krytyczny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Jeśli określono port w oknie właściwości Serwera administracyjnego w Konsoli administracyjnej, **Kaspersky Security Center opublikuje metryki** i zdarzenia krytyczne, które mają zostać pozyskane przez Prometheus, system monitorowania i ostrzegania. Prometheus pozyskuje metryki i zdarzenia krytyczne, a następnie generuje ostrzeżenia dla każdego zdarzenia.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Zdarzenia krytyczne Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Limit licencji został przekroczony	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Raz dziennie Kaspersky Security Center sprawdza, czy limity licencji nie zostały przekroczone. Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre ograniczenia licencyjne są przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją przekracza 110% całkowitej liczby jednostek objętych licencją. Nawet jeśli to zdarzenie wystąpi, urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu. • Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center określa reguły generowania zdarzeń, gdy limit licencji zostanie przekroczony.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Epidemia wirusa	26 (dla Ochrony plików)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	180 dni
Epidemia wirusa	27 (dla Ochrony poczty)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	180 dni
Epidemia wirusa	28 (dla Zapory sieciowej)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	180 dni
Zarządzanie urządzeniem nie jest możliwe	4111	KLSRV_HOST_OUT_CONTROL	Zdarzenia tego typu występują, jeśli zarządzane urządzenie jest widoczne w sieci, ale nie ma podłączonego Serwera administracyjnego przez pewien czas. Dowiedz się, co uniemożliwia poprawne działanie Agenta sieciowego na urządzeniu. Możliwe przyczyny obejmują problemy z siecią i usuwanie Agenta sieciowego z urządzenia.	180 dni
Stan urządzenia: Krytyczny	4113	KLSRV_HOST_STATUS_CRITICAL	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan *Krytyczny*. Możesz skonfigurować warunki, zgodnie z którymi stan urządzenia zostanie zmieniony na *Krytyczny*.	180 dni
Plik klucza został dodany do listy zablokowanych	4124	KLSRV_LICENSE_BLACKLISTED	Zdarzenia tego typu występują, gdy firma Kaspersky dodała kod aktywacyjny lub plik klucza, którego używasz, do listy zablokowanych. Aby uzyskać więcej informacji, skontaktuj się z działem pomocy technicznej.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Tryb ograniczonej funkcjonalności	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Zdarzenia tego typu występują, gdy Kaspersky Security Center zaczyna działać z podstawową funkcjonalnością, bez funkcji Zarządzanie lukami i poprawkami oraz bez funkcji Zarządzanie urządzeniami mobilnymi. Poniższe elementy są przyczynami i odpowiednimi odpowiedziami na zdarzenie: • Okres licencji wygasł. Zapewnij licencję do korzystania z trybu pełnej funkcjonalności Kaspersky Security Center (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). • Serwer administracyjny zarządza większą liczbą urządzeń niż określona przez ograniczenie licencji. Przenieś urządzenia z grup administracyjnych Serwera administracyjnego do tych należących do innego Serwera administracyjnego (jeśli ograniczenie licencji innego Serwera administracyjnego zezwala na to).	180 dni
Licencja wkrótce utraci ważność	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Tego typu zdarzenia mają miejsce, gdy zbliża się data wygaśnięcia licencji komercyjnej. Raz dziennie Kaspersky Security Center sprawdza, czy nie zbliża się data wygaśnięcia licencji. Wydarzenia tego typu publikowane są 30 dni, 15 dni, 5 dni i 1 dzień przed datą wygaśnięcia licencji. Nie możesz zmienić liczby dni. Jeśli Serwer administracyjny zostanie wyłączony określonego dnia przed datą wygaśnięcia licencji, zdarzenie nie zostanie opublikowane, aż do następnego dnia. Po wygaśnięciu licencji komercyjnej Kaspersky Security Center zapewnia tylko podstawową funkcjonalność. Możesz zareagować na zdarzenie w następujące sposoby: • Upewnij się, że zapasowy klucz licencyjny został dodany do Serwera administracyjnego. • Jeśli korzystasz z subskrypcji, pamiętaj o jej odnowieniu. Nieograniczona subskrypcja jest odnawiana automatycznie, jeśli została opłacona w odpowiednim terminie.	180 dni
Certyfikat wygasł	4132	KLSRV_CERTIFICATE_EXPIRED	Wydarzenia tego typu występują, gdy certyfikat mobilny klienta na urządzeniu mobilnym wygaśnie.	180 dni
Certyfikat Serwera administracyjnego wygasł.	6129	ServerCertificateExpired	Zdarzenia tego typu występują, gdy certyfikat Serwera administracyjnego dla urządzeń mobilnych i urządzeń UEFI utraci ważność. Należy zaktualizować certyfikat, który utracił ważność.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Aktualizacje dla modułów aplikacji Kaspersky zostały wycofane	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Zdarzenia tego typu występują, jeśli aktualizacje typu seamless zostały wycofane (dla tych aktualizacji wyświetlany jest stan *Wycofano*) przez specjalistów z pomocy technicznej Kaspersky; na przykład, muszą zostać zaktualizowane do nowszej wersji. Zdarzenie dotyczy poprawek Kaspersky Security Center i nie dotyczy modułów zarządzanych aplikacji firmy Kaspersky. Zdarzenie zawiera przyczynę niezainstalowania aktualizacji typu seamless.	180 dni
Audyt: Eksport do SIEM nie powiódł się	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Zdarzenia tego typu mają miejsce, gdy eksport zdarzeń do systemu SIEM nie powiódł się z powodu błędu połączenia z systemem SIEM.	180 dni

Zdarzenia błędu funkcjonalnego Serwera administracyjnego

Poniższa tabela wyświetla zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Błąd funkcjonalny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia błędu funkcjonalnego Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Błąd w czasie wykonywania	4125	KLSRV_RUNTIME_ERROR	Zdarzenia tego typu występują w wyniku nieznanych problemów. Najczęściej są to problemy z systemem DBMS, problemy z siecią oraz inne problemy z oprogramowaniem i sprzętem. Szczegóły zdarzenia można znaleźć w opisie zdarzenia.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Przekroczono limit instalacji dla jednej z grup licencjonowanych aplikacji	4126	KLSRV_INVLICPROD_EXCEDED	Serwer administracyjny generuje zdarzenia tego typu okresowo (co godzinę). Zdarzenia tego typu występują, jeśli w Kaspersky Security Center zarządzasz kluczami licencyjnymi aplikacji innych firm i jeśli liczba instalacji przekroczyła ograniczenie ustawione przez klucz licencyjny aplikacji innej firmy. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń aplikację innej firmy z urządzeń, na których aplikacja nie jest używana. • Użyj licencji innej firmy dla większej liczby urządzeń. Możesz zarządzać kluczami licencyjnymi aplikacji firm trzecich, korzystając z funkcjonalności grup licencjonowanych aplikacji. Grupa licencjonowanych aplikacji zawiera aplikacje firm trzecich spełniające kryteria ustalone przez Ciebie.	180 dni
Przeszukanie segmentu chmury nie powiodło się	4143	KLSRV_KLCLOUD_SCAN_ERROR	Zdarzenia tego typu mają miejsce, gdy serwer administracyjny nie może przeszukać segmentu sieci w środowisku chmury. Przeczytaj szczegóły w opisie zdarzenia i zareaguj odpowiednio.	Nie jest przechowywany
Kopiowanie aktualizacji do określonego folderu nie powiodło się	4123	KLSRV_UPD_REPL_FAIL	Zdarzenia tego typu występują, gdy aktualizacje oprogramowania są kopiowane do dodatkowych folderów współdzielonych. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy konto użytkownika, który ma uzyskać dostęp do folderu(ów) posiada prawo do zapisu. • Sprawdź, czy nazwa użytkownika i/lub hasło do folderu/-ów nie uległy zmianie. • Sprawdź połączenie z internetem, gdyż to może być przyczyną zdarzenia. Aby zaktualizować bazy danych i moduły oprogramowania, postępuj zgodnie z instrukcjami.	180 dni
Brak wolnego miejsca na dysku	4107	KLSRV_DISK_FULL	Tego typu zdarzenia występują, gdy dysk twardy urządzenia, na którym jest zainstalowany Serwer administracyjny, zabraknie wolnego miejsca. Zwolnij miejsce na dysku na urządzeniu.	180 dni
Folder współdzielony nie jest dostępny	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Zdarzenia tego typu występują, jeśli folder współdzielony Serwera administracyjnego jest niedostępny. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy Serwer administracyjny (na którym znajduje się folder współdzielony) jest włączony i dostępny. • Sprawdź, czy nazwa użytkownika i/lub hasło do folderu uległy zmianie. • Sprawdź połączenie sieciowe.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Baza danych Serwera administracyjnego jest niedostępna	4109	KLSRV_DATABASE_UNAVAILABLE	Zdarzenia tego typu występują, jeśli baza danych Serwera administracyjnego stała się niedostępna. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy zdalny serwer, na którym jest zainstalowany serwer SQL, jest dostępny. • Przejrzyj raporty systemu DBMS, aby odkryć przyczynę braku dostępności bazy danych Serwera administracyjnego. Na przykład, ze względu na profilaktyczną obsługę, zdalny serwer z zainstalowanym serwerem SQL może być niedostępny.	180 dni
Brak wolnego miejsca w bazie danych Serwera administracyjnego	4110	KLSRV_DATABASE_FULL	Zdarzenia tego typu występują, gdy nie ma wolnego miejsca w bazie danych Serwera administracyjnego. Serwer administracyjny nie działa, gdy jego baza danych osiągnęła swoją pojemność i gdy dalsze zapisywanie w bazie danych nie jest możliwe. Poniżej wymienione są przyczyny tego zdarzenia, w zależności od systemu DBMS, którego używasz, oraz odpowiednie reakcje na to zdarzenie: • Korzystasz z SQL Server Express Edition DBMS: W dokumentacji SQL Server Express sprawdź ograniczenie rozmiaru bazy danych dla wersji, której używasz. Prawdopodobnie Twoja baza danych Serwera administracyjnego przekroczyła ograniczenie rozmiaru bazy danych. Ograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. W bazie danych Serwera administracyjnego istnieje zbyt dużo zdarzeń wysłanych przez komponent Kontrola aplikacji. Możesz zmienić ustawienia zasady Kaspersky Endpoint Security for Windows dotyczące przechowywania zdarzeń Kontroli aplikacji w bazie danych Serwera administracyjnego. • Używasz systemu DBMS innego niż SQL Server Express Edition: Nieograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Zmniejszanie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Przeglądanie informacji dotyczących wyboru systemu DBMS.	180 dni

Zdarzenia ostrzegające Serwera administracyjnego

Poniższa tabela prezentuje zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Ostrzeżenie**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia ostrzegające Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Wykryto często występujące zdarzenie		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje często występujące zdarzenie na zarządzanym urządzeniu. Aby uzyskać szczegółowe informacje, zapoznaj się z następującą sekcją: Blokowanie często występujących zdarzeń.	90 dni
Limit licencji został przekroczony	4098	KLSRV_EV_LICENSE_CHECK_100_110	Raz dziennie Kaspersky Security Center sprawdza, czy limity licencji nie zostały przekroczone. Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre ograniczenia licencyjne są przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją stanowi od 100% do 110% całkowitej liczby jednostek objętych licencją. Nawet jeśli to zdarzenie wystąpi, urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu. • Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center określa reguły generowania zdarzeń, gdy limit licencji zostanie przekroczony.	90 dni
Urządzenie było nieaktywne w sieci od dłuższego czasu	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Zdarzenia tego typu występują, gdy zarządzane urządzenie nie wykazuje brak aktywności przez pewien czas. Najczęściej dzieje się tak, gdy zarządzane urządzenie zostaje wycofane z eksploatacji. Możesz zareagować na zdarzenie w następujące sposoby: • W celu usunięcia urządzenia z listy zarządzanych urządzeń. • Określ przedział czasu, po którym tworzone jest zdarzenie **Urządzenie było nieaktywne w sieci od dłuższego czasu**, przy użyciu Konsoli administracyjnej lub przy użyciu Kaspersky Security Center Web Console. • Określ przedział czasu, po którym urządzenie zostanie automatycznie usunięte z grupy, przy użyciu Konsoli administracyjnej lub Kaspersky Security Center Web Console.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Konflikt nazw urządzeń	4102	KLSRV_EVENT_HOSTS_CONFLICT	Zdarzenia tego typu występują, gdy Serwer administracyjny traktuje dwa lub więcej zarządzanych urządzeń jako jedno urządzenie. Ma to miejsce najczęściej wtedy, gdy sklonowany dysk twardy został użyty do wdrożenia oprogramowania na zarządzanych urządzeniach i bez przełączania Agenta sieciowego do trybu klonowania dedykowanego dysku na odpowiednim urządzeniu. Aby uniknąć tego problemu, przełącz Agenta sieciowego do trybu klonowania dysku na odpowiednim urządzeniu przed sklonowaniem dysku twardego tego urządzenia.	90 dni
Stan urządzenia: Ostrzeżenie	4114	KLSRV_HOST_STATUS_WARNING	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan *Ostrzeżenie*. Możesz skonfigurować warunki, zgodnie z którymi stan urządzenia zostanie zmieniony na *Ostrzeżenie*.	90 dni
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony	4127	KLSRV_INVLICPROD_FILLED	Zdarzenia tego typu występują, gdy liczba instalacji aplikacji innych firm, zawartych w grupie licencjonowanych aplikacji osiągnie 90% maksymalnej dozwolonej wartości określonej we właściwościach klucza licencyjnego. Możesz zareagować na zdarzenie w następujące sposoby: • Jeśli aplikacja innej firmy nie jest używana na niektórych zarządzanych urządzeniach, usuń aplikację z tych urządzeń. • Jeśli spodziewasz się, że w najbliższej przyszłości liczba instalacji dla aplikacji innej firmy przekroczy dozwoloną maksymalną wartość, uwzględnij uzyskanie licencji innej firmy dla większej liczby urządzeń w przyszłości. Możesz zarządzać kluczami licencyjnymi aplikacji firm trzecich, korzystając z funkcjonalności grup licencjonowanych aplikacji.	90 dni
Certyfikat został zażądany	4133	KLSRV_CERTIFICATE_REQUESTED	Zdarzenia tego typu występują, gdy certyfikat dla Zarządzania urządzeniami mobilnymi nie zostanie automatycznie wystawiony ponownie. Poniżej znajdują się możliwe przyczyny wystąpienia tego zdarzenia oraz odpowiednie reakcje na nie: • Automatyczne ponowne wydawanie zostało zainicjowane dla certyfikatu, dla którego wyłączona jest opcja **Odnów certyfikat automatycznie, jeśli jest to możliwe**. Może to być spowodowane błędem, który wystąpił podczas tworzenia certyfikatu. Konieczne może być ręczne ponowne wystawienie certyfikatu. • Jeśli korzystasz z integracji z infrastrukturą klucza publicznego, przyczyną może być brak atrybutu SAM-Account-Name konta użytego do integracji z PKI oraz do wystawienia certyfikatu. Przejrzyj właściwości konta.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Certyfikat został usunięty	4134	KLSRV_CERTIFICATE_REMOVED	Zdarzenia tego typu występują, gdy administrator usunie dowolny typ certyfikatu (Ogólny, Poczta, VPN) dla Zarządzania urządzeniami mobilnymi. Po usunięciu certyfikatu urządzenia mobilne, podłączone za pośrednictwem tego certyfikatu, nie nawiążą połączenia z Serwerem administracyjnym. To zdarzenie może być pomocne podczas sprawdzania problemów z działaniem, skojarzonych z zarządzaniem urządzeń mobilnych.	90 dni
Certyfikat wygasa	6128	ServerCertificateExpiresSoon	Zdarzenia tego typu występują, gdy certyfikat Serwera administracyjnego dla urządzeń mobilnych i urządzeń UEFI utraci ważność. Należy zaktualizować certyfikat, który utracił ważność.	90 dni
Certyfikat APNs wygasł	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Zdarzenia tego typu występują, gdy certyfikat APNs utraci ważność. Należy ręcznie odnowić certyfikat APNs i zainstalować go na serwerze iOS MDM.	Nie jest przechowywany
Certyfikat APNs wkrótce utraci ważność	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Zdarzenia tego typu występują, gdy do wygaśnięcia certyfikatu APNs pozostało mniej niż 14 dni. Jeśli certyfikat APNs utraci ważność, należy ręcznie odnowić certyfikat APNs i zainstalować go na serwerze iOS MDM. Zalecane jest wcześniejsze utworzenie terminarza odnawiania certyfikatu APNs.	Nie jest przechowywany
Błąd podczas przesyłania wiadomości FCM do urządzenia mobilnego	4138	KLSRV_GCM_DEVICE_ERROR	Zdarzenia tego typu występują, gdy Zarządzanie urządzeniami mobilnymi jest skonfigurowane do użycia Firebase Cloud Messaging (FCM) w celu połączenia z zarządzanymi urządzeniami mobilnymi z systemem operacyjnym Android, a serwer FCM nie może obsłużyć niektórych żądań otrzymanych z Serwera administracyjnego. To oznacza, że niektóre zarządzane urządzenia mobilne nie otrzymają powiadomienia push. Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio. Więcej informacji na temat kodów HTTP otrzymanych z serwera FCM i powiązanych błędów można znaleźć w dokumentacji do usługi Firebase (zajrzyj do rozdziału „Podrzędne kody odpowiedzi na komunikaty o błędzie").	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Błąd HTTP podczas wysyłania wiadomości FCM do serwera FCM	4139	KLSRV_GCM_HTTP_ERROR	Zdarzenia tego typu występują, gdy Zarządzanie urządzeniami mobilnymi jest skonfigurowane do użycia Firebase Cloud Messaging (FCM) w celu połączenia z zarządzanymi urządzeniami mobilnymi z systemem operacyjnym Android, a serwer FCM przywróci żądanie Serwera administracyjnego z kodem HTTP innym niż 200 (OK). Poniżej znajdują się możliwe przyczyny wystąpienia tego zdarzenia oraz odpowiednie reakcje na nie: • Problemy po stronie serwera FCM. Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio. Więcej informacji na temat kodów HTTP otrzymanych z serwera FCM i powiązanych błędów można znaleźć w dokumentacji do usługi Firebase (zajrzyj do rozdziału „Podrzędne kody odpowiedzi na komunikaty o błędzie"). • Problemy po stronie serwera proxy (jeśli korzystasz z serwera proxy). Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio.	90 dni
Błąd podczas przesyłania wiadomości FCM do serwera FCM	4140	KLSRV_GCM_GENERAL_ERROR	Zdarzenia tego typu występują w wyniku niespodziewanych błędów po stronie Serwera administracyjnego podczas pracy z protokołem Firebase Cloud Messaging HTTP. Przeczytaj szczegóły w opisie zdarzenia i zareaguj odpowiednio. Jeżeli nie znajdziesz rozwiązania swojego problemu, skontaktuj się z działem pomocy technicznej firmy Kaspersky.	90 dni
Pozostała niewielka ilość wolnego miejsca na dysku twardym	4105	KLSRV_NO_SPACE_ON_VOLUMES	Tego typu zdarzenia występują, gdy dysk twardy urządzenia, na którym jest zainstalowany Serwer administracyjny, prawie zabraknie wolnego miejsca. Zwolnij miejsce na dysku na urządzeniu.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Mała ilość wolnego miejsca w bazie danych Serwera administracyjnego	4106	KLSRV_NO_SPACE_IN_DATABASE	Zdarzenia tego typu występują, jeśli miejsce w bazie danych Serwera administracyjnego jest zbyt ograniczone. Jeśli nie rozwiążesz tego problemu, wkrótce baza danych Serwera administracyjnego osiągnie swoją pojemność, a Serwer administracyjny nie będzie działał. Poniżej wymienione są przyczyny tego zdarzenia, w zależności od systemu DBMS, którego używasz, oraz odpowiednie reakcje na to zdarzenie. Korzystasz z SQL Server Express Edition DBMS: • W dokumentacji SQL Server Express sprawdź ograniczenie rozmiaru bazy danych dla wersji, której używasz. Prawdopodobnie Twoja baza danych Serwera administracyjnego zaraz osiągnie ograniczenie rozmiaru bazy danych. • Ograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • W bazie danych Serwera administracyjnego istnieje zbyt dużo zdarzeń wysłanych przez komponent Kontrola aplikacji. Możesz zmienić ustawienia zasady Kaspersky Endpoint Security for Windows dotyczące przechowywania zdarzeń Kontroli aplikacji w bazie danych Serwera administracyjnego. Używasz systemu DBMS innego niż SQL Server Express Edition: • Nieograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Przeglądanie informacji dotyczących wyboru systemu DBMS.	90 dni
Połączenie z podrzędnym Serwerem administracyjnym zostało zerwane	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Zdarzenia tego typu występują, gdy połączenie z podrzędnym Serwerem administracyjnym zostanie przerwane. Przeczytaj dziennik zdarzeń aplikacji Kaspersky na urządzeniu, na którym jest zainstalowany podrzędny Serwer administracyjny i zareaguj odpowiednio.	90 dni
Połączenie z głównym Serwerem administracyjnym zostało zerwane	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Zdarzenia tego typu występują, gdy połączenie z głównym Serwerem administracyjnym zostanie przerwane. Przeczytaj dziennik zdarzeń aplikacji Kaspersky na urządzeniu, na którym jest zainstalowany główny Serwer administracyjny i zareaguj odpowiednio.	90 dni
Zarejestrowano nowe aktualizacje dla modułów aplikacji Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Zdarzenia tego typu występują, gdy Serwer administracyjny zarejestruje nowe aktualizacje dla oprogramowania firmy Kaspersky, zainstalowanego na zarządzanych urządzeniach, których instalacja wymaga zatwierdzenia. Zatwierdź lub odrzuć aktualizacje, korzystając z Konsoli administracyjnej lub Kaspersky Security Center Web Console.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Przekroczono limit wydarzeń w bazie danych. Rozpoczęto usuwanie wydarzeń	4145	KLSRV_EVP_DB_TRUNCATING	Zdarzenia tego typu występują, jeśli usuwanie starszych zdarzeń z bazy danych Serwera administracyjnego rozpoczęło się, gdy pojemność bazy danych Serwera administracyjnego została osiągnięta. Możesz zareagować na zdarzenie w następujące sposoby: • Zmiana maksymalnej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	Nie jest przechowywany
Przekroczono limit wydarzeń w bazie danych. Usunięto wydarzenia	4146	KLSRV_EVP_DB_TRUNCATED	Zdarzenia tego typu występują, jeśli starsze zdarzenia zostały usunięte z bazy danych Serwera administracyjnego po osiągnięciu pojemności bazy danych Serwera administracyjnego. Możesz zareagować na zdarzenie w następujące sposoby: • Zmiana maksymalnej dozwolonej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	Nie jest przechowywany
Audyt (połączenie testowe z serwerem SIEM nie powiodło się)	5120	KLAUD_EV_SIEM_TEST_FAILED	Zdarzenia tego typu mają miejsce w przypadku niepowodzenia połączenia testowego z serwerem SIEM.	30 dni
Nie udało się automatycznie wystawić certyfikatu		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Zdarzenia tego typu mają miejsce w przypadku wystąpienia błędu podczas tworzenia certyfikatu klienta dla urządzenia mobilnego (urządzenia działającego w oparciu o protokół mobilny).	90 dni

Zdarzenia informacyjne Serwera administracyjnego

Poniższa tabela prezentuje zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Informacja**.

Zdarzenia informacyjne Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania	Uwagi
Ponad 90% tego klucza licencyjnego jest wykorzystane	4097	KLSRV_EV_LICENSE_CHECK_90	30 dni	
Wykryto nowe urządzenie	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 dni	
Urządzenie zostało automatycznie dodane do grupy	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 dni	
Urządzenie zostało automatycznie przeniesione zgodnie z regułą	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 dni	
Urządzenie zostało usunięte z grupy: nieaktywność w sieci od dłuższego czasu	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 dni	

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania	Uwagi
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony (wykorzystywanych jest więcej niż 95%)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 dni	
Wykryto pliki do przesłania do firmy Kaspersky w celu analizy	4131	KLSRV_APS_FILE_APPEARED	30 dni	
ID instancji FCM na tym urządzeniu mobilnym zmieniło się	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 dni	
Aktualizacje zostały pomyślnie skopiowane do wskazanego folderu	4122	KLSRV_UPD_REPL_OK	30 dni	
Nawiązano połączenie z podrzędnym Serwerem administracyjnym	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 dni	
Nawiązano połączenie z głównym Serwerem administracyjnym	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 dni	
Bazy danych zostały zaktualizowane	4144	KLSRV_UPD_BASES_UPDATED	30 dni	
Audyt: Połączenie z Serwerem administracyjnym zostało nawiązane	4147	KLAUD_EV_SERVERCONNECT	30 dni	
Audyt: Obiekt został zmodyfikowany	4148	KLAUD_EV_OBJECTMODIFY	30 dni	To zdarzenie śledzi zmiany w następujących obiektach: • Grupa administracyjna • Grupa bezpieczeństwa • Użytkownik • Pakiet • Zadanie • Zasada • Serwer • Wirtualny serwer
Audyt: Stan obiektu zmienił się	4150	KLAUD_EV_TASK_STATE_CHANGED	30 dni	Na przykład to zdarzenie występuje, gdy zadanie nie powiodło się z powodu błędu.
Audyt: Ustawienia grupy zostały zmodyfikowane	4149	KLAUD_EV_ADMGROUP_CHANGED	30 dni	
Audyt: Połączenie z Serwerem administracyjnym zostało zakończone	4151	KLAUD_EV_SERVERDISCONNECT	30 dni	
Audyt: Właściwości obiektu zostały zmodyfikowane	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 dni	To zdarzenie śledzi zmiany w następujących właściwościach: • Użytkownik • Licencja • Serwer • Wirtualny serwer

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania	Uwagi
Audyt: uprawnienia użytkownika zostały zmodyfikowane	4153	KLAUD_EV_OBJECTACLMODIFIED	30 dni	
Audyt: Klucze szyfrowania zostały zaimportowane lub wyeksportowane z Serwera administracyjnego	5100	KLAUD_EV_DPEKEYSEXPORT	30 dni	
Audyt (połączenie testowe z serwerem SIEM powiodło się)	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 dni	Zdarzenia tego typu mają miejsce w przypadku udanego połączenia testowego z serwerem SIEM.
Utworzono certyfikat zapasowy		ServerReserveCertificateCreated	30 dni	To zdarzenie występuje, gdy zostanie utworzony certyfikat Serwera administracyjnego.
Odnowienie certyfikatu		ServerCertificateRenewed	30 dni	To zdarzenie występuje, gdy zostanie odnowiony certyfikat Serwera administracyjnego.
Certyfikat został pomyślnie wystawiony automatycznie		KLSRV_CERTIFICATE_AUTO_ISSUED	30 dni	Zdarzenie tego typu występuje, gdy certyfikat dla urządzenia mobilnego (urządzenia działającego w oparciu o protokół mobilny) zostanie pomyślnie utworzony.

Zdarzenia **Utworzono certyfikat zapasowy, Odnowienie certyfikatu** oraz **Certyfikat został pomyślnie wystawiony automatycznie** są automatycznie publikowane przez Serwer administracyjny i wyświetlane w Konsoli administracyjnej tylko wtedy, gdy operacje odpowiadające tym zdarzeniom zostaną wykonane dla certyfikatów Serwera administracyjnego dla urządzeń mobilnych i urządzeń UEFI.

Zdarzenia Agenta sieciowego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Agenta sieciowego.

Zdarzenia błędu funkcjonalnego Agenta sieciowego

Poniższa tabela wyświetla typy zdarzeń Agenta sieciowego Kaspersky Security Center, których priorytet to **Błąd funkcjonalny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Błąd podczas instalacji aktualizacji	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli automatyczne aktualizowanie i instalowanie poprawek dla składników Kaspersky Security Center nie zakończyło się pomyślnie. Zdarzenie nie dotyczy aktualizacji zarządzanych aplikacji firmy Kaspersky. Przeczytaj opis zdarzenia. Przyczyną tego zdarzenia może być problem z systemem Windows na Serwerze administracyjnym. Jeśli w opisie wspomniany jest jakikolwiek problem z konfiguracją systemu Windows, rozwiąż ten problem.	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej nie powiodła się	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli używane są funkcje Zarządzanie lukami i poprawkami i Zarządzanie urządzeniami mobilnymi oraz jeśli aktualizacja oprogramowania innych firm nie zakończyła się pomyślnie. Sprawdź, czy odnośnik do oprogramowania innej firmy jest ważny. Przeczytaj opis zdarzenia.	30 dni
Zainstalowanie aktualizacji Windows Update nie powiodło się	7717	KLNAG_EV_WUA_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli aktualizacje systemu Windows nie zakończyły się pomyślnie. Konfiguruj aktualizacji systemu Windows w zasadzie Agenta sieciowego. Przeczytaj opis zdarzenia. Poszukaj błędu w Bazie wiedzy Microsoft. Skontaktuj się z pomocą techniczną Microsoft, jeśli sam nie możesz rozwiązać problemu.	30 dni
Zarządzanie użytkownikami: błędy	7723	KLNAG_EV_USR_MNG_ERR	Ogólne zdarzenie ostrzegające.	30 dni
Nie udało się przywrócić pliku sudoers do wartości referencyjnej	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Zdarzenie zawiera opis błędu zamiany pliku sudoers.	30 dni
Instalacja certyfikatów głównych nie powiodła się	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Zdarzenie zawiera opis błędu instalacji certyfikatów.	30 dni
Usunięcie certyfikatów głównych nie powiodło się	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Zdarzenie zawiera opis błędu usunięcia certyfikatów.	30 dni

Zdarzenia ostrzegające Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego Kaspersky Security Center, które posiadają priorytet **Ostrzeżenie**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia ostrzegające Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Proces instalacji aktualizacji modułów oprogramowania zwrócił ostrzeżenie	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została zakończona ostrzeżeniem	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została odroczona	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 dni
Wystąpił incydent związany z bezpieczeństwem	549	GNRL_EV_APP_INCIDENT_OCCURED	30 dni
Serwer KSN proxy został uruchomiony. Sprawdzenie dostępności KSN nie powiodło się	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 dni
Zarządzanie użytkownikami: ostrzeżenia	7722	KLNAG_EV_USR_MNG_WRN	30 dni
Plik Sudoers nie pasuje do wartości referencyjnej	7724	KLNAG_EV_SUDOER_DIFFERENT	30 dni

Zdarzenia informacyjne Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego Kaspersky Security Center, które posiadają priorytet **Informacja**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia informacyjne Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Aktualizacja modułów aplikacji została pomyślnie zainstalowana	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 dni
Instalacja aktualizacji modułów oprogramowania została uruchomiona	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 dni
Aplikacja została zainstalowana	7703	KLNAG_EV_INV_APP_INSTALLED	30 dni
Aplikacja została odinstalowana	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 dni
Monitorowana aplikacja została zainstalowana	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 dni
Monitorowana aplikacja została odinstalowana	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 dni
Aplikacja innego producenta została zainstalowana	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 dni
Dodano nowe urządzenie	7708	KLNAG_EV_DEVICE_ARRIVAL	30 dni
Urządzenie zostało usunięte	7709	KLNAG_EV_DEVICE_REMOVE	30 dni
Wykryto nowe urządzenie	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 dni
Urządzenie zostało zautoryzowane	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 dni
Udostępnianie pulpitu Windows: Plik został odczytany	7712	KLUSRLOG_EV_FILE_READ	30 dni
Udostępnianie pulpitu Windows: Plik został zmodyfikowany	7713	KLUSRLOG_EV_FILE_MODIFIED	30 dni
Udostępnianie pulpitu Windows: Aplikacja została uruchomiona	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 dni
Udostępnianie pulpitu Windows: Uruchomiono	7715	KLUSRLOG_EV_WDS_BEGIN	30 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Udostępnianie pulpitu Windows: Zatrzymano	7716	KLUSRLOG_EV_WDS_END	30 dni
Aktualizacja oprogramowania firmy trzeciej została pomyślnie zainstalowana	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została uruchomiona	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 dni
Serwer KSN proxy został uruchomiony. Sprawdzenie dostępności KSN zostało pomyślnie zakończone	7719	KSNPROXY_STARTED_CON_CHK_OK	30 dni
KSN Proxy został zatrzymany	7720	KSNPROXY_STOPPED	30 dni

Zdarzenia serwera iOS MDM

Ta sekcja zawiera informacje o zdarzeniach dotyczących serwera iOS MDM.

Zdarzenia błędu funkcjonalnego serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Błąd funkcjonalny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia błędu funkcjonalnego serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Pobranie listy profili nie powiodło się	PROFILELIST_COMMAND_FAILED	30 dni
Instalacja profilu nie powiodła się	INSTALLPROFILE_COMMAND_FAILED	30 dni
Usunięcie profilu nie powiodło się	REMOVEPROFILE_COMMAND_FAILED	30 dni
Pobranie listy profili informacyjnych nie powiodło się	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 dni
Instalacja profilu informacyjnego nie powiodła się	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 dni
Usunięcie profilu informacyjnego nie powiodło się	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 dni
Usunięcie profilu informacyjnego nie powiodło się	CERTIFICATELIST_COMMAND_FAILED	30 dni
Pobranie listy zainstalowanych aplikacji nie powiodło się	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 dni
Pobranie ogólnych informacji o urządzeniu mobilnym nie powiodło się	DEVICEINFORMATION_COMMAND_FAILED	30 dni
Pobranie informacji o zabezpieczeniach nie powiodło się	SECURITYINFO_COMMAND_FAILED	30 dni
Zablokowanie urządzenia mobilnego nie powiodło się	DEVICELOCK_COMMAND_FAILED	30 dni
Zresetowanie hasła nie powiodło się	CLEARPASSCODE_COMMAND_FAILED	30 dni
Usunięcie danych z urządzenia mobilnego nie powiodło się	ERASEDEVICE_COMMAND_FAILED	30 dni
Instalacja aplikacji nie powiodła się	INSTALLAPPLICATION_COMMAND_FAILED	30 dni
Ustawienie kodu wykupu dla aplikacji nie powiodło się	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 dni

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Pobranie listy zarządzanych aplikacji nie powiodło się	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 dni
Usunięcie zarządzanej aplikacji nie powiodło się	REMOVEAPPLICATION_COMMAND_FAILED	30 dni
Ustawienia roamingu zostały odrzucone	SETROAMINGSETTINGS_COMMAND_FAILED	30 dni
Wystąpił błąd działania aplikacji	PRODUCT_FAILURE	30 dni
Wynik polecenia zawiera niepoprawne dane	MALFORMED_COMMAND	30 dni
Przesłanie powiadomienia push nie powiodło się	SEND_PUSH_NOTIFICATION_FAILED	30 dni
Wysłanie polecenia nie powiodło się	SEND_COMMAND_FAILED	30 dni
Nie odnaleziono urządzenia	DEVICE_NOT_FOUND	30 dni

Zdarzenia ostrzegające serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Ostrzeżenie**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia ostrzegające serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Wykryto próbę podłączenia zablokowanego urządzenia mobilnego	INACTICE_DEVICE_TRY_CONNECTED	30 dni
Profil został usunięty	MDM_PROFILE_WAS_REMOVED	30 dni
Wykryto próbę ponownego użycia certyfikatu klienta	CLIENT_CERT_ALREADY_IN_USE	30 dni
Wykryto nieaktywne urządzenie	FOUND_INACTIVE_DEVICE	30 dni
Wymagany jest kod wykupu	NEED_REDEMPTION_CODE	30 dni
Profil zawarty w zasadach został usunięty z urządzenia	UMDM_PROFILE_WAS_REMOVED	30 dni

Zdarzenia informacyjne serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Informacja**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia informacyjne serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Podłączono nowe urządzenie mobilne	NEW_DEVICE_CONNECTED	30 dni
Lista profili została pomyślnie pobrana	PROFILELIST_COMMAND_SUCCESSFULL	30 dni
Profil został pomyślnie zainstalowany	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 dni
Profil został pomyślnie usunięty	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 dni

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Lista profili informacyjnych została pomyślnie pobrana	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 dni
Profil informacyjny został pomyślnie zainstalowany	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dni
Profil informacyjny został pomyślnie usunięty	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dni
Lista certyfikatów cyfrowych została pomyślnie pobrana	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 dni
Lista zainstalowanych aplikacji została pomyślnie zażądana	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dni
Ogólne informacje o urządzeniu mobilnym zostały pomyślnie pobrane	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 dni
Informacje o zabezpieczeniach zostały pomyślnie pobrane	SECURITYINFO_COMMAND_SUCCESSFULL	30 dni
Urządzenie mobilne zostało pomyślnie zablokowane	DEVICELOCK_COMMAND_SUCCESSFULL	30 dni
Hasło zostało pomyślnie zresetowane	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 dni
Dane zostały pomyślnie usunięte z urządzenia mobilnego	ERASEDEVICE_COMMAND_SUCCESSFULL	30 dni
Aplikacja została pomyślnie zainstalowana	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 dni
Kod wykupu aplikacji został pomyślnie ustawiony dla aplikacji	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 dni
Lista zarządzanych aplikacji została pomyślnie pobrana	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dni
Zarządzana aplikacja została pomyślnie usunięta	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 dni
Ustawienia roamingu zostały pomyślnie zastosowane	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 dni

Blokowanie często występujących zdarzeń

Ta sekcja zawiera informacje dotyczące zarządzania blokowaniem często występujących zdarzeń, usuwania blokowania często występujących zdarzeń oraz eksportowania listy często występujących zdarzeń do pliku.

Informacje o blokowaniu często występujących zdarzeń

Zarządzana aplikacja, na przykład Kaspersky Endpoint Security for Windows, zainstalowana na jednym lub kilku zarządzanych urządzeniach, może wysyłać wiele zdarzeń tego samego typu do Serwera administracyjnego. Otrzymywanie częstych zdarzeń może przeciążyć bazę danych Serwera administracyjnego i nadpisać inne zdarzenia. Serwer administracyjny zaczyna blokować najczęstsze zdarzenia, gdy liczba wszystkich odebranych zdarzeń przekracza określony limit dla bazy danych.

Serwer administracyjny blokuje automatyczne odbieranie często występujących zdarzeń. Nie możesz samodzielnie blokować często występujących zdarzeń ani wybierać, które zdarzenia mają być blokowane.

Jeśli chcesz dowiedzieć się, czy zdarzenie jest zablokowane, możesz sprawdzić, czy to zdarzenie jest obecne w sekcji **Blokowanie często występujących zdarzeń** właściwości Serwera administracyjnego. Jeśli zdarzenie jest zablokowane, możesz wykonać następujące czynności:

- Jeśli chcesz zapobiec nadpisywaniu bazy danych, możesz kontynuować blokowanie odbieranie tego typu zdarzeń.
- Jeśli chcesz, na przykład, znaleźć przyczynę wysyłania często występujących zdarzeń na Serwer administracyjny, możesz odblokować często występujące zdarzenia i mimo wszystko nadal otrzymywać tego typu zdarzenia.
- Jeśli chcesz nadal otrzymywać często występujące zdarzenia, dopóki nie zostaną ponownie zablokowane, możesz usunąć z blokowania często występujące zdarzenia.

Zarządzanie blokowaniem często występujących zdarzeń

Serwer administracyjny automatycznie blokuje odbieranie często występujących zdarzeń, ale możesz zatrzymać blokowanie i nadal odbierać często występujące zdarzenia. Możesz także zablokować odbieranie często występujących zdarzeń, które wcześniej odblokowałeś.

W celu zarządzania blokowaniem często występujących zdarzeń:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Blokowanie często występujących zdarzeń**.
3. W sekcji **Blokowanie często występujących zdarzeń**:
   - Wybierz opcje **Typ zdarzenia** zdarzeń, których odbieranie chcesz zablokować.
   - Odznacz opcje **Typ zdarzenia** zdarzeń, które chcesz nadal otrzymywać.
4. Kliknij przycisk **Zastosuj**.
5. Kliknij przycisk **OK**.

Serwer administracyjny odbiera często występujące zdarzenia, dla których usunięto zaznaczenie opcji **Typ zdarzenia** i blokuje odbieranie często występujących zdarzeń, dla których wybrałeś opcję **Typ zdarzenia**.

Usuwanie blokowania często występujących zdarzeń

Możesz usunąć blokowanie często występujących zdarzeń i zacząć je otrzymywać, dopóki Serwer administracyjny nie zablokuje ponownie tego typu często występujących zdarzeń.

W celu usunięcia blokowania często występujących zdarzeń:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Blokowanie często występujących zdarzeń**.
3. W sekcji **Blokowanie często występujących zdarzeń** kliknij wiersz często występującego zdarzenia, dla którego chcesz usunąć blokowanie.
4. Kliknij przycisk **Usuń**.

Często występujące zdarzenie zostanie usunięte z listy często występujących zdarzeń. Serwer administracyjny będzie odbierał zdarzenia tego typu.

Eksportowanie listy często występujących zdarzeń do pliku

W celu wyeksportowania listy często występujących zdarzeń do pliku:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Blokowanie często występujących zdarzeń**.
3. Kliknij przycisk **Eksportuj do pliku**.
4. W oknie **Zapisz jako**, które zostanie otwarte, określ ścieżkę dostępu do pliku, do którego chcesz zapisać listę.
5. Kliknij przycisk **Zapisz**.

Wszystkie wpisy z listy często występujących zdarzeń są eksportowane do pliku.

Kontrolowanie zmian w stanie maszyn wirtualnych

Serwer administracyjny przechowuje informacje o stanie zarządzanych urządzeń, takie jak rejestr sprzętu i lista zainstalowanych aplikacji, a także ustawienia zarządzanych aplikacji, zadań i zasad. Jeśli maszyna wirtualna funkcjonuje jak zarządzane urządzenie, użytkownik może przywrócić jego stan w dowolnym momencie przy pomocy wcześniej utworzonych zrzutów ekranu maszyny wirtualnej. Informacje o stanie maszyny wirtualnej na Serwerze administracyjnym mogą stać się nieaktualne.

Na przykład administrator utworzył zasadę ochrony na Serwerze administracyjnym o godzinie 12:00, który zaczął funkcjonować na maszynie wirtualnej VM_1 o godzinie 12:01. O godzinie 12:30 użytkownik maszyny wirtualnej VM_1 zmienił jej stan, przywracając ją ze zrzutu ekranu zrobionego o godzinie 11:00. Zasada ochrony przestaje działać na maszynie wirtualnej. Jednakże w przestarzałych informacjach przechowywanych na Serwerze administracyjnym można przeczytać, że zasada ochrony na maszynie wirtualnej VM_1 wciąż działa.

Program Kaspersky Security Center pomaga monitorować zmiany w stanie maszyn wirtualnych.

Po każdej synchronizacji z urządzeniem, Serwer administracyjny generuje unikatowy numer ID, który jest przechowywany na urządzeniu i na Serwerze administracyjnym. Przed rozpoczęciem kolejnej synchronizacji Serwer administracyjny porównuje wartości tych numerów ID po obu stronach. Jeśli wartości numerów ID nie zgadzają się, Serwer administracyjny rozpoznaje, że maszyna wirtualna została przywrócona ze zrzutu ekranu. Serwer administracyjny resetuje wszystkie ustawienia zasad i zadań, które są aktywne dla maszyny wirtualnej, i wysyła na nią aktualne zasady oraz listę zadań grupowych.

Monitorowanie stanu ochrony antywirusowej przy użyciu informacji z rejestru systemu

W celu monitorowania stanu ochrony antywirusowej na urządzeniu klienckim przy użyciu informacji zarejestrowanych przez Agenta sieciowego, w zależności od systemu operacyjnego urządzenia:

- Na urządzeniach działających pod kontrolą systemu Windows:

  1. Otwórz rejestr systemu urządzenia klienckiego (na przykład, lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).

  2. Przejdź do gałęzi:

     - W systemach 32-bitowych:
       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

     - W systemach 64-bitowych:
       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     Rejestr systemu wyświetli informacje o stanie ochrony antywirusowej urządzenia klienckiego.

- Na urządzeniach działających pod kontrolą systemu Linux:

  - Informacje są umieszczane w oddzielnych plikach tekstowych, jeden dla każdego typu danych, znajdujących się w następującym miejscu: /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/.

- Na urządzeniach działających pod kontrolą systemu macOS:

  - Informacje są umieszczane w oddzielnych plikach tekstowych, jeden dla każdego typu danych, znajdujących się w następującym miejscu: /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/.

Stan ochrony antywirusowej odpowiada wartościom kluczy opisanym w tabeli znajdującej się poniżej.

Klucze rejestru i ich możliwe wartości

Klucz (typ danych)	Wartość	Opis
`Protection_LastConnected (REG_SZ)`	DD-MM-RRRR GG-MM-SS	Data i godzina (w formacie UTC) ostatniego połączenia z Serwerem administracyjnym
`Protection_AdmServer (REG_SZ)`	IP, nazwa DNS lub nazwa NetBIOS	Nazwa Serwera administracyjnego zarządzającego urządzeniem
`Protection_NagentVersion (REG_SZ)`	a.b.c.d	Numer kompilacji Agenta sieciowego zainstalowanego na urządzeniu
`Protection_NagentFullVersion (REG_SZ)`	a.b.c.d (patch1; patch2; ...; patchN)	Pełny numer wersji Agenta sieciowego (z poprawkami) zainstalowanego na urządzeniu
`Protection_HostId (REG_SZ)`	ID urządzenia	ID urządzenia

Klucz (typ danych)	Wartość	Opis
`Protection_DynamicVM (REG_DWORD)`	0 — nie 1 — tak	Agent sieciowy jest instalowany w dynamicznym trybie VDI
`Protection_AvInstalled (REG_DWORD)`	0 — nie 1 — tak	Aplikacja antywirusowa jest zainstalowana na urządzeniu
`Protection_AvRunning (REG_DWORD)`	0 — nie 1 — tak	Ochrona w czasie rzeczywistym jest włączona na urządzeniu
`Protection_HasRtp (REG_DWORD)`	0 — nie 1 — tak	Moduł ochrony w czasie rzeczywistym jest zainstalowany
`Protection_RtpState (REG_DWORD)`	Stan ochrony w czasie rzeczywistym:	
	0	Nieznany
	1	Wyłączony
	2	Wstrzymane
	3	Uruchamiana
	4	Włączona
	5	Włączona z wysokim poziomem ochrony (maksymalna ochrona)
	6	Włączona z niskim poziomem ochrony (maksymalna szybkość)
	7	Włączona z ustawieniami domyślnymi (zalecanymi)
	8	Włączona z ustawieniami niestandardowymi
	9	Błąd działania
`Protection_LastFscan (REG_SZ)`	DD-MM-RRRR GG-MM-SS	Data i godzina (w formacie UTC) ostatniego pełnego skanowania
`Protection_BasesDate (REG_SZ)`	DD-MM-RRRR GG-MM-SS	Data i godzina (w formacie UTC) opublikowania baz danych aplikacji

Przeglądanie i konfigurowanie działań, gdy urządzenia wykazują brak aktywności

Jeśli urządzenia klienckie w grupie są nieaktywne, możesz otrzymać informacje na ten temat. Możesz także automatycznie usuwać takie urządzenia.

W celu przejrzenia lub skonfigurowania działań, gdy urządzenia w grupie wykazują brak aktywności:

1. W drzewie konsoli kliknij prawym klawiszem myszy nazwę żądanej grupy administracyjnej.
2. Z menu kontekstowego wybierz **Właściwości**.

   Spowoduje to otwarcie okna właściwości grupy administracyjnej.
3. W oknie **Właściwości** przejdź do sekcji **Urządzenia**.
4. Jeśli to konieczne, włącz lub wyłącz następujące opcje:

   - **Powiadom administratora, jeżeli urządzenie jest nieaktywne dłużej niż (dni)**

     Jeśli ta opcja jest włączona, administrator otrzyma powiadomienie o nieaktywnych urządzeniach. Możesz określić przedział czasu, po upływie którego tworzone jest zdarzenie **Urządzenie było nieaktywne w sieci od bardzo dawna**. Domyślny przedział czasu wynosi 7 dni.

     Domyślnie opcja ta jest włączona.

- **Usuń urządzenie z grupy, jeżeli było nieaktywne dłużej niż (dni)**

  Jeśli ta opcja jest włączona, możesz określić przedział czasu, po upływie którego urządzenie zostanie automatycznie usunięte z grupy. Domyślny przedział czasu wynosi 60 dni.

  Domyślnie opcja ta jest włączona.

- **Dziedzicz z grupy nadrzędnej**

  Ustawienia z tej sekcji są dziedziczone od grupy nadrzędnej, w której znajduje się urządzenie klienckie. Jeśli ta opcja jest włączona, ustawienia w sekcji **Aktywność urządzenia w sieci** nie mogą być modyfikowane.

  Ta opcja jest dostępna tylko wtedy, gdy grupa administracyjna posiada grupę nadrzędną.

  Domyślnie opcja ta jest włączona.

- **Wymuś dziedziczenie w grupach podrzędnych**

  Wartości ustawień zostaną rozesłane do grup podrzędnych ale we właściwościach grup podrzędnych te ustawienia są zablokowane.

  Domyślnie opcja ta jest wyłączona.

5. Kliknij **OK**.

Twoje zmiany zostaną zapisane i zastosowane.

Wyłączanie ogłoszeń Kaspersky

W Kaspersky Security Center Web Console sekcja Ogłoszenia firmy Kaspersky (**Monitorowanie i raportowanie → Ogłoszenia firmy Kaspersky**) zawiera informacje dotyczące Twojej wersji Kaspersky Security Center i zarządzanych aplikacji, zainstalowanych na zarządzanych urządzeniach. Jeśli nie chcesz otrzymywać ogłoszeń firmy Kaspersky, możesz wyłączyć tę funkcję.

Ogłoszenia firmy Kaspersky obejmują dwa rodzaje informacji: ogłoszenia związane z bezpieczeństwem oraz ogłoszenia marketingowe. Możesz wyłączyć ogłoszenia każdego typu osobno.

W celu wyłączenia ogłoszeń związanych z bezpieczeństwem:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz wyłączyć ogłoszenia dotyczące bezpieczeństwa.

2. Kliknij go prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Właściwości**.

3. W otwartym oknie właściwości Serwera administracyjnego, w sekcji **Ogłoszenia Kaspersky** wyłącz opcję **Włącz wyświetlanie ogłoszeń Kaspersky w Kaspersky Security Center Web Console**.

4. Kliknij **OK**.

Ogłoszenia firmy Kaspersky są wyłączone.

Ogłoszenia marketingowe są domyślnie wyłączone. Otrzymujesz ogłoszenia marketingowe tylko wtedy, gdy włączyłeś Kaspersky Security Network (KSN). Możesz wyłączyć tego typu ogłoszenia, wyłączając KSN.

Dostosowanie punktów dystrybucji i bram połączenia

Struktura grup administracyjnych w Kaspersky Security Center pełni następujące funkcje:

- Tworzy zakres zasad

  Istnieje alternatywny sposób stosowania odpowiednich ustawień na urządzeniach przy użyciu *profili zasad*. W tym przypadku ustawiasz zakres zasad ze znacznikami, lokalizacjami urządzeń w jednostkach organizacyjnych Active Directory, członkostwem w grupach zabezpieczeń Active Directory.

- Tworzy zakres zadań grupowych

  Istnieje sposób określania zakresu zadań grupowych, który nie jest oparty na hierarchii grup administracyjnych: korzystanie z zadań dla wyboru urządzeń oraz z zadań dla określonych urządzeń.

- Nadaje urządzeniom, wirtualnym Serwerom administracyjnym oraz podrzędnym Serwerom administracyjnym prawa dostępu

- Przypisuje punkty dystrybucji

Podczas tworzenia struktury grup administracyjnych należy wziąć pod uwagę topologię sieci organizacji dla optymalnego przydzielenia punktów dystrybucji. Optymalne przydzielenie punktów dystrybucji pozwala na zmniejszenie ruchu w sieci organizacji.

W zależności od schematu organizacyjnego oraz topologii sieci, w strukturze grup administracyjnych można zastosować następujące standardowe konfiguracje:

- Jedno biuro

- Wiele małych, zdalnych biur

Urządzenia pełniące rolę punktów dystrybucji muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

Standardowa konfiguracja punktów dystrybucji: Jedno biuro

W standardowej konfiguracji „jedno biuro" wszystkie urządzenia znajdują się w obrębie sieci organizacji i są dla siebie widoczne. Sieć organizacji może zawierać kilka oddzielnych części (sieci lub fragmentów sieci) połączonych ze sobą wąskimi kanałami.

Dostępne są następujące metody tworzenia struktury grup administracyjnych:

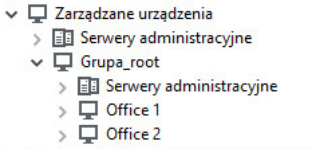
- Tworzenie struktury grup administracyjnych z uwzględnieniem topologii sieci. Struktura grup administracyjnych nie musi odzwierciedlać topologii sieci z absolutną dokładnością. Wystarczy dopasowanie oddzielnych części sieci i pewnych grup administracyjnych. Możesz skorzystać z automatycznego przydzielenia punktów dystrybucji lub zrobić to ręcznie.

- Tworzenie struktury grup administracyjnych bez uwzględnienia topologii sieci. W tym przypadku należy wyłączyć automatyczne przydzielanie punktów dystrybucji, a następnie wskazać jedno lub kilka urządzeń jako punkty dystrybucji dla głównej grupy administracyjnej w każdej z oddzielnych części sieci, na przykład dla grupy **Zarządzane urządzenia**. Wszystkie punkty dystrybucji będą na tym samym poziomie i będą obejmować ten sam obszar, uwzględniając wszystkie urządzenia w sieci organizacji. W takim przypadku każdy z Agentów sieciowych połączy się z punktem dystrybucji o najkrótszej trasie. Trasę do punktu dystrybucji można ustalić za pomocą narzędzia tracert.

Standardowa konfiguracja punktów dystrybucji: Małe zdalne biura

Ta standardowa konfiguracja została utworzona z myślą o małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem internetu. Każde zdalne biuro znajduje się poza NAT, czyli połączenie jednego zdalnego biura z innym jest niemożliwe, gdyż biura są od siebie odizolowane.

Konfiguracja musi być odzwierciedlona w strukturze grup administracyjnych: dla każdego zdalnego biura musi zostać utworzona oddzielna grupa administracyjna (grupy **Office 1** i **Office 2** na rysunku poniżej).



Zdalne biura uwzględnione w strukturze grupy administracyjnej

Do każdej grupy administracyjnej odpowiadającej biuru należy przydzielić jeden lub kilka punktów dystrybucji. Punktami dystrybucji muszą być urządzenia w zdalnym biurze, które posiadają wystarczającą ilość wolnego miejsca na dysku. Urządzenia z grupy **Office 1** będą, na przykład, łączyć się z punktami dystrybucji przydzielonymi do grupy administracyjnej **Office 1**.

Jeśli niektórzy użytkownicy poruszają się między biurami ze swoimi laptopami, w każdym zdalnym biurze, dla grupy administracyjnej najwyższego poziomu (**Główna grupa dla biur** na poniższym rysunku) należy wskazać dwa lub więcej urządzeń jako punkty dystrybucji (oprócz już istniejących punktów dystrybucji).

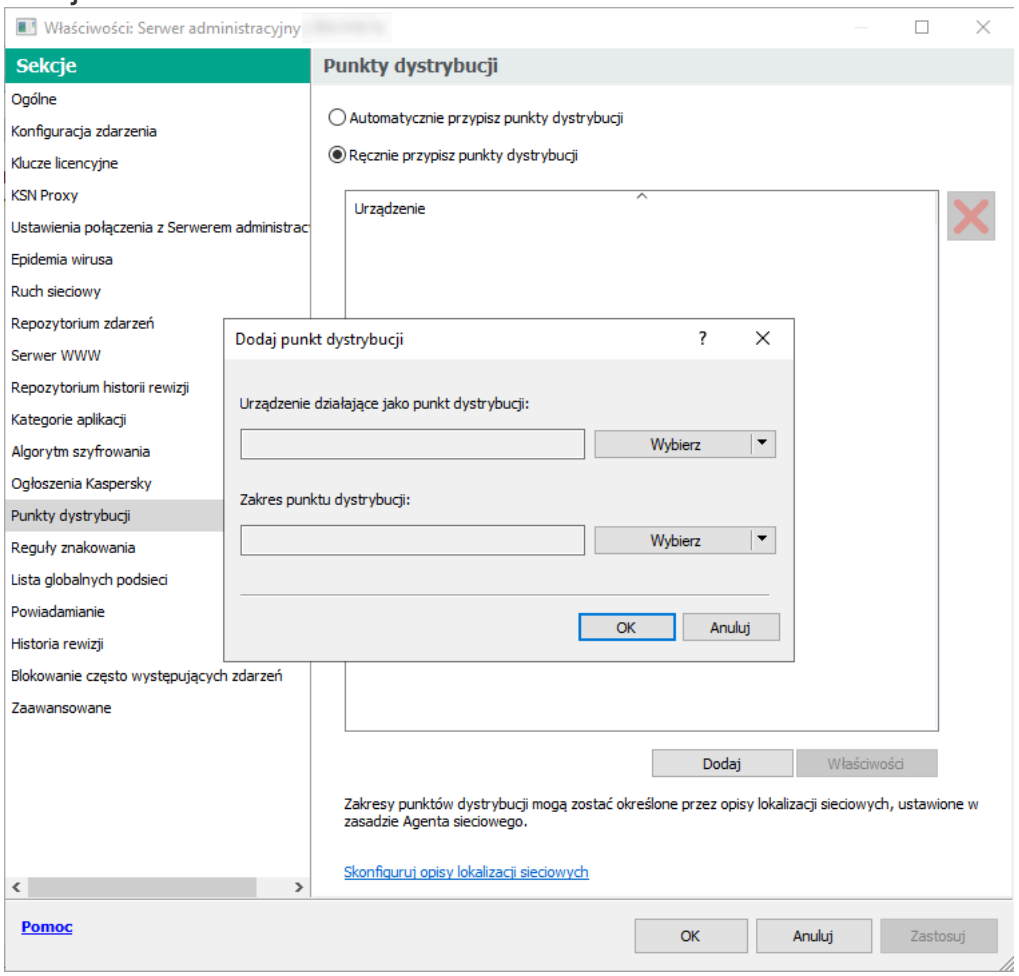
Na przykład: Laptop znajduje się w grupie administracyjnej **Office 1**, a następnie zostaje fizycznie przeniesiony do biura, które odpowiada grupie administracyjnej **Office 2**. Po przeniesieniu laptopa, Agent sieciowy spróbuje połączyć się z punktami dystrybucji przypisanymi do grupy **Office 1**, ale te punkty dystrybucji są niedostępne. Następnie Agent sieciowy próbuje połączyć się z punktami dystrybucji, które zostały przypisane do **Głównej grupy dla biur**. Ponieważ zdalne biura są odizolowane od siebie, próby nawiązania połączenia z punktami dystrybucji przypisanymi do grupy administracyjnej **Główna grupa dla biur** zakończą się pomyślnie tylko wtedy, gdy Agent sieciowy spróbuje połączyć się z punktami dystrybucji w grupie **Office 2**. Oznacza to, że laptop pozostanie w grupie administracyjnej, która odpowiada pierwszemu biuru, ale będzie korzystał z punktu dystrybucji biura, w którym aktualnie się znajduje.

Wskazywanie zarządzanego urządzenia jako punktu dystrybucji

Możesz ręcznie wskazać urządzenie jako punkt dystrybucji dla grupy administracyjnej i skonfigurować go jako bramę połączenia w Konsoli administracyjnej.

W celu wskazania urządzenia jako punktu dystrybucji dla grupy administracyjnej:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.
4. W prawej części okna wybierz opcję **Ręcznie przypisz punkty dystrybucji**.
5. Kliknij przycisk **Dodaj**.



Przypisz punkt dystrybucji ręcznie

Zostanie otwarte okno **Dodaj punkt dystrybucji**.

6. W oknie **Dodaj punkt dystrybucji** wykonaj następujące działania:

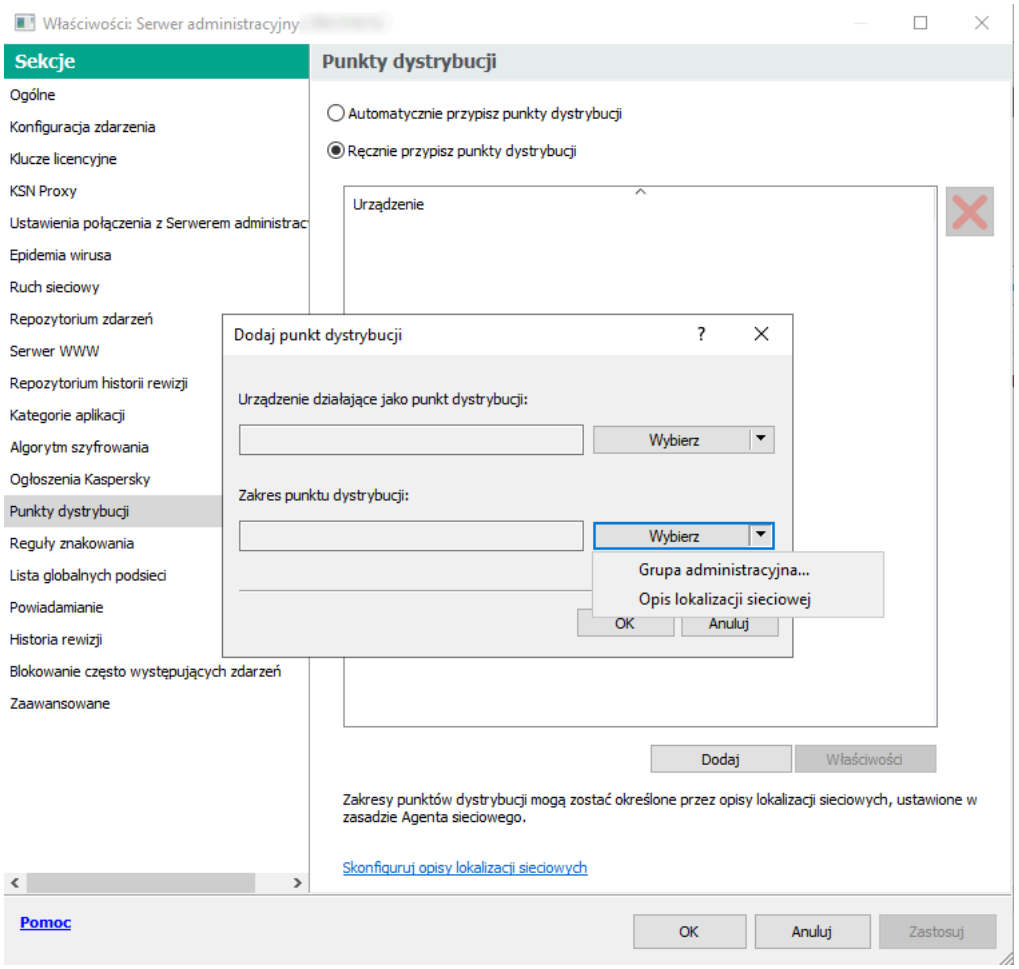
   a. Pod sekcją **Urządzenie**, które ma działać jako punkt dystrybucji kliknij strzałkę (▾) skierowaną w dół obok przycisku **Wybierz** i wybierz opcję **Dodaj urządzenie z grupy**.

   b. W otwartym oknie **Wybierz urządzenia** wybierz urządzenie, które będzie pełniło rolę punktu dystrybucji.

c. Pod sekcją **Obszar punktu dystrybucji** kliknij strzałkę skierowaną w dół (▾) obok przycisku **Wybierz**.

d. Wskaż określone urządzenia, na które punkt dystrybucji roześle uaktualnienia. Możesz określić opis grupy administracyjnej lub lokalizacji sieciowej.

e. Kliknij **OK**, aby zamknąć okno **Dodaj punkt dystrybucji**.



Wybieranie zakresu punktu dystrybucji

Dodany punkt dystrybucji będzie wyświetlany na liście punktów dystrybucji, w sekcji **Punkty dystrybucji**.

Pierwsze urządzenie z zainstalowanym Agentem sieciowym, które nawiąże połączenie z wirtualnym Serwerem administracyjnym, zostanie automatycznie wskazane jako punkt dystrybucji i skonfigurowane jako brama połączenia.

Podłączanie urządzenia Linux jako bramy połączenia w strefie zdemilitaryzowanej

W celu podłączenia urządzenia Linux jako bramy połączenia w strefie zdemilitaryzowanej (DMZ):

1. Pobierz i zainstaluj Agenta sieciowego na urządzeniu Linux.

2. Uruchom skrypt poinstalacyjny i postępuj zgodnie z instrukcjami kreatora, aby ustawić konfigurację środowiska lokalnego. W wierszu polecenia uruchom następujące polecenie:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Na kroku z pytaniem o tryb Agenta sieciowego wybierz opcję **Użyj jako bramy połączenia**.

4. W Konsoli administracyjnej opartej na MMC, w menu kontekstowym Serwera administracyjnego wybierz **Właściwości**.

5. W otwartym oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.

6. W otwartym oknie **Punktów dystrybucji**, w prawej części okna:

   a. Wybierz opcję **Ręcznie przypisz punkty dystrybucji**.

   b. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Dodaj punkt dystrybucji**.

7. W oknie **Dodaj punkt dystrybucji** wykonaj następujące działania:

   a. W obszarze **Urządzenie**, które ma działać jako punkt dystrybucji, kliknij strzałkę w dół (▾) na przycisku podzielonym **Wybierz**, a następnie wybierz opcję **Dodaj bramę połączenia w DMZ na podstawie adresu**.

   b. Pod sekcją **Obszar punktu dystrybucji** kliknij strzałkę skierowaną w dół (▾) obok przycisku **Wybierz**.

   c. Wskaż określone urządzenia, na które punkt dystrybucji roześle uaktualnienia. Możesz określić grupę administracyjną.

   d. Kliknij **OK**, aby zamknąć okno **Dodaj punkt dystrybucji**.

8. Dodany punkt dystrybucji będzie wyświetlany na liście punktów dystrybucji, w sekcji **Punkty dystrybucji**.

9. Uruchom narzędzie klnagchk, aby sprawdzić, czy połączenie z Kaspersky Security Center zostało pomyślnie skonfigurowane. W wierszu polecenia uruchom:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

10. W menu głównym przejdź do Kaspersky Security Center i wykryj urządzenie.

11. W otwartym oknie kliknij przycisk <Nazwa urządzenia>.

12. Z listy rozwijalnej wybierz odnośnik **Przenieś do grupy**.

13. W otwartym oknie **Wybierz grupy** kliknij odnośnik **Punktów dystrybucji**.

14. Kliknij **OK**.

15. Uruchom ponownie usługę Agenta sieciowego na kliencie Linux, wykonując następujące polecenie w wierszu poleceń:
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
    ```

Podłączanie urządzenia Linux jako bramy połączenia w strefie zdemilitaryzowanej zostało zakończone.

Następnie możesz podłączyć urządzenie z systemem Linux do Serwera administracyjnego poprzez skonfigurowaną bramę połączenia. Postępuj zgodnie z tymi procedurami dopiero po ukończeniu głównego scenariusza instalacji.

Podłączanie urządzenia Linux do Serwera administracyjnego za pośrednictwem bramy połączenia

Brama połączenia umożliwia podłączenie urządzeń klienckich ze strefy zdemilitaryzowanej (DMZ) do Serwera administracyjnego. Urządzenia z systemem Windows i Linux mogą działać jako brama połączenia. Po podłączeniu i skonfigurowaniu bramy połączenia możesz użyć tej bramy do połączenia urządzenia z systemem Linux z Serwerem administracyjnym. Postępuj zgodnie z poniższą procedurą dopiero po ukończeniu głównego scenariusza instalacji.

Aby podłączyć urządzenie Linux do Serwera administracyjnego za pośrednictwem bramy połączenia, wykonaj następujące czynności na tym urządzeniu:

1. Pobierz i zainstaluj Agenta sieciowego na urządzeniu Linux.
2. Uruchom skrypt poinstalacyjny Agenta sieciowego, wykonując następujące polecenie w wierszu poleceń:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```
3. W kroku z pytaniem o tryb Agenta sieciowego wybierz opcję **Połącz z Serwerem, korzystając z bramy połączenia** i wprowadź adres bramy połączenia.
4. Sprawdź połączenie z Kaspersky Security Center i bramę połączenia, używając następującego polecenia w wierszu polecenia:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   Adres bramy połączenia jest wyświetlany w danych wyjściowych.

Podłączanie urządzenia Linux do Serwera administracyjnego za pośrednictwem bramy połączenia zostało zakończone. Tego urządzenia można używać do dystrybucji aktualizacji, do zdalnej instalacji aplikacji oraz do pobierania informacji o urządzeniach sieciowych.

Dodawanie bramy połączenia w strefie DMZ jako punktu dystrybucji

Brama połączenia oczekuje na połączenia z Serwerem administracyjnym bardziej niż nawiązuje te połączenia z Serwerem administracyjnym. To oznacza, że od razu po zainstalowaniu bramy połączenia na urządzeniu w DMZ, Serwer administracyjny nie wyświetla urządzenia wśród zarządzanych urządzeń. Dlatego też należy przeprowadzić specjalną procedurę w celu zapewnienia, że Serwer administracyjny zainicjuje połączenie z bramą połączenia.

W celu dodania urządzenia z bramą połączenia jako punktu dystrybucji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.
4. W prawej części okna wybierz opcję **Ręcznie przypisz punkty dystrybucji**.
5. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Dodaj punkt dystrybucji**.

6. W oknie **Dodaj punkt dystrybucji** wykonaj następujące działania:

   a. W obszarze **Urządzenie, które ma działać jako punkt dystrybucji** kliknij strzałkę w dół (▾) na przycisku podzielonym **Wybierz**, a następnie wybierz opcję **Dodaj bramę połączenia w DMZ na podstawie adresu**.

   b. W otwartym oknie **Wprowadź adres bramy połączenia** wprowadź adres IP bramy połączenia (lub wprowadź nazwę, jeśli brama połączenia jest dostępna według nazwy).

   c. Pod sekcją **Obszar punktu dystrybucji** kliknij strzałkę skierowaną w dół (▾) obok przycisku **Wybierz**.

   d. Wskaż określone urządzenia, na które punkt dystrybucji roześle uaktualnienia. Możesz określić opis grupy administracyjnej lub lokalizacji sieciowej.

      Zalecamy posiadanie oddzielnej grupy dla zewnętrznych zarządzanych urządzeń.

Po wykonaniu tych działań, lista punktów dystrybucji zawiera nowy wpis o nazwie **Tymczasowy wpis dla bramy połączenia**.

Serwer administracyjny prawie natychmiast próbuje nawiązać połączenie z bramą połączenia pod podanym adresem. Jeśli się powiedzie, nazwa wpisu zmieni się na nazwę urządzenia bramy połączenia. Ten proces trwa do pięciu minut.

Podczas gdy tymczasowy wpis dla bramy połączenia jest konwertowany na nazwany wpis, brama połączenia pojawia się również w grupie **Nieprzypisane urządzenia**.

Aby dodać bramę połączenia do wcześniej skonfigurowanej sieci, zainstaluj ponownie Agenta sieciowego na urządzeniach, które chcesz połączyć z nowo dodaną bramą połączenia.

Automatyczne przypisywanie punktów dystrybucji

Zalecane jest automatyczne przypisywanie punktów dystrybucji. Kaspersky Security Center sam wybierze urządzenia, które mają być punktami dystrybucji.

Aby automatycznie przypisać punkty dystrybucji:

1. Otwórz okno główne aplikacji.
2. W drzewie konsoli należy wybrać węzeł z nazwą Serwera administracyjnego, dla którego chcesz automatycznie przypisać punkty dystrybucji.
3. W menu kontekstowym Serwera administracyjnego kliknij **Właściwości**.
4. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Punkty dystrybucji**.
5. W prawej części okna wybierz opcję **Automatycznie przypisz punkty dystrybucji**.

   Jeśli włączone jest automatyczne wskazywanie urządzeń jako punktów dystrybucji, nie można ręcznie skonfigurować punktów dystrybucji, ani też zmodyfikować listy punktów dystrybucji.

6. Kliknij **OK**.

Serwer administracyjny automatycznie przypisze i skonfiguruje punkty dystrybucji.

Informacje o lokalnej instalacji Agenta sieciowego na urządzeniu określonym jako punkt dystrybucji

Aby umożliwić urządzeniu wybranemu na punkt dystrybucji bezpośrednią komunikację z wirtualnym Serwerem administracyjnym tak, aby służył jako brama połączenia, Agent sieciowy musi zostać zainstalowany lokalnie na tym urządzeniu.

Procedura lokalnej instalacji Agenta sieciowego na urządzeniu określonym jako punkt dystrybucji jest identyczna jak lokalna instalacja Agenta sieciowego na dowolnym urządzeniu w sieci.

Dla urządzenia wybranego jako punkt dystrybucji muszą zostać spełnione następujące warunki:

- Podczas lokalnej instalacji Agenta sieciowego określ adres wirtualnego Serwera administracyjnego zarządzającego urządzeniem w polu **Adres serwera**, w oknie **Serwer administracyjny** kreatora instalacji. Można użyć adresu IP lub nazwy urządzenia w sieci Windows.

  Dla adresu Serwera wirtualnego używany jest następujący format: <Pełny adres fizycznego Serwera administracyjnego, do którego należy wirtualny Serwer>/<Nazwa wirtualnego Serwera administracyjnego>.

- Aby mógł on pełnić rolę bramy połączenia, otwórz wszystkie porty urządzenia, które są niezbędne dla komunikacji z Serwerem administracyjnym.

Po zainstalowaniu na tym urządzeniu Agenta sieciowego z określonymi ustawieniami, Kaspersky Security Center automatycznie wykonuje następujące akcje:

- Dodaje to urządzenie do grupy **Zarządzane urządzenia** wirtualnego Serwera administracyjnego.

- Wskazuje to urządzenie jako punkt dystrybucji dla grupy **Zarządzane urządzenia** wirtualnego Serwera administracyjnego.

Konieczne i wystarczające jest przeprowadzenie lokalnej instalacji Agenta sieciowego na urządzeniu wskazanym jako punkt dystrybucji dla grupy **Zarządzane urządzenia** w sieci organizacji. Możesz zainstalować Agenta sieciowego zdalnie na urządzeniach służących jako punkty dystrybucji w zagnieżdżonych grupach administracyjnych. W tym celu użyj punkt dystrybucji grupy **Zarządzane urządzenia** jako bramy połączenia.

Informacje o używaniu punktu dystrybucji jako bramy połączenia

Jeśli Serwer administracyjny znajduje się poza strefą zdemilitaryzowaną (demilitarized zone, DMZ), Agenty sieciowe z tej strefy nie mogą nawiązać połączenia z Serwerem administracyjnym.

Podczas łączenia Serwera administracyjnego z Agentami sieciowymi możesz użyć punktu dystrybucji jako bramy połączenia. Punkt dystrybucji otworzy port dla Serwera administracyjnego w celu nawiązania połączenia. Po uruchomieniu Serwera administracyjnego połączy się on z punktem dystrybucji i utrzyma to połączenie podczas całej sesji.

Po otrzymaniu sygnału z Serwera administracyjnego, punkt dystrybucji wyśle sygnał UDP do Agentów sieciowych w celu zezwolenia na połączenie z Serwerem administracyjnym. Po odebraniu sygnału przez Agenty sieciowe, połączą się one z punktem dystrybucji, który będzie wymieniał informacje między Agentami sieciowymi a Serwerem administracyjnym. Wymiana informacji może odbywać się za pośrednictwem sieci IPv4 lub IPv6.

Zalecane jest użycie jako bramy połączenia specjalnie przypisanego urządzenia oraz przydzielenie do bramy połączenia maksymalnie 10 000 urządzeń klienckich (w tym urządzeń mobilnych).

Aby dodać bramę połączenia do wcześniej skonfigurowanej sieci:

1. Zainstaluj Agenta sieciowego w trybie bramy połączenia.
2. Ponownie zainstaluj Agenta sieciowego na urządzeniach, które chcesz połączyć z nowo dodaną bramą połączenia.

Dodawanie zakresów adresów IP do listy zakresów przeszukiwanych przez punkt dystrybucji

Możesz dodać zakresy IP do listy skanowanych zakresów punktu dystrybucji.

Aby dodać zakres IP do listy skanowanych zakresów:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z otwartego menu kontekstowego węzła wybierz **Właściwości**.
3. W otwartym oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.
4. Na liście wybierz żądany punkt dystrybucji, a następnie kliknij **Właściwości**.
5. W otwartym oknie właściwości punktów dystrybucji, w lewym panelu **Sekcje** wybierz **Wykrywanie urządzeń** → **Zakresy IP**.
6. Zaznacz pole **Włącz przeszukiwanie zakresów**.
7. Kliknij przycisk **Dodaj**.

   Przycisk **Dodaj** jest aktywny tylko wtedy, gdy zaznaczysz pole **Włącz przeszukiwanie zakresów**.

   Zostanie otwarte okno **Zakres IP**.
8. W oknie **Zakres IP** wprowadź nazwę nowego zakresu IP (domyślna nazwa to Nowy zakres).
9. Kliknij przycisk **Dodaj**.
10. Wykonaj jedną z poniższych czynności:
    - Określ zakres IP, używając początkowego i końcowego adresu IP.
    - Określ zakres IP, używając adresu oraz maski podsieci.
    - Kliknij **Przeglądaj** i dodaj podsieć z globalnej listy podsieci.
11. Kliknij **OK**.
12. Kliknij **OK**, aby dodać nowy zakres z określoną nazwą.

    Nowy zakres pojawi się na liście skanowanych zakresów.

Używanie punktu dystrybucji jako serwera push

W Kaspersky Security Center punkt dystrybucji może działać jako serwer push dla urządzeń zarządzanych za pośrednictwem protokołu mobilnego oraz zarządzanych za pośrednictwem agenta sieciowego. Na przykład, serwer push musi być włączony, jeśli chcesz mieć możliwość wymuszenia synchronizacji urządzeń KasperskyOS z Serwerem administracyjnym. Serwer push posiada ten sam obszar zarządzanych urządzeń jako punkt dystrybucji, na którym włączono serwer push. Jeśli posiadasz kilka punktów dystrybucji przypisanych dla tej samej grupy administracyjnej, możesz włączyć serwer push na każdym punkcie dystrybucji. W tym przypadku Serwer administracyjny rozkłada obciążenie między punkty dystrybucji.

Serwer push obsługuje do 50 000 jednoczesnych połączeń.

Punktów dystrybucji można używać jako serwerów push, aby zapewnić ciągłą łączność między zarządzanym urządzeniem a Serwerem administracyjnym. W przypadku niektórych operacji, takich jak uruchamianie i zatrzymywanie zadań lokalnych, odbieranie statystyk dla zarządzanej aplikacji lub tworzenie tunelu, wymagana jest ciągła łączność. Jeśli używasz punktu dystrybucji jako serwera push, nie musisz używać opcji **Nie odłączaj od Serwera administracyjnego** na zarządzanych urządzeniach lub wysyłaj pakiety do portu UDP Agenta sieciowego.

W celu użycia punktu dystrybucji jako serwera push:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z otwartego menu kontekstowego węzła wybierz **Właściwości**.
3. W otwartym oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.
4. Na liście wybierz żądany punkt dystrybucji, a następnie kliknij **Właściwości**.
5. W otwartym oknie właściwości punktu dystrybucji, w sekcji **Ogólne** lewego panelu **Sekcje** wybierz opcję **Użyj tego punktu dystrybucji jako serwer push**.
6. Określ numer portu serwera push, czyli portu na punkcie dystrybucji, którego urządzenia klienckie będą używać do nawiązywania połączeń.

   Domyślnie wykorzystywany jest port 13295.
7. Kliknij przycisk **OK**, aby zamknąć okno właściwości punktu dystrybucji.
8. Otwórz okno właściwości zasady Agenta sieciowego.
9. W sekcji **Łączność** przejdź do podsekcji **Sieć**.

10. W podsekcji **Sieć** wybierz opcję **Użyj punktu dystrybucji, aby wymusić połączenie z Serwerem administracyjnym**.

11. Kliknij przycisk **OK**, aby zamknąć okno.

    Punkt dystrybucji zacznie działać jako serwer push. Teraz może wysyłać powiadomienia push na urządzenia klienckie.

Jeśli zarządzasz urządzeniami z zainstalowanym KasperskyOS lub planujesz to zrobić, musisz użyć punktu dystrybucji jako serwera push. Możesz także użyć punktu dystrybucji jako serwera push, jeśli chcesz wysłać powiadomienia push na urządzenia klienckie.

Inne podstawowe prace

Ta sekcja zawiera zalecenia dotyczące codziennej pracy z Kaspersky Security Center.

Zarządzanie Serwerami administracyjnymi

Ta sekcja zawiera informacje na temat pracy z Serwerami administracyjnymi i ich konfiguracji.

Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego Serwera administracyjnego

Możesz dodać Serwer administracyjny jako podrzędny Serwer administracyjny, a tym samym utworzyć hierarchię „główny/podrzędny". Dodanie podrzędnego Serwera administracyjnego jest możliwe niezależnie od tego, czy Serwer administracyjny, którego zamierzasz używać jako podrzędny, jest dostępny do podłączenia poprzez Konsolę administracyjną.

Podczas łączenia dwóch Serwerów administracyjnych w hierarchię upewnij się, że port 13291 jest dostępny na obu Serwerach administracyjnych. Port 13291 jest wymagany do odbierania połączeń od Konsoli administracyjnej do Serwera administracyjnego.

Podłączanie Serwera administracyjnego jako podrzędnego w odniesieniu do głównego Serwera administracyjnego

Możesz dodać Serwer administracyjny jako podrzędny, podłączając go do głównego Serwera administracyjnego poprzez port 13000. Potrzebne jest urządzenie z zainstalowaną Konsolą administracyjną, z której można uzyskać dostęp do portów TCP o numerze 13291 na obu Serwerach administracyjnych: domniemany główny Serwer administracyjny i domniemany podrzędny Serwer administracyjny.

W celu dodania podrzędnego Serwera administracyjnego, który jest dostępny dla połączenia poprzez Konsolę administracyjną:

1. Upewnij się, że port 13000 przyszłego głównego Serwera administracyjnego jest dostępny do odbierania połączeń od podrzędnych Serwerów administracyjnych.

2. Użyj Konsoli administracyjnej do nawiązywania połączenia z domniemanym głównym Serwerem administracyjnym.

3. Wybierz grupę administracyjną, do której chcesz dodać podrzędny Serwer administracyjny.

4. W obszarze roboczym węzła **Serwery administracyjne** wybranej grupy kliknij odnośnik **Dodaj podrzędny Serwer administracyjny**.

   Zostanie uruchomiony Kreator dodawania podrzędnego Serwera administracyjnego.

5. W pierwszym kroku kreatora (wprowadzanie adresu Serwera administracyjnego dodawanego do grupy) wprowadź nazwę sieci domniemanego podrzędnego Serwera administracyjnego.

6. Postępuj zgodnie z instrukcjami kreatora.

Zostanie utworzona hierarchia „główny/podrzędny". Główny Serwer administracyjny będzie odbierał połączenie od podrzędnego Serwera administracyjnego.

Jeśli nie posiadasz urządzenia z zainstalowaną Konsolą administracyjną, z której można uzyskać dostęp do portów TCP o numerze 13291 na obu Serwerach administracyjnych (jeśli, na przykład, domniemany podrzędny Serwer administracyjny znajduje się w zdalnym biurze, a administrator systemu z tego biura nie może otworzyć dostępu do Internetu dla portu 13291 ze względów bezpieczeństwa), nadal będziesz mógł dodać podrzędny Serwer administracyjny.

W celu dodania podrzędnego Serwera administracyjnego, który nie jest dostępny dla połączenia poprzez Konsolę administracyjną:

1. Upewnij się, że port 13000 domniemanego głównego Serwera administracyjnego jest dostępny dla połączenia z podrzędnych Serwerów administracyjnych.

2. Zapisz plik certyfikatu domniemanego głównego Serwera administracyjnego na urządzeniu zewnętrznym, takim jak dysk flash, lub wyślij go do administratora systemu w zdalnym biurze, w którym znajduje się Serwer administracyjny.

   Plik certyfikatu Serwera administracyjnego znajduje się na tym samym Serwerze administracyjnym, w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. Zapisz plik certyfikatu domniemanego podrzędnego Serwera administracyjnego na urządzeniu zewnętrznym, takim jak dysk flash. Jeśli domniemany podrzędny Serwer administracyjny znajduje się w zdalnym biurze, skontaktuj się z administratorem systemu z tego biura, aby poprosić go/ją o przesłanie certyfikatu.

   Plik certyfikatu Serwera administracyjnego znajduje się na tym samym Serwerze administracyjnym, w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. Użyj Konsoli administracyjnej do nawiązywania połączenia z domniemanym głównym Serwerem administracyjnym.

5. Wybierz grupę administracyjną, do której chcesz dodać podrzędny Serwer administracyjny.

6. W obszarze roboczym węzła **Serwery administracyjne** kliknij odnośnik **Dodaj podrzędny Serwer administracyjny**.

   Zostanie uruchomiony Kreator dodawania podrzędnego Serwera administracyjnego.

7. W pierwszym kroku kreatora (wprowadzanie adresu) pozostaw pole **Adres podrzędnego Serwera administracyjnego (opcjonalnie)** puste.

8. W oknie **Plik certyfikatu podrzędnego Serwera administracyjnego** kliknij przycisk **Przeglądaj** i wybierz plik certyfikatu podrzędnego Serwera administracyjnego, który zapisałeś.

9. Po zakończeniu pracy kreatora użyj innej instancji Konsoli administracyjnej do nawiązania połączenia z domniemanym podrzędnym Serwerem administracyjnym. Jeśli ten Serwer administracyjny znajduje się w zdalnym biurze, skontaktuj się z administratorem systemu z tego biura, aby poprosić go/ją o połączenie z domniemanym podrzędnym Serwerem administracyjnym i wykonaj dalsze kroki.

10. Z menu kontekstowego węzła **Serwer administracyjny** wybierz **Właściwości**.

11. We właściwościach Serwera administracyjnego przejdź do sekcji **Zaawansowane**, a następnie do podsekcji **Hierarchia Serwerów administracyjnych**.

12. Zaznacz pole **Ten Serwer administracyjny jest podrzędnym w hierarchii**.

    Pola wejściowe stają się dostępne do wprowadzenia i edycji danych.

13. W polu **Adres głównego Serwera administracyjnego** wprowadź nazwę sieci domniemanego głównego Serwera administracyjnego.

14. Wybierz wcześniej zapisany plik z certyfikatem domniemanego głównego Serwera administracyjnego, klikając przycisk **Przeglądaj**.

15. Kliknij **OK**.

Zostanie utworzona hierarchia „główny/podrzędny". Możesz nawiązać połączenie z podrzędnym Serwerem administracyjnym poprzez Konsolę administracyjną. Główny Serwer administracyjny będzie odbierał połączenie od podrzędnego Serwera administracyjnego.

Nawiązywanie połączenia między głównym Serwerem administracyjnym a podrzędnym Serwerem administracyjnym

Możesz dodać nowy Serwer administracyjny jako podrzędny, aby główny Serwer administracyjny nawiązywał połączenie z podrzędnym Serwerem administracyjnym poprzez port 13000. Jest to zalecane w sytuacjach, gdy, na przykład, umieszczasz podrzędny Serwer administracyjny w strefie DMZ.

Potrzebne jest urządzenie z zainstalowaną Konsolą administracyjną, z której można uzyskać dostęp do portów TCP o numerze 13291 na obu Serwerach administracyjnych: domniemany główny Serwer administracyjny i domniemany podrzędny Serwer administracyjny.

W celu dodania nowego Serwera administracyjnego jako podrzędnego i podłączenia go do głównego Serwera administracyjnego poprzez port 13000:

1. Upewnij się, że port 13000 domniemanego podrzędnego Serwera administracyjnego jest dostępny do odbierania połączeń z głównego Serwera administracyjnego.

2. Użyj Konsoli administracyjnej do nawiązywania połączenia z domniemanym głównym Serwerem administracyjnym.

3. Wybierz grupę administracyjną, do której chcesz dodać podrzędny Serwer administracyjny.

4. W obszarze roboczym węzła **Serwery administracyjne** odpowiedniej grupy administracyjnej kliknij odnośnik **Dodaj podrzędny Serwer administracyjny**.

   Zostanie uruchomiony Kreator dodawania podrzędnego Serwera administracyjnego.

5. W pierwszym kroku kreatora (wprowadzanie adresu Serwera administracyjnego dodawanego do grupy) wprowadź nazwę sieci domniemanego podrzędnego Serwera administracyjnego i zaznacz pole **Połącz główny Serwer administracyjny z podrzędnym Serwerem administracyjnym w DMZ**.

6. Jeśli nawiązujesz połączenie z domniemanym podrzędnym Serwerem administracyjnym przy użyciu serwera proxy, w pierwszym kroku kreatora zaznacz pole **Użyj serwera proxy** i określ ustawienia połączenia.

7. Postępuj zgodnie z instrukcjami kreatora.

Hierarchia Serwerów administracyjnych zostanie utworzona. Podrzędny Serwer administracyjny będzie odbierał połączenie od głównego Serwera administracyjnego.

Nawiązywanie połączenia z Serwerem administracyjnym i przełączanie pomiędzy Serwerami administracyjnymi

Po uruchomieniu programu Kaspersky Security Center próbuje on nawiązać połączenie z Serwerem administracyjnym. Jeżeli w sieci jest dostępnych kilka Serwerów administracyjnych, aplikacja będzie próbowała nawiązać połączenie z tym Serwerem, z którym była połączona podczas poprzedniej sesji Kaspersky Security Center.

Jeżeli aplikacja jest uruchamiana po raz pierwszy po jej zainstalowaniu, próbuje nawiązać połączenie z Serwerem administracyjnym określonym podczas instalacji Kaspersky Security Center.

Po nawiązaniu połączenia z Serwerem administracyjnym, drzewo folderów tego Serwera jest wyświetlane w drzewie konsoli.

Jeśli do drzewa konsoli było dodanych kilka Serwerów administracyjnych, możesz się pomiędzy nimi przełączać.

Konsola administracyjna jest wymagana do pracy z każdym Serwerem administracyjnym. Przed pierwszym połączeniem z nowym Serwerem administracyjnym upewnij się, że port 13291, który odbiera połączenia od Konsoli administracyjnej, jest otwarty, a także wszystkie pozostałe porty wymagane do komunikacji między Serwerem administracyjnym a innymi komponentami Kaspersky Security Center.

W celu przełączenia się na inny Serwer administracyjny:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.

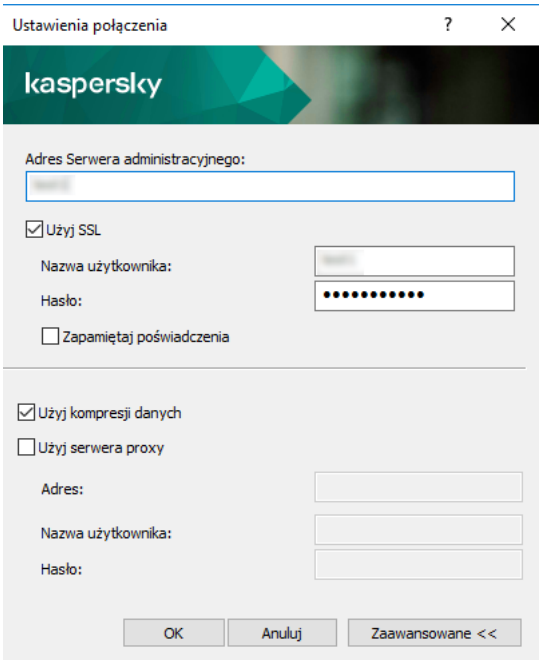
2. Z menu kontekstowego węzła wybierz **Połącz z Serwerem administracyjnym**.

3. W otwartym oknie **Ustawienia połączenia**, w polu **Adres Serwera administracyjnego** określ nazwę Serwera administracyjnego, z którym chcesz nawiązać połączenie. Jako nazwę Serwera administracyjnego można określić adres IP lub nazwę urządzenia w sieci Windows. Kliknięcie przycisku **Zaawansowane** umożliwi skonfigurowanie ustawień połączenia z Serwerem administracyjnym (patrz rysunek poniżej).

   W celu nawiązania połączenia z Serwerem administracyjnym poprzez port inny niż domyślny, w polu **Adres Serwera administracyjnego** należy wprowadzić wartość w formacie <Nazwa Serwera administracyjnego>:<Numer portu>.

   Aby połączyć się z wirtualnym Serwerem administracyjnym, wprowadź wartość w polu **Adres Serwera administracyjnego** w formacie <Adres Serwera administracyjnego>/<nazwa serwera wirtualnego>.

Użytkownicy, którzy nie posiadają uprawnień do **Odczytu**, nie będą mieli dostępu do Serwera administracyjnego.



Nawiązywanie połączenia z Serwerem administracyjnym

4. Aby zakończyć przełączanie pomiędzy Serwerami, kliknij przycisk **OK**.

   Po podłączeniu Serwera administracyjnego, w drzewie konsoli zaktualizowane zostanie drzewo folderów odpowiedniego węzła.

Uprawnienia dostępu do Serwera administracyjnego i jego obiektów

Podczas instalacji Kaspersky Security Center automatycznie tworzone są grupy **KLAdmins** i **KLOperators**. Grupom tym nadawane są uprawnienia do nawiązywania połączeń z Serwerem administracyjnym i do przetwarzania jego obiektów.

W zależności od typu konta użytego przy instalacji Kaspersky Security Center, grupy **KLAdmins** i **KLOperators** są tworzone w następujący sposób:

- Jeśli aplikacja jest instalowana z poziomu konta użytkownika znajdującego się w domenie, grupy są tworzone na Serwerze administracyjnym i w domenie zawierającej Serwer administracyjny.
- Jeśli aplikacja jest instalowana z poziomu konta systemowego, grupy są tworzone jedynie na Serwerze administracyjnym.

Możesz przeglądać grupy **KLAdmins** i **KLOperators** oraz modyfikować uprawnienia dostępu użytkowników należących do grup **KLAdmins** i **KLOperators**, korzystając ze standardowych narzędzi administracyjnych systemu operacyjnego.

Grupa **KLAdmins** ma wszystkie uprawnienia dostępu, a grupa **KLOperators** ma jedynie uprawnienia Odczytu i Wykonywania. Uprawnienia nadane grupie **KLAdmins** są zablokowane.

Użytkownicy należący do grupy **KLAdmins** są nazywani *administratorami Kaspersky Security Center*, użytkownicy z grupy **KLOperators** są zwani *operatorami Kaspersky Security Center*.

Oprócz użytkowników z grupy **KLAdmins**, uprawnienia administratora Kaspersky Security Center są nadawane lokalnym administratorom urządzeń, na których zainstalowano Serwer administracyjny.

Możesz wykluczyć lokalnych administratorów z listy użytkowników, którzy posiadają uprawnienia administratora Kaspersky Security Center.

Wszystkie działania rozpoczęte przez administratorów Kaspersky Security Center zostaną wykonane przy użyciu uprawnień konta Serwera administracyjnego.

Dla każdego Serwera administracyjnego w sieci można utworzyć indywidualną grupę **KLAdmins**; będzie ona posiadać uprawnienia do pracy tylko z tym Serwerem administracyjnym.

Jeśli urządzenia należące do tej samej domeny znajdują się w grupach administracyjnych różnych Serwerów administracyjnych, wówczas administrator domeny jest administratorem Kaspersky Security Center dla wszystkich grup. Grupa **KLAdmins** jest wspólna dla tych grup administracyjnych; tworzona jest podczas instalacji pierwszego Serwera administracyjnego. Wszystkie działania podejmowane przez administratora Kaspersky Security Center są wykonywane przy pomocy uprawnień dostępu Serwera administracyjnego, dla którego rozpoczęto te działania.

Po zainstalowaniu aplikacji, administrator Kaspersky Security Center może:

- Modyfikować uprawnienia nadane grupom **KLOperators**.
- Nadawać uprawnienia dostępu do funkcji Kaspersky Security Center innym grupom bezpieczeństwa i pojedynczym użytkownikom zarejestrowanym na stacji roboczej administratora.
- Przydzielać uprawnienia dostępu każdej grupie administracyjnej.

Administrator Kaspersky Security Center może przydzielić uprawnienia dostępu do każdej grupy administracyjnej lub do innych obiektów Serwera administracyjnego w sekcji **Zabezpieczenia**, w oknie właściwości wybranego obiektu.

Możesz śledzić aktywność użytkowników przy pomocy wpisów dotyczących zdarzeń, które wystąpiły w trakcie pracy Serwera administracyjnego. Wpisy dotyczące zdarzeń są wyświetlane w węźle **Serwer administracyjny**, na zakładce **Zdarzenia**. Priorytetem tych zdarzeń jest **Informacja o zdarzeniach**, a typy zdarzeń rozpoczynają się od "**Audyt**".

Warunki połączenia z Serwerem administracyjnym przez internet

Jeżeli Serwer administracyjny jest zdalny (znajduje się poza siecią firmową), urządzenia klienckie mogą łączyć się z nim przez internet.

Aby urządzenia klienckie łączyły się z Serwerem administracyjnym przez Internet, muszą być spełnione następujące warunki:

- Zdalny Serwer administracyjny musi posiadać zewnętrzny adres IP, a port dla ruchu przychodzącego o numerze 13000 musi pozostać otwarty (dla połączenia z Agentami sieciowymi). Zalecane jest także otwarcie portu UDP o numerze 13000 (do odbierania powiadomień o zamknięciu urządzeń).
- Agenty sieciowe powinny zostać zainstalowane na urządzeniach.

- Podczas instalacji Agenta sieciowego na urządzeniach powinieneś określić zewnętrzny adres IP zdalnego Serwera administracyjnego. Jeżeli do instalacji wykorzystywany jest pakiet instalacyjny, zewnętrzny adres IP jest określany ręcznie we właściwościach tego pakietu instalacyjnego, na zakładce **Ustawienia**.

- Aby użyć zdalnego Serwera administracyjnego do zarządzania aplikacjami i zadaniami dla urządzenia, w oknie właściwości tego urządzenia, w sekcji **Ogólne** zaznacz pole **Nie odłączaj od Serwera administracyjnego**. Po zaznaczeniu tego pola, należy zaczekać, aż Serwer administracyjny zsynchronizuje się ze zdalnym urządzeniem. Liczba urządzeń klienckich mających stałe połączenie z Serwerem administracyjnym nie może przekraczać 300.

Aby zwiększyć wydajność zadań zainicjowanych przez zdalny Serwer administracyjny, możesz otworzyć na urządzeniu port o numerze 15000. W tym przypadku, aby uruchomić zadanie, Serwer administracyjny wysyła specjalny pakiet do Agenta sieciowego przez port 15000, bez oczekiwania na zakończenie synchronizacji z urządzeniem.

Nawiązywanie szyfrowanego połączenia z Serwerem administracyjnym

Wymiana danych między urządzeniami klienckimi a Serwerem administracyjnym, jak również połączenia Konsoli administracyjnej z Serwerem administracyjnym, może być przeprowadzana z użyciem protokołu TLS (Transport Layer Security). Protokół TLS może identyfikować współdziałające strony, szyfrować przesyłane dane oraz chronić je przed modyfikacją podczas transferu. Protokół TLS używa kluczy publicznych do autoryzowania współdziałających stron oraz szyfrowania danych.

Autoryzacja Serwera administracyjnego po podłączeniu urządzenia

Podczas pierwszego łączenia urządzenia klienckiego z Serwerem administracyjnym Agent sieciowy na urządzeniu pobiera certyfikat Serwera administracyjnego i zapisuje go lokalnie.

> Jeśli instalujesz Agenta sieciowego lokalnie na urządzeniu, możesz ręcznie wybrać certyfikat Serwera administracyjnego.

Pobrana kopia certyfikatu jest używana do weryfikowania praw i przyzwoleń Serwera administracyjnego podczas kolejnych połączeń.

W trakcie następnych sesji Agent sieciowy będzie żądał certyfikatu Serwera administracyjnego przy każdym połączeniu urządzenia z Serwerem administracyjnym i będzie go porównywał z lokalną kopią. W przypadku, gdy obie kopie nie będą do siebie pasowały, urządzenie nie uzyska pozwolenia na dostęp do Serwera administracyjnego.

Autoryzacja Serwera administracyjnego podczas podłączania Konsoli administracyjnej

Podczas pierwszego połączenia z Serwerem administracyjnym Konsola administracyjna żąda certyfikatu Serwera administracyjnego i zapisuje go lokalnie na stacji roboczej administratora. Następnie, przy każdej próbie połączenia Konsoli administracyjnej z tym Serwerem administracyjnym, Serwer administracyjny zostanie zidentyfikowany na podstawie kopii certyfikatu.

Jeśli certyfikat Serwera administracyjnego nie odpowiada kopii przechowywanej na stacji roboczej administratora, Konsola administracyjna wyświetli pytanie o potwierdzenie nawiązania połączenia z Serwerem administracyjnym o określonej nazwie i pobranie nowego certyfikatu. Po nawiązaniu połączenia Konsola administracyjna zapisuje kopię nowego certyfikatu Serwera administracyjnego, która będzie wykorzystywana do identyfikowania Serwera administracyjnego w przyszłości.

Konfigurowanie listy dozwolonych adresów IP do łączenia się z Serwerem administracyjnym

Domyślnie użytkownicy mogą logować się do Kaspersky Security Center na dowolnym urządzeniu, na którym można otworzyć konsolę Kaspersky Security Center Web Console (zwaną dalej Web Console) lub konsolę administracyjną opartą na MMC. Możesz jednak skonfigurować serwer administracyjny tak, aby użytkownicy mogli łączyć się z nim tylko z urządzeń o dozwolonych adresach IP. W takim przypadku, nawet jeśli intruz ukradnie konto Kaspersky Security Center, nie będzie mógł zalogować się do Kaspersky Security Center, ponieważ adres IP urządzenia intruza nie znajduje się na liście zezwolonych.

Adres IP jest sprawdzany, gdy użytkownik loguje się do Kaspersky Security Center lub uruchamia aplikację, która współdziała z Serwerem administracyjnym poprzez Kaspersky Security Center OpenAPI. W tym momencie urządzenie użytkownika próbuje nawiązać połączenie z Serwerem administracyjnym. Jeśli adresu IP urządzenia nie ma na liście zezwolonych, wystąpi błąd uwierzytelniania, a zdarzenie KLAUD_EV_SERVERCONNECT powiadamia, że połączenie z serwerem administracyjnym nie zostało nawiązane.

Wymagania dotyczące listy zezwolonych adresów IP

Adresy IP są weryfikowane tylko wtedy, gdy następujące aplikacje próbują połączyć się z serwerem administracyjnym:

- Web Console Server

  Jeśli logujesz się do Web Console na jednym urządzeniu, a serwer Web Console jest zainstalowany na innym, możesz skonfigurować zaporę sieciową na urządzeniu, na którym zainstalowano serwer konsoli internetowej, przy użyciu standardowych środków systemu operacyjnego. Następnie, jeśli ktoś spróbuje zalogować się do Web Console, zapora sieciowa pomoże zapobiec ingerencji intruzów.

- Konsola administracyjna
- Aplikacje współpracujące z serwerem administracyjnym za pośrednictwem obiektów automatyzacji klakaut
- Aplikacje współpracujące z serwerem administracyjnym za pośrednictwem interfejsu OpenAPI, takie jak Kaspersky Anti Targeted Attack Platform lub Kaspersky Security for Virtualization

Dlatego należy podać adresy urządzeń, na których zainstalowane są wymienione powyżej aplikacje.

Możesz ustawić adresy IPv4 i IPv6. Nie możesz określić zakresów adresów IP.

Jak ustanowić listę zezwolonych adresów IP

Jeśli wcześniej nie ustawiono listy dozwolonych, postępuj zgodnie z poniższymi instrukcjami.

W celu ustanowienia listy zezwolonych adresów IP do logowania się do Kaspersky Security Center:

1. Na urządzeniu serwera administracyjnego uruchom wiersz poleceń na koncie z uprawnieniami administratora.
2. Zmień bieżący katalog na folder instalacyjny Kaspersky Security Center (zwykle <dysk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).
3. Wpisz następujące polecenie, korzystając z uprawnień administratora:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<adresy IP>" -t s`

   Określ adresy IP, które spełniają powyższe wymagania. Wiele adresów IP należy oddzielać średnikami.

   Przykład — jak zezwolić tylko jednemu urządzeniu na łączenie się z serwerem administracyjnym:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Przykład — jak zezwolić wielu urządzeniom na łączenie się z serwerem administracyjnym:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`
4. Uruchom ponownie usługę Serwera administracyjnego.

Możesz dowiedzieć się, czy pomyślnie skonfigurowano listę zezwolonych adresów IP w dzienniku zdarzeń aplikacji Kaspersky na serwerze administracyjnym.

Jak zmienić listę dozwolonych adresów IP

Listę zezwolonych adresów można zmienić tak samo, jak podczas jej tworzenia. W tym celu uruchom to samo polecenie i określ nową listę zezwolonych adresów:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<adresy IP>" -t s
```

Jeśli chcesz usunąć niektóre adresy IP z listy zezwolonych, przepisz je. Na przykład, lista zezwolonych zawiera następujące adresy IP: 192.0.2.0; 198.51.100.0; 203.0.113.0. Chcesz usunąć adres IP 198.51.100.0. Aby to zrobić, wpisz następujące polecenie w wierszu polecenia:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

Nie zapomnij ponownie uruchomić usługi serwera administracyjnego.

Jak zresetować skonfigurowaną listę zezwolonych adresów IP

Aby zresetować już skonfigurowaną listę dozwolonych adresów IP:

1. Wpisz następujące polecenie w wierszu polecenia, korzystając z uprawnień administratora:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`
2. Uruchom ponownie usługę Serwera administracyjnego.

Następnie adresy IP nie będą już weryfikowane.

Użycie narzędzia klscflag do zamknięcia portu 13291

Port 13291 na serwerze administracyjnym jest używany do odbierania połączeń z konsoli administracyjnych. Ten port jest domyślnie otwarty. Jeśli nie chcesz używać konsoli administracyjnej opartej na MMC ani narzędzia klakaut, możesz zamknąć ten port za pomocą narzędzia klscflag. To narzędzie zmienia wartość parametru KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Aby zamknąć port 13291:

1. Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Wykonaj następujące polecenie w wierszu poleceń:
   ```
   klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```

3. Uruchom ponownie usługę Serwera administracyjnego Kaspersky Security Center.

Port 13291 jest zamknięty.

Aby sprawdzić, czy port 13291 został pomyślnie zamknięty:

Wykonaj następujące polecenie w wierszu poleceń:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

To polecenie zwraca następujący wynik:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

Wartość `false` oznacza, że port jest zamknięty. W przeciwnym razie wyświetlana jest wartość `true`.

Odłączanie od Serwera administracyjnego

W celu odłączenia się od Serwera administracyjnego:

1. W drzewie konsoli wybierz węzeł odpowiadający Serwerowi administracyjnemu, który ma zostać odłączony.

2. Z menu kontekstowego węzła wybierz **Odłącz od Serwera administracyjnego**.

Dodawanie Serwera administracyjnego do drzewa konsoli

W celu dodania Serwera administracyjnego do drzewa konsoli:

1. W oknie głównym Kaspersky Security Center, w drzewie konsoli wybierz węzeł **Kaspersky Security Center**.
2. Z menu kontekstowego węzła wybierz **Nowy** → **Serwer administracyjny**.

   Węzeł **Serwer administracyjny - <Nazwa urządzenia> (Niepołączony)** zostanie utworzony w drzewie konsoli, z której będziesz mógł połączyć się z dowolnym Serwerem administracyjnym zainstalowanym w sieci.

Usuwanie Serwera administracyjnego z drzewa konsoli

W celu usunięcia Serwera administracyjnego z drzewa konsoli:

1. W drzewie konsoli wybierz węzeł odpowiadający Serwerowi administracyjnemu, który ma zostać usunięty.
2. Z menu kontekstowego węzła wybierz **Usuń**.

Dodawanie wirtualnego Serwera administracyjnego do drzewa konsoli

W celu dodania wirtualnego Serwera administracyjnego do drzewa konsoli:

1. W drzewie konsoli należy wybrać węzeł z nazwą Serwera administracyjnego, dla którego chcesz utworzyć wirtualny Serwer administracyjny.
2. W węźle Serwera administracyjnego wybierz folder **Serwery administracyjne**.
3. W obszarze roboczym folderu **Serwery administracyjne** kliknij odnośnik **Dodaj wirtualny Serwer administracyjny**.

   Zostanie uruchomiony Kreator tworzenia nowego wirtualnego Serwera administracyjnego.
4. W oknie **Nazwa wirtualnego Serwera administracyjnego** określ nazwę tworzonego wirtualnego Serwera administracyjnego.

   Nazwa wirtualnego Serwera administracyjnego nie może zawierać więcej niż 255 znaków oraz nie może zawierać żadnych znaków specjalnych (takich jak "*<>?\:|).
5. W oknie **Wprowadzanie adresu połączenia urządzenia z wirtualnym Serwerem administracyjnym** określ adres połączenia urządzenia

   Adres połączenia wirtualnego Serwera administracyjnego to adres sieciowy, poprzez który urządzenia będą nawiązywać połączenie z tym Serwerem. Adres połączenia posiada dwie części: adres sieciowy fizycznego Serwera administracyjnego oraz nazwę wirtualnego Serwera administracyjnego, oddzielone ukośnikiem. Nazwa wirtualnego Serwera administracyjnego zostanie zastąpiona automatycznie. Określony adres będzie używany na wirtualnym Serwerze administracyjnym jako domyślny adres w pakietach instalacyjnych Agenta sieciowego.

6. W oknie **Utwórz konto administratora wirtualnego Serwera administracyjnego** wskaż użytkownika z listy, który będzie administratorem wirtualnego Serwera administracyjnego, lub dodaj nowe konto administratora, klikając przycisk **Utwórz**.

   Możesz określić kilka kont.

W drzewie konsoli tworzony jest węzeł o nazwie **Serwer administracyjny <Nazwa wirtualnego Serwera administracyjnego>**.

Zmienianie konta usługi Serwera administracyjnego. Narzędzie klsrvswch

Jeżeli chcesz zmienić konto usługi Serwera administracyjnego ustawione podczas instalacji Kaspersky Security Center, możesz użyć narzędzia klsrvswch, zaprojektowanego do zmieniania konta Serwera administracyjnego.

Podczas instalacji Kaspersky Security Center narzędzie jest automatycznie kopiowane do folderu instalacyjnego aplikacji.

Liczba uruchomień narzędzia jest właściwie nieograniczona.

Musisz uruchomić narzędzie klsrvswch na urządzeniu Serwera administracyjnego z poziomu konta z uprawnieniami administratora, które zostało użyte do instalacji Serwera administracyjnego.

Narzędzie klsrvswch umożliwia zmianę typu konta. Na przykład, jeśli korzystasz z konta lokalnego, możesz zmienić je na konto domenowe lub na zarządzane konto usługi (i odwrotnie). Narzędzie klsrvswch nie pozwala na zmianę typu konta na konto usługi zarządzane przez grupę (gMSA).

Windows Vista i późniejsze wersje systemu Windows nie pozwalają na użycie konta SystemLokalny dla Serwera administracyjnego. W tych wersjach systemu Windows opcja **Konto SystemLokalny** jest nieaktywna.

W celu zmiany konta usługi Serwera administracyjnego na konto domeny:

1. Z folderu instalacyjnego Kaspersky Security Center użyj narzędzia klsrvswch. Domyślna ścieżka instalacji: <Disk>:\Program Files (x86)\ Kaspersky Lab\ Kaspersky Security Center.

   Ta akcja uruchamia również Kreator modyfikacji konta usługi Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

2. W oknie **Konto usługi Serwera administracyjnego** wybierz **Konto SystemLokalny**.

Po zakończeniu działania kreatora, zostanie zmienione konto Serwera administracyjnego. Serwer administracyjny rozpocznie pracę przy użyciu *Konto SystemLokalny* i użyje jego danych uwierzytelniających.

Do poprawnego działania Kaspersky Security Center wymagane jest, aby konto używane do uruchamiania Serwera administracyjnego posiadało uprawnienia administratora do zasobu, w którym przechowywana jest baza danych Serwera administracyjnego.

W celu zmiany konta usługi Serwera administracyjnego na konto użytkownika lub konto zarządzanej usługi:

1. Z folderu instalacyjnego Kaspersky Security Center użyj narzędzia klsrvswch. Domyślna ścieżka instalacji: <Disk>:\Program Files (x86)\ Kaspersky Lab\ Kaspersky Security Center.

   Ta akcja uruchamia również Kreator modyfikacji konta usługi Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

2. W oknie **Konto usługi Serwera administracyjnego** wybierz **Konto niestandardowe**.

3. Kliknij przycisk **Znajdź teraz**.

   Zostanie otwarte okno **Wybierz użytkownika**.

4. W otwartym oknie **Wybierz użytkownika** kliknij przycisk **Typy obiektów**.

5. Na liście typów obiektów wybierz **Użytkownicy** (jeśli chcesz konto użytkownika) lub **Konta usługi** (jeśli chcesz zarządzane konto usługi) i kliknij **OK**.

6. W polu nazwy obiektu wpisz nazwę konta lub część nazwy i kliknij **Sprawdź nazwy**.

7. Na liście pasujących nazw wybierz żądaną nazwę, a następnie kliknij **OK**.

8. Jeśli wybrałeś **Konta usługi**, w oknie **Hasło do konta** pozostaw pola **Hasło** i **Potwierdź hasło** puste. Jeśli wybrałeś **Użytkownicy**, wprowadź nowe hasło dla użytkownika i potwierdź je.

Konto usługi Serwera administracyjnego zostanie zmienione na konto, które wybrałeś.

Podczas korzystania z Microsoft SQL Server w trybie uwierzytelniania konta użytkownika przy użyciu narzędzi Microsoft Windows, nadane muszą zostać uprawnienia dostępu do bazy danych. Baza danych Kaspersky Security Center powinna należeć do tego konta użytkownika. Domyślnie używany jest schemat dbo.

Zmiana poświadczeń DBMS

Może zajść potrzeba zmiany poświadczeń DBMS, na przykład w celu wykonania rotacji poświadczeń ze względów bezpieczeństwa.

W celu zmiany poświadczeń DBMS w środowisku Windows przy użyciu klsrvswch.exe:

1. Uruchom narzędzie klsrvswch znajdujące się w folderze instalacyjnym programu Kaspersky Security Center. Domyślna ścieżka instalacji: <Disk>:\Program Files (x86)\ Kaspersky Lab\ Kaspersky Security Center.

   Musisz uruchomić narzędzie klsrvswch na urządzeniu Serwera administracyjnego z poziomu konta z uprawnieniami administratora, które zostało użyte do instalacji Serwera administracyjnego.

2. Kliknij przycisk **Dalej** kreatora, aż dojdziesz do kroku **Zmień poświadczenia dostępu do DBMS**.

3. W tym kroku **Zmień poświadczenia dostępu do DBMS** wykonaj następujące czynności:

Krok kreatora **Zmień poświadczenia dostępu do DBMS** jest pomijany, jeśli używane jest uwierzytelnianie systemu Windows.

- Wybierz opcję **Zastosuj nowe poświadczenia**.
- Podaj nową nazwę konta w polu **Konto**.
- Podaj nowe hasło do konta w polu **Hasło**.
- Określ nowe hasło w polu **Potwierdź hasło**.

Powinieneś określić poświadczenia konta, które istnieje w DBMS.

4. Kliknij przycisk **Dalej**.

Po zakończeniu pracy kreatora poświadczenia DBMS zostają zmienione.

Narzędzie klsrvswch może być używane wyłącznie do zmiany hasła konta w celu uwierzytelnienia SQL. Zmiana metody autoryzacji nie jest obsługiwana. Aby zmienić metodę autoryzacji, zainstaluj ponownie Serwer administracyjny i określ żądane ustawienia.

Zmiana folderu współdzielonego Serwera administracyjnego

Folder współdzielony Serwera administracyjnego jest określany podczas instalacji Serwera administracyjnego. Zmiana lokalizacji folderu współdzielonego jest także możliwe we właściwościach Serwera administracyjnego.

Aby zmienić folder współdzielony:

1. Utwórz folder udziału sieciowego i skonfiguruj uprawnienia do udziału oraz struktury folderów, aby zapewnić prawa do pełnej kontroli podgrupie **Wszyscy**.
2. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Zaawansowane**, a następnie Folder współdzielony **Folder współdzielony Serwera administracyjnego**.
4. W sekcji **Folder współdzielony Serwera administracyjnego** kliknij przycisk **Zmień**.
5. Wybierz folder, którego chcesz użyć jako współdzielonego.
6. Kliknij przycisk **OK**, aby zamknąć okno właściwości Serwera administracyjnego.
7. Przypisz podgrupie **Wszyscy** prawa do odczytu do folderu, który został wybrany jako współdzielony.

Rozwiązywanie problemów z węzłami Serwera administracyjnego

Drzewo konsoli w lewej części Konsoli administracyjnej zawiera węzły Serwerów administracyjnych. W drzewie konsoli możesz dodać tyle Serwerów administracyjnych, ile potrzebujesz.

Lista węzłów Serwerów administracyjnych w drzewie konsoli jest przechowywana w kopii pliku .msc w tle przy użyciu konsoli Microsoft Management Console. Kopia w tle tego pliku znajduje się w folderze %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ na urządzeniu, na którym jest zainstalowana Konsola administracyjna. Dla każdego węzła Serwera administracyjnego plik zawiera następujące informacje:

- Adres Serwera administracyjnego
- Numer portu
- Czy TLS jest używany

  Ten parametr zależy od numeru portu, użytego do nawiązania połączenia między Konsolą administracyjną a Serwerem administracyjnym.
- Nazwa użytkownika
- Certyfikatu Serwera administracyjnego

Rozwiązywanie problemów

Jeśli Konsola administracyjna nawiąże połączenie z Serwerem administracyjnym, certyfikat przechowywany lokalnie jest porównywany do certyfikatu Serwera administracyjnego. Jeśli certyfikaty nie pasują do siebie, Konsola administracyjna wygeneruje błąd. Na przykład, niedopasowanie certyfikatów może wystąpić, gdy zastąpisz certyfikat Serwera administracyjnego. W tym przypadku, w konsoli utwórz ponownie węzeł Serwera administracyjnego.

W celu ponownego utworzenia węzła Serwera administracyjnego:

1. Zamknij okno Konsoli administracyjnej Kaspersky Security Center.
2. Usuń plik w Kaspersky Security Center 15.1 w %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.
3. Uruchom Konsolę administracyjną Kaspersky Security Center.

   Zostanie wyświetlone pytanie o nawiązanie połączenia z Serwerem administracyjnym i zaakceptowanie jego istniejącego certyfikatu.
4. Wykonaj jedną z poniższych czynności:
   - Zaakceptuj istniejący certyfikat, klikając przycisk **Tak**.
   - Aby określić swój certyfikat, kliknij przycisk **Nie**, a następnie odszukaj plik certyfikatu, który zostanie użyty do autoryzacji na Serwerze administracyjnym.

Problem z certyfikatem zostanie rozwiązany. Do nawiązania połączenia z Serwerem administracyjnym możesz użyć Konsoli administracyjnej.

Przeglądanie i modyfikowanie ustawień Serwera administracyjnego

Ustawienia Serwera administracyjnego można dostosować w oknie właściwości tego Serwera.

W celu otwarcia okna Właściwości: Serwer administracyjny:

Z menu kontekstowego węzła Serwera administracyjnego w drzewie konsoli wybierz element **Właściwości**.

Dostosowywanie ogólnych ustawień Serwera administracyjnego

Ogólne ustawienia Serwera administracyjnego można dostosować w sekcjach **Ogólne**, **Ustawienia połączenia z Serwerem administracyjnym**, **Repozytorium zdarzeń** i **Zabezpieczenia**, dostępnych w oknie właściwości Serwera administracyjnego.

Sekcja **Zabezpieczenia** nie jest wyświetlana w oknie właściwości Serwera administracyjnego, jeśli wyświetlanie zostało wyłączone w interfejsie Konsoli administracyjnej.

*W celu włączenia wyświetlania sekcji **Zabezpieczenia** w Konsoli administracyjnej:*

1. W drzewie konsoli wybierz Serwer administracyjny, którego potrzebujesz.
2. W menu **Widok** okna głównego aplikacji wybierz **Konfiguruj interfejs**.
3. W otwartym oknie **Konfiguruj interfejs** zaznacz pole **Wyświetl sekcje ustawień zabezpieczeń** i kliknij **OK**.
4. W oknie z wiadomością aplikacji kliknij **OK**.

Sekcja **Zabezpieczenia** będzie wyświetlana w oknie właściwości Serwera administracyjnego.

Ustawienia interfejsu Konsoli administracyjnej

Możesz dostosować ustawienia interfejsu Konsoli administracyjnej do wyświetlania lub ukrywania kontrolek interfejsu użytkownika związanych z następującymi funkcjami:

- Zarządzanie lukami i poprawkami
- Szyfrowanie i ochrona danych
- Ustawienia kontroli węzła końcowego
- Zarządzanie urządzeniami mobilnymi
- Podrzędne Serwery administracyjne
- Sekcje Ustawienia zabezpieczeń

W celu skonfigurowania ustawień interfejsu Konsoli administracyjnej:

1. W drzewie konsoli wybierz Serwer administracyjny, którego potrzebujesz.
2. W menu **Widok** okna głównego aplikacji wybierz **Konfiguruj interfejs**.
3. W otwartym oknie **Konfiguruj interfejs** zaznacz pola obok funkcji, które mają być wyświetlane, a następnie kliknij **OK**.
4. W oknie z wiadomością aplikacji kliknij **OK**.

Wybrane funkcje zostaną wyświetlone w interfejsie Konsoli administracyjnej.

Przetwarzanie i przechowywanie zdarzeń na Serwerze administracyjnym

Informacje o zdarzeniach, występujących podczas działania aplikacji, oraz o zarządzanych urządzeniach są zapisywane w bazie danych Serwera administracyjnego. Każdemu zdarzeniu przypisywany jest określony typ i priorytet (*Zdarzenie krytyczne*, *Błąd funkcjonalny*, *Ostrzeżenie* lub *Informacja*). W zależności od warunków, przez które pojawiło się zdarzenie, do zdarzeń tego samego typu aplikacja może przypisywać różne priorytety.

Typy i priorytety przypisane do zdarzeń można sprawdzić w sekcji **Konfiguracja zdarzenia** okna właściwości Serwera administracyjnego. W sekcji **Konfiguracja zdarzenia** możesz także skonfigurować przetwarzanie każdego zdarzenia przez Serwer administracyjny:

- Rejestrację zdarzeń na Serwerze administracyjnym i w raporcie zdarzeń systemu operacyjnego na urządzeniu i na Serwerze administracyjnym.
- Metodę używaną do informowania administratora o zdarzeniu (na przykład, wiadomość SMS lub e-mail).

W sekcji **Repozytorium zdarzeń** okna właściwości Serwera administracyjnego możesz zmodyfikować ustawienia przechowywania zdarzeń w bazie danych Serwera administracyjnego, ograniczając liczbę wpisów zdarzeń i czas przechowywania wpisów. Jeśli określisz maksymalną liczbę zdarzeń, aplikacja oblicza przybliżoną ilość miejsca przechowywania, wymaganą dla określonej liczby. Możesz użyć tego przybliżonego obliczenia do oszacowania wystarczającej ilości wolnego miejsca na dysku, aby uniknąć przepełnienia bazy danych. Domyślna pojemność bazy danych Serwera administracyjnego wynosi 400 000 zdarzeń. Maksymalną dozwoloną pojemnością bazy danych jest 45 milionów zdarzeń.

Aplikacja sprawdza bazę danych co 10 minut. Jeśli liczba zdarzeń osiągnie określoną maksymalną wartość plus 10 000, aplikacja usunie najstarsze zdarzenia, tak aby pozostała tylko określona maksymalna liczba zdarzeń.

Jeśli Serwer administracyjny usuwa starsze zdarzenia, nie może zapisywać nowych zdarzeń do bazy danych. W tym czasie informacje o odrzuconych zdarzeniach są zapisywane w dzienniku zdarzeń aplikacji Kaspersky. Nowe zdarzenia zostają zakolejkowane, a następnie zapisane do bazy danych po zakończeniu operacji usuwania.

Możesz zmienić ustawienia dowolnego zadania zapisywać zdarzenia związane z postępem zadania lub zapisywać tylko wyniki wykonania zadania. Postępując w ten sposób, zmniejszysz liczbę zdarzeń w bazie danych, zwiększysz prędkość wykonywania scenariuszy skojarzonych z analizą tabeli zdarzeń w bazie danych, a także zmniejszysz ryzyko nadpisania krytycznych zdarzeń przez dużą liczbę zdarzeń.

Przeglądanie raportów połączeń z Serwerem administracyjnym

Historia połączeń i prób nawiązania połączenia z Serwerem administracyjnym podczas jego działania może zostać zapisana w pliku raportu. Informacje w pliku umożliwiają śledzenie nie tylko połączeń w obrębie infrastruktury sieci, ale także nieautoryzowanych prób uzyskania dostępu do Serwera administracyjnego.

W celu zapisania zdarzeń nawiązania połączenia z Serwerem administracyjnym:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz włączyć zapisywanie zdarzeń połączenia.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W otwartym oknie właściwości, w sekcji **Ustawienia połączenia z Serwerem administracyjnym** wybierz podsekcję **Porty połączenia**.

4. Włącz opcję **Zapisuj zdarzenia połączenia z Serwerem administracyjnym**.

5. Kliknij przycisk **OK**, aby zamknąć okno właściwości Serwera administracyjnego.

Wszystkie dalsze zdarzenia przychodzących połączeń z Serwerem administracyjnym, wyniki autoryzacji i błędy SSL zostaną zapisane do pliku %ProgramData%\KasperskyLab\adminkit\logs\SC.syslog.

Kontrola epidemii wirusów

Kaspersky Security Center umożliwia szybkie reagowanie na pojawiające się zagrożenia epidemiami wirusów. Ryzyko wystąpienia epidemii wirusów jest szacowane w oparciu o kontrolę aktywności wirusów na urządzeniach.

W sekcji **Epidemia wirusa**, dostępnej w oknie właściwości Serwera administracyjnego, możesz skonfigurować reguły oceny dla zagrożeń epidemią wirusów i akcje wykonywane w razie epidemii.

Możesz określić procedurę powiadamiania dla zdarzenia *Epidemia wirusa* w sekcji **Konfiguracja zdarzenia** okna właściwości Serwera administracyjnego, w oknie właściwości zdarzenia *Epidemia wirusa*.

Zdarzenie *Epidemia wirusa* jest generowane w przypadku wykrycia zdarzeń *Wykryto szkodliwy obiekt* w trakcie działania aplikacji zabezpieczających. Dlatego też należy zapisywać informacje o wszystkich zdarzeniach *Wykryto szkodliwy obiekt* na Serwerze administracyjnym, aby móc rozpoznać epidemie wirusów.

Możesz określić ustawienia zapisywania informacji o każdym zdarzeniu *Wykryto szkodliwy obiekt* w zasadach aplikacji zabezpieczających.

Podczas zliczania zdarzeń *Wykryto szkodliwy obiekt* pod uwagę brane są wyłącznie informacje z urządzeń głównego Serwera administracyjnego. Informacje od podrzędnych Serwerów administracyjnych nie są brane pod uwagę. Ustawienia zdarzenia *Epidemia wirusa* są konfigurowane indywidualnie dla każdego Serwera podrzędnego.

Ograniczanie ruchu sieciowego

Aby zmniejszyć ruch sieciowy w obrębie sieci, aplikacja posiada opcję ograniczania prędkości przesyłania danych na Serwer administracyjny z określonych zakresów IP i podsieci IP.

Reguły ograniczania ruchu sieciowego można utworzyć i skonfigurować w sekcji **Ruch sieciowy** okna właściwości Serwera administracyjnego.

W celu utworzenia reguły ograniczania ruchu sieciowego:

1. W drzewie konsoli należy wybrać węzeł z nazwą Serwera administracyjnego, dla którego chcesz utworzyć regułę ograniczenia ruchu sieciowego.

2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.

3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Ruch sieciowy**.

4. Kliknij przycisk **Dodaj**.

5. W sekcji **Nowa reguła** określ następujące ustawienia:

W sekcji **Zakres IP, dla którego ograniczany jest ruch sieciowy** wybierz metodę, która będzie używana do określenia podsieci lub zakresu, dla którego przesyłanie danych będzie ograniczone, a następnie wprowadź wartości ustawień dla wybranej metody. Wybierz jedną z następujących metod:

- **Określ zakres poprzez adres oraz maskę sieci**

  Ruch sieciowy jest ograniczony na podstawie ustawień podsieci. Określ adres podsieci i maskę podsieci do określania zakresu, w którym ruch sieciowy będzie ograniczony.

  Możesz także kliknąć **Przeglądaj**, aby dodać podsieci z globalnej listy podsieci.

- **Określ zakres podając adres początkowy i końcowy**

  Ruch sieciowy jest ograniczony w oparciu o zakres adresów IP. Określ zakres adresów IP w polach **Adres początkowy** oraz **Adres końcowy**.

  Opcja ta jest wybrana domyślnie.

W sekcji **Ograniczenie ruchu sieciowego** możesz dostosować następujące restrykcyjne ustawienia współczynnika przesyłania danych:

- **Przedział czasu**

  Przedział czasu, w trakcie którego zostanie zastosowane ograniczenie ruchu sieciowego. W polach do wprowadzania danych można określić granice przedziału czasu.

- **Ograniczenie (KB/s)**

  Maksymalna łączna szybkość transferu danych przychodzących i wychodzących Serwera administracyjnego. Ograniczenie ruchu sieciowego będzie stosowane tylko w obrębie przedziału czasu określonego w polu **Przedział czasu**.

- **Ogranicz ruch w pozostałym czasie (KB/s)**

  Ruch sieciowy będzie ograniczony nie tylko w czasie określonym w polu **Przedział czasu**, ale także w pozostałym czasie.

  Domyślnie pole to nie jest zaznaczone. Wartość tego pola nie może odpowiadać wartości pola **Ograniczenie (KB/s)**.

Przede wszystkim, reguły ograniczenia ruchu sieciowego wpływają na przesyłanie plików. Te reguły nie są stosowane do ruchu sieciowego wygenerowanego przez synchronizację między Serwerem administracyjnym a Agentem sieciowym lub między głównym a podrzędnym Serwerem administracyjnym.

Konfigurowanie serwera sieciowego

Serwer sieciowy został zaprojektowany do publikowania autonomicznych pakietów instalacyjnych, profili iOS MDM oraz plików z folderu współdzielonego.

Możesz zdefiniować ustawienia łączenia serwera sieciowego z Serwerem administracyjnym oraz określić certyfikat serwera sieciowego w sekcji **Serwer WWW** okna właściwości Serwera administracyjnego.

Praca z użytkownikami wewnętrznymi

Konta *użytkowników wewnętrznych* są używane do pracy z wirtualnymi Serwerami administracyjnymi. Kaspersky Security Center nadaje wewnętrznym użytkownikom aplikacji uprawnienia rzeczywistych użytkowników.

Konta wewnętrznych użytkowników są tworzone i używane tylko w obrębie Kaspersky Security Center. Do systemu operacyjnego nie są przesyłane żadne dane dotyczące wewnętrznych użytkowników. Kaspersky Security Center autoryzuje wewnętrznych użytkowników.

Możesz skonfigurować konta użytkowników wewnętrznych w folderze **Konta użytkowników** drzewa konsoli.

Tworzenie kopii zapasowej i przywracanie ustawień Serwera administracyjnego

Tworzenie kopii zapasowej ustawień Serwera administracyjnego i jego baz danych odbywa się przy użyciu zadania tworzenia kopii zapasowej oraz narzędzia klbackup. Kopia zapasowa zawiera wszystkie główne ustawienia i obiekty dotyczące Serwera administracyjnego, takie jak certyfikaty, klucze główne do szyfrowania dysków na zarządzanych urządzeniach, klucze dla różnych licencji, strukturę grup administracyjnych z całą ich zawartością, zadaniami, zasadami itd. Przy pomocy kopii zapasowej można przywrócić działanie Serwera administracyjnego tak szybko, jak to możliwe, poświęcając na to od kilkunastu minut do kilku godzin.

Jeśli nie ma dostępnej kopii zapasowej, błąd może doprowadzić do bezpowrotnej utraty certyfikatów i wszystkich ustawień Serwera administracyjnego. Będzie to wymagało przeprowadzenia konfiguracji Kaspersky Security Center od początku oraz ponownego zainstalowania Agenta sieciowego w sieci organizacji. Wszystkie klucze główne do szyfrowania dysków na zarządzanych urządzeniach zostaną utracone, co spowoduje ryzyko utraty zaszyfrowanych danych na urządzeniach z zainstalowanym programem Kaspersky Endpoint Security. Dlatego też nigdy nie rezygnuj z regularnego wykonywania kopii zapasowej Serwera administracyjnego przy użyciu standardowego zadania tworzenia kopii zapasowej.

Kreator wstępnej konfiguracji tworzy zadanie wykonywania kopii zapasowej dla ustawień Serwera administracyjnego i ustawia jego codzienne wykonywanie na godzinę 4:00. Kopie zapasowe są domyślnie zapisywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskySC.

Jeśli serwer Microsoft SQL Server, zainstalowany na innym urządzeniu, jest używany jako DBMS, należy zmodyfikować zadanie tworzenia kopii zapasowej, określając jako folder do przechowywania kopii zapasowych ścieżkę UNC, która jest używana do zapisywania usługi Serwera administracyjnego oraz usługi SQL Server. To wymaganie wynika ze specyfiki specjalnej funkcji kopii zapasowej w systemie DBMS serwera Microsoft SQL Server.

Jeśli jako system DBMS używana jest lokalna instancja serwera Microsoft SQL Server, zalecane jest zapisanie kopii zapasowych na dedykowanym nośniku w celu zabezpieczenia ich przed uszkodzeniem wraz z Serwerem administracyjnym.

Ponieważ kopia zapasowa zawiera ważne dane, zadanie tworzenia kopii zapasowej oraz narzędzie klbackup oferują ochronę kopii zapasowej przy użyciu hasła. Domyślnie zadanie tworzenia kopii zapasowej wykonuje kopię zapasową z pustym hasłem. Hasło należy ustawić we właściwościach zadania tworzenia kopii zapasowej. Pominięcie tego wymagania doprowadza do sytuacji, w której wszystkie klucze certyfikatów Serwera administracyjnego, klucze dla licencji oraz klucze główne dla szyfrowania dysków na zarządzanych urządzeniach pozostaną niezaszyfrowane.

Oprócz regularnych kopii zapasowych, kopie zapasowe należy tworzyć także przed każdą znaczącą zmianą, w tym instalacją aktualizacji i łat Serwera administracyjnego.

Jeśli używasz Microsoft SQL Server jako DBMS, możesz zminimalizować rozmiar kopii zapasowych. W tym celu włącz opcję **Kompresuj kopię zapasową** w ustawieniach SQL Server.

Przywracanie kopii zapasowej odbywa się przy użyciu narzędzia klbackup na działającej instancji Serwera administracyjnego, który został właśnie zainstalowany i posiada tę samą wersję (lub nowszą), dla której kopia zapasowa została utworzona.

Instancja Serwera administracyjnego, na którym kopia zapasowa ma zostać przywrócona, musi korzystać z systemu DBMS tego samego typu (na przykład ten sam SQL Server lub MariaDB) i tej samej lub nowszej wersji. Wersja Serwera administracyjnego może być taka sama (z tą samą lub późniejszą łatą) lub nowsza.

Sekcja opisuje standardowe scenariusze przywracania ustawień i obiektów Serwera administracyjnego.

Używanie migawek systemu plików do skrócenia czasu tworzenia kopii zapasowej

W Kaspersky Security Center 15.1 czas bezczynności serwera administracyjnego w trakcie wykonywania kopii zapasowej został skrócony w porównaniu do wcześniejszych wersji. Co więcej, funkcja **Użyj migawki systemu plików do wykonania kopii zapasowej danych** została dodana do ustawień zadania. Ta funkcja zapewnia dodatkową redukcję czasu bezczynności przy użyciu narzędzia klbackup, które tworzy w tle kopię dysku podczas wykonywania kopii zapasowej (zajmuje to kilka sekund) i jednocześnie kopiuje bazę danych (najdłużej może to potrwać kilka minut). Jeśli narzędzie klbackup utworzy w tle kopię dysku oraz kopię bazy danych, ponownie umożliwi połączenie z Serwerem administracyjnym.

Funkcja tworzenia migawek systemu plików może być używana tylko wtedy, gdy spełnione są te dwa warunki:

- Folder współdzielony Serwera administracyjnego oraz folder %ALLUSERSPROFILE%\KasperskyLab znajdują się na tym samym dysku logicznym i są lokalne w odniesieniu do Serwera administracyjnego.
- Folder %ALLUSERSPROFILE%\KasperskyLab nie zawiera żadnych łączy symbolicznych, które zostały utworzone ręcznie.

Nie używaj tej funkcji, jeśli żaden z tych warunków nie może zostać spełniony. W tym przypadku, w odpowiedzi na jakąkolwiek próbę utworzenia migawki systemu plików aplikacja zwróci komunikat o błędzie.

Aby użyć funkcji, musisz posiadać konto, któremu nadano uprawnienie do tworzenia migawek dysku logicznego, na którym znajduje się folder %ALLUSERSPROFILE%. Należy pamiętać, że konto usługi Serwera administracyjnego nie posiada takiego uprawnienia.

W celu użycia funkcji tworzenia migawek systemu plików do skrócenia czasu tworzenia kopii zapasowej:

1. W sekcji **Zadania** wybierz zadanie tworzenia kopii zapasowej.
2. Z menu kontekstowego wybierz **Właściwości**.
3. W oknie właściwości zadania wybierz sekcję **Ustawienia**.
4. Zaznacz pole **Użyj migawki systemu plików do wykonania kopii zapasowej danych**.
5. W polach **Nazwa użytkownika** i **Hasło** wprowadź nazwę i hasło dla konta, któremu nadano uprawnienie do tworzenia migawek dysku logicznego, na którym znajduje się folder %ALLUSERSPROFILE%.
6. Kliknij **Zastosuj**.

Przy każdym kolejnym uruchomieniu zadania tworzenia kopii zapasowej narzędzie klbackup utworzy migawki systemu plików, skracając czas bezczynności Serwera administracyjnego podczas wykonywania zadania.

Urządzenie z zainstalowanym Serwerem administracyjnym nie działa

Jeśli urządzenie, na którym jest zainstalowany Serwer administracyjny, nie działa z powodu błędu, zalecane jest wykonanie następujących działań:

- Nowy Serwer administracyjny musi posiadać ten sam adres: nazwę NetBIOS, nazwę FQDN lub statyczny adres IP (w zależności od tego, co zostało ustawione podczas instalacji Agentów sieciowych).
- Zainstaluj Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą lub nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu kreatora.
- W menu **Start** uruchom narzędzie klbackup i wykonaj przywracanie.

Ustawienia Serwera administracyjnego lub bazy danych są uszkodzone

Jeżeli Serwer administracyjny nie działa ze względu na uszkodzone ustawienia lub bazę danych (na przykład, w wyniku przepięcia), zalecane jest użycie następujących scenariuszy:

1. Przeskanuj system plików na uszkodzonym urządzeniu.
2. Odinstaluj niedziałającą wersję Systemu operacyjnego.
3. Zainstaluj ponownie Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej (lub nowszej) wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą lub nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu kreatora.
4. Z poziomu menu **Start** uruchom narzędzie klbackup i przywróć kopię zapasową.

Zabronione jest przywracanie Serwera administracyjnego w sposób inny niż przy użyciu narzędzia klbackup.

Wszelkie próby przywrócenia Serwera administracyjnego przy użyciu oprogramowania firm trzecich doprowadzą do desynchronizacji danych na węzłach aplikacji Kaspersky Security Center i w konsekwencji - do niepoprawnego działania aplikacji.

Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego

Tworzenie kopii zapasowej danych umożliwia przeniesienie Serwera administracyjnego z jednego urządzenia na inne, bez utraty danych. Dzięki kopii zapasowej możesz przywrócić dane podczas przenoszenia bazy danych Serwera administracyjnego na inne urządzenie lub podczas aktualizacji do nowszej wersji Kaspersky Security Center. Możesz również wykorzystać Kopię zapasową danych do przeniesienia danych Serwera administracyjnego z Kaspersky Security Center Windows zarządzanego przez Kaspersky Security Center Linux (przenoszenie danych z Kaspersky Security Center Linux do Kaspersky Security Center Windows nie jest obsługiwane).

Nie są tworzone kopie zapasowe zainstalowanych wtyczek zarządzających. Po przywróceniu danych Serwera administracyjnego z kopii zapasowej należy pobrać i ponownie zainstalować wtyczki dla zarządzanych aplikacji.

Zanim utworzysz kopię zapasową danych Serwera administracyjnego, sprawdź, czy do grupy administracyjnej został dodany wirtualny Serwer administracyjny. Jeśli dodany jest wirtualny Serwer administracyjny, przed utworzeniem kopii zapasowej upewnij się, że do tego wirtualnego Serwera administracyjnego został przypisany administrator. Po utworzeniu kopii zapasowej nie możesz nadać administratorowi praw dostępu do wirtualnego Serwera administracyjnego. Należy pamiętać, że w przypadku utraty poświadczeń konta administratora nie będzie można przypisać nowego administratora do wirtualnego Serwera administratora.

Aby utworzyć kopię zapasową lub przywrócić klaster pracy awaryjnej Kaspersky Security Center, należy zatrzymać cały klaster w celu przeprowadzenia konserwacji, a następnie ponownie go uruchomić po zakończeniu tworzenia kopii zapasowej lub przywracania.

Możesz utworzyć kopię zapasową danych Serwera administracyjnego w jeden z następujących sposobów:

- Tworząc i uruchamiając zadanie wykonywania kopii zapasowej danych poprzez Konsolę administracyjną.
- Uruchamiając narzędzie klbackup na urządzeniu, na którym jest zainstalowany Serwer administracyjny. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center. Po zainstalowaniu Serwera administracyjnego, narzędzie jest umieszczane w katalogu głównym folderu docelowego, określonego podczas instalacji aplikacji.

W kopii zapasowej Serwera administracyjnego zapisywane są następujące dane:

- Baza danych Serwera administracyjnego (zasady, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym).
- Informacje o konfiguracji struktury grup administracyjnych i urządzeń klienckich.
- Repozytorium pakietów dystrybucyjnych aplikacji przeznaczonych do zdalnego zainstalowania.
- Certyfikat Serwera administracyjnego.

- Zawartość folderu *Aktualizacje*.

  Domyślna ścieżka do folderu to C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

Odzyskanie danych Serwera administracyjnego jest możliwe tylko przy użyciu narzędzia klbackup. Należy wykonać przywracanie kopii zapasowej na działającej instancji Serwera administracyjnego, który został właśnie zainstalowany i posiada tę samą wersję (lub nowszą), dla której kopia zapasowa została utworzona.

Zadanie Utwórz kopię zapasową danych Serwera administracyjnego

Tworzenie zadania kopii zapasowej danych Serwera administracyjnego

Zadanie kopii zapasowej jest zadaniem Serwera administracyjnego; jest tworzone przez Kreator wstępnej konfiguracji. Jeśli zadanie kopii zapasowej utworzone przez Kreator wstępnej konfiguracji zostało usunięte, możesz je utworzyć ręcznie.

Aby utworzyć zadanie kopii zapasowej danych Serwera administracyjnego:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania w jeden z następujących sposobów:
   - Wybierając **Nowe** → **Zadanie** w menu kontekstowym folderu **Zadania** w drzewie konsoli.
   - Kliknij przycisk **Utwórz zadanie** w obszarze roboczym.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora. W oknie **Wybierz typ zadania** wybierz typ zadania **Kopia zapasowa danych Serwera administracyjnego**.

Zadanie **Kopia zapasowa danych Serwera administracyjnego** może zostać utworzone tylko w jednej kopii. Jeśli dla Serwera administracyjnego już utworzono zadanie tworzenia kopii zapasowych danych Serwera administracyjnego, nie będzie wyświetlane w oknie wyboru typu zadania kreatora tworzenia zadania kopii zapasowej Serwera administracyjnego.

Konfigurowanie zadania Utwórz kopię zapasową danych Serwera administracyjnego

Po utworzeniu zadania kopii zapasowej możesz skonfigurować ustawienia zadania.

Aby skonfigurować zadanie Kopia zapasowa danych Serwera administracyjnego:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Z menu kontekstowego zadania **Kopia zapasowa danych Serwera administracyjnego** wybierz **Właściwości**.

   Otworzy się okno właściwości zadania *Kopia zapasowa danych Serwera administracyjnego*. Dostępne są następujące właściwości:

- **Ogólne**

  W sekcji **Ogólne** możesz określić nazwę zadania, wyświetlić datę utworzenia zadania, datę ostatniego polecenia, statusy uruchomienia zadania i wyniki zadania.

- **Powiadamianie**

  W sekcji **Powiadamianie** możesz określić ustawienia przechowywania zdarzeń związanych z wynikami wykonywanych zadań, a także skonfigurować powiadomienia o wynikach wykonania zadania.

- **Terminarz**

  W sekcji **Terminarz** możesz określić harmonogram rozpoczęcia zadania.

- **Miejsce docelowe**

  W sekcji **Miejsce docelowe** możesz określić ścieżkę do folderu, w którym będą przechowywane kopie zapasowe danych Serwera administracyjnego.

- **Ustawienia**

  W sekcji **Ustawienia** możesz w razie potrzeby ustawić hasło ochrony kopii zapasowych i liczbę kopii zapasowych.

  Możesz także utworzyć kopię w tle dysku logicznego przechowującego folder %ALLUSERSPROFILE% i skopiować bazę danych Serwera administracyjnego. W tym celu należy włączyć opcję **Użyj migawki systemu plików do wykonania kopii zapasowej danych**, a następnie podać nazwę i hasło konta posiadającego uprawnienia do tworzenia migawek.

- **Zabezpieczenia**

  W sekcji **Zabezpieczenia** możesz nadać użytkownikom i grupom uprawnienia do wykonywania operacji na Serwerze administracyjnym. Jeżeli opcja **Dziedzicz ustawienia od Serwera administracyjnego** jest włączona, ustawienia zabezpieczeń zadania zostaną odziedziczone z Serwera administracyjnego.

  Jeśli ta opcja jest wyłączona, możesz skonfigurować ustawienia zabezpieczeń dla zadania. Możesz przypisać rolę do użytkownika lub grupy użytkowników lub przypisać uprawnienia do użytkownika lub grupy użytkowników, jak zastosowano do zadania.

  Domyślnie opcja **Dziedzicz ustawienia od Serwera administracyjnego** jest włączona.

- **Historia rewizji**

  W sekcji **Historia rewizji** możesz śledzić modyfikację zadania. Za każdym razem, gdy zapisujesz zmiany wprowadzone w zadaniu, tworzona jest rewizja.

Narzędzie do tworzenia kopii zapasowej i odzyskiwania danych (klbackup)

Możesz utworzyć kopie danych Serwera administracyjnego w celu przechowywania kopii zapasowych oraz przyszłego ich odzyskania przy użyciu narzędzia klbackup stanowiącego część pakietu dystrybucyjnego Kaspersky Security Center.

Narzędzie klbackup można uruchomić w jednym z dwóch trybów:

- Interaktywnym
- Cichy

Tworzenie kopii zapasowej i przywracanie danych w trybie interaktywnym

Przywracanie danych Serwera administracyjnego z kopii zapasowej utworzonej za pomocą narzędzia klbackup w trybie interaktywnym może zakończyć się błędem. Jeśli zainstalowałeś poprawkę 15.1.0.20748-pf2 dla Serwera administracyjnego, a następnie utworzyłeś kopię zapasową za pomocą narzędzia klbackup z wyłączoną opcją **Przeprowadź migrację bazę danych**, podczas przywracania tej kopii wystąpi błąd (dotyczy wszystkich systemów DBMS z wyjątkiem MySQL i MariaDB). Jeśli masz zainstalowaną poprawkę 15.1.0.20748-pf2 dla Serwera administracyjnego i chcesz utworzyć kopię zapasową bez migracji do innego systemu DBMS, użyj zadania tworzenia kopii zapasowej danych lub uruchom narzędzie klbackup z wiersza poleceń.

W celu utworzenia kopii zapasowej danych Serwera administracyjnego w trybie interaktywnym:

1. Uruchom narzędzie klbackup znajdujące się w folderze instalacyjnym Kaspersky Security Center.

   Zostanie uruchomiony Kreator tworzenia kopii zapasowej i przywracania.

2. W pierwszym oknie kreatora wybierz **Wykonaj kopię zapasową danych Serwera administracyjnego**.

   Jeśli wybierzesz opcję **Przywróć lub wykonaj kopię zapasową jedynie certyfikatu Serwera administracyjnego**, zostanie zapisana tylko kopia zapasowa certyfikatu i klucza prywatnego Serwera administracyjnego. Tworzenie kopii zapasowej certyfikatu i klucza prywatnego Serwera administracyjnego może okazać się przydatne podczas wykonywania migracji z Serwera administracyjnego Kaspersky Security Center Windows na Serwer administracyjnych Kaspersky Security Center Linux. Możesz również migrować zarządzane urządzenia pomiędzy Serwerami administracyjnymi Kaspersky Security Center Linux, a także pomiędzy Serwerami administracyjnymi Kaspersky Security Center Windows. Aby uzyskać więcej informacji, zobacz Używanie narzędzia klbackup w celu przełączania zarządzanych urządzeń na zarządzenie przez inny Serwer administracyjny.

   Kliknij **Dalej**.

3. W kolejnym oknie Kreatora określ następujące opcje:

   - **Folder docelowy kopii zapasowej**
   - **Przeprowadź migrację bazy danych**

     Włącz tę opcję, jeśli obecnie przechowujesz dane Serwera administracyjnego w bazie danych Microsoft SQL Server i musisz je przenieść do jednej z następujących baz danych: MySQL lub MariaDB, PostgreSQL lub Postgres Pro, Azure SQL. Domyślnie opcja ta jest wyłączona.

     - **Wykonaj migrację do formatu MySQL/MariaDB**

       Włącz tę opcję, jeśli obecnie używasz SQL Server jako DBMS dla Serwera administracyjnego i chcesz przeprowadzić migrację danych z SQL Server do MySQL lub MariaDB DBMS. Kaspersky Security Center utworzy kopię zapasową kompatybilną z MySQL i MariaDB. Następnie możesz przywrócić dane z kopii zapasowej do MySQL lub MariaDB.

     - **Migracja do Postgres**

       Włącz tę opcję, jeśli obecnie używasz SQL Server jako DBMS dla Serwera administracyjnego i chcesz przeprowadzić migrację danych z SQL Server do PostgreSQL lub Postgres Pro DBMS. Kaspersky Security Center utworzy kopię zapasową kompatybilną z PostgreSQL i Postgres Pro. Następnie możesz przywrócić dane z kopii zapasowej do PostgreSQL lub Postgres Pro.

Ta opcja będzie dostępna po zwróceniu się do pomocy technicznej Kaspersky i zainstalowaniu poprawki 15.1.0.20748-pf2 dla Serwera administracyjnego lub aktualizacji do Kaspersky Security Center Windows w wersji 15.1.0.22239.

- **Wykonaj migrację do formatu Azure**

  Włącz tę opcję, jeśli obecnie używasz SQL Server jako DBMS dla Serwera administracyjnego i chcesz przeprowadzić migrację danych z SQL Server do Azure SQL DBMS. Kaspersky Security Center utworzy kopię zapasową kompatybilną z Azure SQL. Następnie możesz przywrócić dane z kopii zapasowej do Azure SQL.

- **Dołącz bieżącą datę i czas do nazwy folderu docelowego przechowującego kopie zapasowe**

- **Hasło do kopii zapasowej**

4. Kliknij przycisk **Dalej**, aby uruchomić tworzenie kopii zapasowej.

5. Jeśli pracujesz z bazami danych w środowisku chmury, takim jak Amazon Web Services (AWS) lub Microsoft Azure, w oknie **Zaloguj się do magazynu online** wypełnij następujące pola:

   - Dla AWS:

     - **Nazwa komory S3**

       Nazwa komory S3, którą utworzyłeś dla Kopii zapasowej.

     - **Identyfikator klucza dostępu**

       Identyfikator klucza (sekwencja znaków alfanumerycznych) uzyskałeś podczas tworzenia konta użytkownika IAM do pracy z instancją magazynu komory S3.

       Pole jest dostępne, jeśli w komorze S3 wybrałeś bazę danych RDS.

     - **Tajny klucz**

       Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

       Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

       Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

   - Dla Microsoft Azure:

     - **Nazwa konta magazynu Azure**

       Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

     - **ID subskrypcji Azure**

       Subskrypcję utworzyłeś na portalu Azure.

     - **Hasło Azure**

       Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

       Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

- **ID aplikacji Azure**

  Ten ID aplikacji utworzyłeś na portalu Azure.

  Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **Nazwa serwera Azure SQL**

  Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

- **Grupa zasobów serwera Azure SQL**

  Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

- **Klucz dostępu do magazynu Azure**

  Dostępne we właściwościach Twojego konta magazynu, w sekcji Klucze dostępu. Możesz użyć dowolnego klucza (key1 lub key2).

W celu przywrócenia danych Serwera administracyjnego w trybie interaktywnym:

1. Uruchom narzędzie klbackup znajdujące się w folderze instalacyjnym Kaspersky Security Center. Uruchom narzędzie z tego samego konta, którego użyłeś do zainstalowania Serwera administracyjnego. Zalecamy uruchomienie narzędzia na nowo zainstalowanym Serwerze administracyjnym.

   Zostanie uruchomiony Kreator tworzenia kopii zapasowej i przywracania.

2. W pierwszym oknie kreatora wybierz **Przywróć dane Serwera administracyjnego**, i kliknij **Dalej**.

   Jeśli wybierzesz opcję **Przywróć lub wykonaj kopię zapasową jedynie certyfikatu Serwera administracyjnego**, zostanie przywrócony tylko certyfikat i klucz prywatny Serwera administracyjnego.

   Po uruchomieniu narzędzia klbackup na nieaktywnym węźle klastra trybu failover zostaniesz poproszony o wybranie jednej z opcji: określenie certyfikatu Serwera administracyjnego lub automatyczne pobranie danych z Serwera administracyjnego.

3. W oknie **Przywróć ustawienia**:

   - Wskaż folder, który zawiera kopię zapasową danych Serwera administracyjnego.

     Jeśli pracujesz w środowisku chmury, takim jak AWS lub Azure, określ adres magazynu. Musisz się także upewnić, że plik nosi nazwę backup.zip.

   - Określ hasło, które zostało wprowadzone podczas tworzenia kopii zapasowej danych.

     Podczas przywracania danych powinieneś określić to samo hasło, które wprowadziłeś podczas tworzenia kopii zapasowej. Jeśli po utworzeniu kopii zapasowej ścieżka do folderu współdzielonego uległa zmianie, sprawdź działanie zadań wykorzystujących przywrócone dane (zadania przywracania i zadania zdalnej instalacji). Jeśli jest to konieczne, zmodyfikuj ustawienia tych zadań. Podczas przywracania danych z pliku kopii zapasowej nikt nie może mieć dostępu do folderu współdzielonego Serwera administracyjnego. Konto, z poziomu którego uruchamiane jest narzędzie klbackup, musi mieć pełen dostęp do folderu współdzielonego.

4. Kliknij przycisk **Dalej**, aby przywrócić dane.

Tworzenie kopii zapasowej i przywracanie danych w trybie cichym

W celu utworzenia kopii zapasowej lub odzyskania danych Serwera administracyjnego w trybie cichym,

Uruchom narzędzie klbackup z żądanym zestawem przełączników z poziomu wiersza poleceń urządzenia, na którym jest zainstalowany Serwer administracyjny.

Flagi Agenta sieciowego nie są przywracane podczas korzystania z narzędzia klbackup. Należy ręcznie skonfigurować flagi Agenta sieciowego.

Instancja Serwera administracyjnego, na którym kopia zapasowa ma zostać przywrócona, musi korzystać z systemu DBMS tego samego typu. Wersja Serwera administracyjnego może być taka sama (z tą samą lub późniejszą łatą) lub nowsza.

Składnia wiersza poleceń narzędzia:

```
klbackup -path <backup path> [-linux_path <ścieżka do kopii zapasowej serwera SQL>][-node_cert <ścieżka do certyfikatu>] [-logfile <plik dziennika>] [-use_ts]|[-restore] [-password <hasło>] [-cert_only] [-online] [-migrate postgres]
```

Jeśli w wierszu polecenia narzędzia klbackup nie określono hasła, narzędzie zażąda wprowadzenie hasła interaktywnie.

Opisy przełączników:

- `-path <ścieżka do kopii zapasowej>`—Zapisuje informacje w określonym folderze kopii zapasowej, lub używa danych z folderu zawierającego kopię zapasową do ich przywrócenia (wymagany parametr).

  Konto serwera bazy danych i narzędzie klbackup powinny mieć uprawnienia do zmiany danych w folderze zawierającym kopię zapasową.

- `-linux_path <ścieżka do kopii zapasowej serwera SQL>`—Ścieżka lokalna do folderu z danymi kopii zapasowej dla SQL Server w systemie Linux.

  Konto serwera bazy danych i narzędzie klbackup powinny mieć uprawnienia do zmiany danych w folderze zawierającym kopię zapasową serwera SQL.

- `-node_cert <ścieżka do certyfikatu>`—Plik certyfikatu serwera do konfigurowania nieaktywnego węzła klastra trybu failover po odzyskaniu. Jeśli nie zostanie ustawiony, zostanie automatycznie pobrany z Serwera.

  Podczas uruchamiania narzędzia klbackup na nieaktywnym węźle klastra trybu failover należy użyć tego klucza, aby określić ścieżkę do certyfikatu serwera.

- `-logfile <plik raportu>`—Zapisuje raport dotyczący tworzenia kopii zapasowej i przywracania danych Serwera administracyjnego.

- `-use_ts`—Podczas zapisywania danych kopiuje informacje do folderu zawierającego kopię zapasową, do podfolderu o nazwie w formacie `klbackup YYYY-MM-DD # HH-MM-SS`, zawierającego bieżącą datę i godzinę operacji w formacie UTC. Jeśli klucz nie został określony, informacje są zapisywane w głównym folderze folderu zawierającego kopię zapasową.

  Podczas próby zapisu informacji do folderu, w którym już znajduje się kopia zapasowa, zostaje wyświetlona wiadomość o błędzie. Żadne informacje nie zostaną zaktualizowane.

Dostępność klucza `-use_ts` pozwala zachować archiwum danych Serwera administracyjnego. Na przykład jeśli klucz `-path` wskazuje folder `C:\KLBackups`, wówczas folder `klbackup 2022/6/19 # 11-30-18` przechowuje informacje o stanie Serwera administracyjnego na dzień 19 czerwca 2022 roku, godzina 11:30:18.

- `-restore`—przywraca dane Serwera administracyjnego. Przywracanie danych odbywa się w oparciu o informacje znajdujące się w folderze zawierającym kopię zapasową. Jeśli żaden klucz nie jest dostępny, kopie zapasowe danych są tworzone w folderze zawierającym kopię zapasową.

- `-password <hasło>`—Hasło chroniące poufne dane.

  Zapomnianego hasła nie można odzyskać. Nie ma wymagań dotyczących hasła. Długość hasła jest nieograniczona i możliwa jest również długość zerowa (brak hasła).

  Podczas przywracania danych powinieneś określić to samo hasło, które wprowadziłeś podczas tworzenia kopii zapasowej. Jeśli po utworzeniu kopii zapasowej ścieżka do folderu współdzielonego uległa zmianie, sprawdź działanie zadań wykorzystujących przywrócone dane (zadania przywracania i zadania zdalnej instalacji). Jeśli jest to konieczne, zmodyfikuj ustawienia tych zadań. Podczas przywracania danych z pliku kopii zapasowej nikt nie może mieć dostępu do folderu współdzielonego Serwera administracyjnego. Konto, z poziomu którego uruchamiane jest narzędzie klbackup, musi mieć pełen dostęp do folderu współdzielonego. Zalecamy uruchomienie narzędzia na nowo zainstalowanym Serwerze administracyjnym.

- `-cert_only`—zapisz lub odzyskaj tylko certyfikat i klucz prywatny Serwera administracyjnego.

  Ta flaga może być użyteczna podczas wykonywania migracji z Serwera administracyjnego Kaspersky Security Center Windows do Serwera administracyjnego Kaspersky Security Center Linux. Możesz również migrować zarządzane urządzenia pomiędzy Serwerami administracyjnymi Kaspersky Security Center Linux, a także pomiędzy Serwerami administracyjnymi Kaspersky Security Center Windows.

- `-online`—Utwórz kopię zapasową danych Serwera administracyjnego, tworząc migawkę woluminu, aby zminimalizować czas offline Serwera administracyjnego. Jeśli używasz narzędzia do odzyskiwania danych, ta opcja jest ignorowana. Nie należy używać tej flagi podczas tworzenia kopii zapasowej w celu migracji do innego systemu DBMS.

- - archiwum 0—Zachowaj dane serwera w postaci zwykłych plików. Domyślnie (`-archive 1`), dane serwera są przechowywane w pliku archiwum.

- `-migrate mysql`—Utwórz kopię zapasową danych Serwera administracyjnego przechowywanych w bazie danych SQL Server, która jest zgodna z MySQL (w tym MariaDB). Możesz przywrócić dane z kopii zapasowej do MySQL.

- `-migrate postgres`—Utwórz kopię zapasową danych Serwera administracyjnego przechowywanych w bazie danych SQL Server, która jest zgodna z PostgreSQL i Postgres Pro. Możesz przywrócić dane z kopii zapasowej do PostgreSQL lub Postgres Pro. Użyj tej flagi, jeśli wykonujesz migrację do Kaspersky Security Center Linux przy użyciu kopii zapasowej danych Serwera administracyjnego.

  Ta opcja będzie dostępna po zwróceniu się do pomocy technicznej Kaspersky i zainstalowaniu poprawki 15.1.0.20748-pf2 dla Serwera administracyjnego lub aktualizacji do Kaspersky Security Center Windows w wersji 15.1.0.22239.

Korzystanie z narzędzia klbackup w celu przełączania zarządzanych urządzeń pod kontrolą innego Serwera administracyjnego

Narzędzie klbackup umożliwia przełączanie zarządzanych urządzeń pod zarządzanie innego Serwera administracyjnego. Możesz zmienić Serwer administracyjny Kaspersky Security Center Windows na Serwer administracyjny Kaspersky Security Center Linux, korzystając z narzędzia klbackup podczas wykonywania migracji. Możesz również migrować zarządzane urządzenia pomiędzy Serwerami administracyjnymi Kaspersky Security Center Linux, a także pomiędzy Serwerami administracyjnymi Kaspersky Security Center Windows.

Aby przełączyć zarządzane urządzenia pod zarządzanie innego Serwera administracyjnego przy użyciu narzędzia klbackup:

1. Na poprzednim urządzeniu utwórz kopię zapasową certyfikatu Serwera administracyjnego i klucza prywatnego.

   Możesz utworzyć kopię zapasową na jeden z następujących sposobów:

   - Za pomocą interfejsu narzędzia klbackup (tylko dla Serwera administracyjnego Kaspersky Security Center Windows)

     Uruchom narzędzie klbackup znajdujące się w folderze instalacyjnym Kaspersky Security Center, a następnie utwórz kopię zapasową, korzystając z opcji **Przywróć lub wykonaj kopię zapasową jedynie certyfikatu Serwera administracyjnego**.

   - Za pomocą wiersza poleceń (dla Serwerów administracyjnych Kaspersky Security Center Windows i Kaspersky Security Center Linux w wersji 15.1 lub nowszej)

     Uruchom narzędzie klbackup z kluczem `-cert_only` z poziomu wiersza poleceń, aby utworzyć kopię zapasową certyfikatu i klucza prywatnego Serwera administracyjnego:

     ```
     klbackup -path <ścieżka do kopii zapasowej certyfikatu Serwera administracyjnego> -cert_only
     ```

2. Na poprzednim urządzeniu odłącz Serwer administracyjny od sieci.

3. Przypisz urządzeniu ten sam adres za pomocą innego Serwera administracyjnego.

   Nowy Serwer administracyjny może mieć przypisaną nazwę NetBIOS, FQDN i statyczny adres IP. Zależy to od tego, który adres Serwera administracyjnego został ustawiony w pakiecie instalacyjnym Agenta sieciowe w momencie instalacji Agenta sieciowego. Alternatywnie można użyć adresu połączenia, który określa Serwer administracyjny, z którym łączy się Agent sieciowy (możesz uzyskać ten adres na zarządzanych urządzeniach korzystając z narzędzia klnagchk).

4. Na urządzeniu z innym serwerem administracyjnym przywróć certyfikat Serwera administracyjnego i klucz prywatny z kopii zapasowej.

   Możesz przywrócić kopię zapasową na jeden z następujących sposobów:

   - Za pomocą interfejsu narzędzia klbackup (tylko dla Serwera administracyjnego Kaspersky Security Center Windows)

     Uruchom narzędzie klbackup, a następnie przywróć kopię zapasową, korzystając z opcji **Przywróć lub wykonaj kopię zapasową jedynie certyfikatu Serwera administracyjnego**.

   - Za pomocą wiersza poleceń (dla Serwerów administracyjnych Kaspersky Security Center Windows i Kaspersky Security Center Linux w wersji 15.1 lub nowszej)

     Uruchom narzędzie klbackup z kluczem `-cert_only` z poziomu wiersza poleceń, aby przywrócić kopię zapasową certyfikatu i klucza prywatnego Serwera administracyjnego:

```
klbackup -path < ścieżka do kopii zapasowej certyfikatu Serwera administracyjnego >
-restore -cert_only
```

Zarządzane urządzenia są przekazywane pod kontrolę innego Serwera administracyjnego. Możesz przejść do tego Serwera administracyjnego i sprawdzić, czy zarządzane urządzenia są widoczne w sieci oraz czy Agent sieciowy jest na nich zainstalowany i uruchomiony (wartość *Tak* w kolumnach **Widoczny**, **Agent sieciowy jest zainstalowany** i **Agent sieciowy jest uruchomiony**).

Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego podczas korzystania z MySQL lub MariaDB

Możesz użyć kopii zapasowej danych do migracji danych Serwera administracyjnego z Kaspersky Security Center Windows pod zarządzanie Kaspersky Security Center Linux. Migracja przy użyciu kopii zapasowej danych Serwera administracyjnego jest obsługiwana wyłącznie w przypadku migracji do Kaspersky Security Center Linux 15.2 lub nowszej wersji z dowolnej obsługiwanej wersji Kaspersky Security Center dla systemu Windows.

Jeśli używasz MySQL lub MariaDB jako systemu DBMS dla Kaspersky Security Center Windows i Kaspersky Security Center Linux, parametr `lower_case_table_names` musi być taki sam dla bieżącego i nowego systemu DBMS. W przeciwnym wypadku dane Serwera administracyjnego zostaną nieprawidłowo zmigrowane.

Przed utworzeniem kopii zapasowej danych Serwera administracyjnego w Kaspersky Security Center Windows należy sprawdzić wartość parametru `lower_case_table_names`. Jeżeli ten parametr nie zostanie określony wcześniej podczas instalacji systemu DBMS, użyta zostanie wartość domyślna parametru. Wartość domyślna parametru `lower_case_table_names` w systemie Windows wynosi `1`.

Podczas instalacji MySQL lub MariaDB dla Kaspersky Security Center Linux należy ustawić parametr `lower_case_table_names` na taką samą wartość, jaka została określona dla tego parametru w systemie Windows, korzystając z instrukcji ze strony internetowej MySQL. Jeżeli nie określisz tego parametru, używana jest wartość domyślna parametru. W systemach operacyjnych opartych na systemie Linux wartość domyślna parametru `lower_case_table_names` jest inna niż domyślna wartość w systemie Windows.

Jeśli chcesz zainstalować MySQL 8.0, określenie parametru `lower_case_table_names` zgodnie z tą instrukcją może nie zadziałać. W takim przypadku należy najpierw zainstalować MySQL 5.7, określić parametr `lower_case_table_names` za pomocą instrukcji, a następnie wykonać uaktualnienie MySQL 5.7 do wersji MySQL 8.0. Jeżeli parametr `lower_case_table_names` nie jest zgodny z bieżącym i nowym systemem DBMS, dane Serwera administracyjnego zostaną przywrócone nieprawidłowo.

Optymalizacja tworzenia kopii zapasowej i przywracanie danych Serwera administracyjnego

Aby zoptymalizować tworzenie kopii zapasowych i przywracanie danych Serwera administracyjnego w celu skrócenia czasu przestoju Serwera administracyjnego, wykonaj jedną z następujących czynności:

- Włącz opcję **Użyj migawki systemu plików do tworzenia kopii zapasowej danych**.

  Więcej szczegółów znajdziesz w poniższym artykule: Korzystanie z migawki systemu plików w celu skrócenia czasu tworzenia kopii zapasowej.

- Skonfiguruj następujące flagi:

Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na katalog za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\ Kaspersky Lab\ Kaspersky Security Center.

- `KLSRV_BKP_FILES`—Dzieli plik bazy danych na wiele mniejszych plików, od 2 do 32. Może to przyspieszyć tworzenie kopii zapasowych i przywracanie danych, jeśli wydajność systemu DBMS jest ograniczona przez procesor.

  Na przykład:

  ```
  klscflag -fset -pv klserver -n KLSRV_BKP_FILES -t d -v 2
  ```

- `KLSRV_BKP_BACKUP_EXTRA_PARS`—Określa parametry `COMPRESSION` i `MAXTRANSFERSIZE`. Może to przyspieszyć tworzenie kopii zapasowych, jeśli wydajność systemu DBMS jest ograniczona przez wejście/wyjście pliku.

  Na przykład:

  ```
  klscflag -fset -pv klserver -n KLSRV_BKP_BACKUP_EXTRA_PARS -t s -v "COMPRESSION,
  MAXTRANSFERSIZE = 4194304"
  ```

- `KLSRV_BKP_RESTORE_EXTRA_PARS`—Określa parametr `MAXTRANSFERSIZE`. Może to przyspieszyć przywracanie danych, jeśli wydajność systemu DBMS jest ograniczona przez wejście/wyjście pliku.

  Na przykład:

  ```
  klscflag -fset -pv klserver -n KLSRV_BKP_RESTORE_EXTRA_PARS -t s -v "MAXTRANSFERSIZE
  = 4194304"
  ```

- `KLSRV_BKP_ONLINE_DB_BACKUP`—usuwa przestoje Serwera administracyjnego podczas tworzenia kopii zapasowej. Dostępne tylko dla następujących systemów DBMS:

  - PostgreSQL lub Postgres Pro.
  - SQL Server z modelem pełnego odzyskiwania danych. Więcej informacji można znaleźć w dokumentacji SQL Server. Po włączeniu flagi `KLSRV_BKP_ONLINE_DB_BACKUP` system SQL Server DBMS zostanie automatycznie przełączony na model pełnego odzyskiwania.

  Na przykład:

  ```
  klscflag.exe -fset -pv klserver -n KLSRV_BKP_ONLINE_DB_BACKUP -t d -v 1
  ```

Przenoszenie Serwera administracyjnego na inne urządzenie

Jeśli chcesz użyć Serwera administracyjnego na nowym urządzeniu, możesz je przenieść w jeden z następujących sposobów:

- Przenieś Serwer administracyjny i serwer bazy danych na nowe urządzenie (serwer bazy danych może być zainstalowany na nowym urządzeniu wraz Serwerem administracyjnym, lub na innym urządzeniu).
- Zachowaj serwer bazy danych na poprzednim urządzeniu i przenieś tylko Serwer administracyjny na nowe urządzenie.

W celu przeniesienia Serwera administracyjnego na nowe urządzenie:

1. Na poprzednim urządzeniu utwórz kopię zapasową danych Serwera administracyjnego.

   W tym celu możesz uruchomić zadanie tworzenia kopii zapasowej danych poprzez Konsolę administracyjną lub uruchomić narzędzie klbackup.

Jeśli używasz SQL Server jako DBMS dla Serwera administracyjnego, możesz migrować dane z SQL Server do MySQL lub MariaDB DBMS. Aby to zrobić, uruchom narzędzie klbackup w trybie interaktywnym, aby utworzyć kopię zapasową danych. Włącz opcję **Wykonaj migrację do formatu MySQL/MariaDB** w oknie **Ustawienia kopii zapasowej** kopii zapasowej Kreatora kopii zapasowych i przywracania. Kaspersky Security Center utworzy kopię zapasową kompatybilną z MySQL i MariaDB. Następnie możesz przywrócić dane z kopii zapasowej do MySQL lub MariaDB.

Możesz również włączyć opcję **Wykonaj migrację do formatu Azure** jeśli chcesz migrować dane z SQL Server do Azure SQL DBMS.

2. Na poprzednim urządzeniu odłącz Serwer administracyjny od sieci.

3. Wybierz nowe urządzenie, na którym chcesz zainstalować Serwer administracyjny. Upewnij się, że sprzęt i oprogramowanie na wybranym urządzeniu spełniają wymagania Serwera administracyjnego, Konsoli administracyjnej i Agenta sieciowego. Sprawdź również, czy dostępne są porty używane na Serwerze administracyjnym.

4. Przypisz ten sam adres do nowego urządzenia.

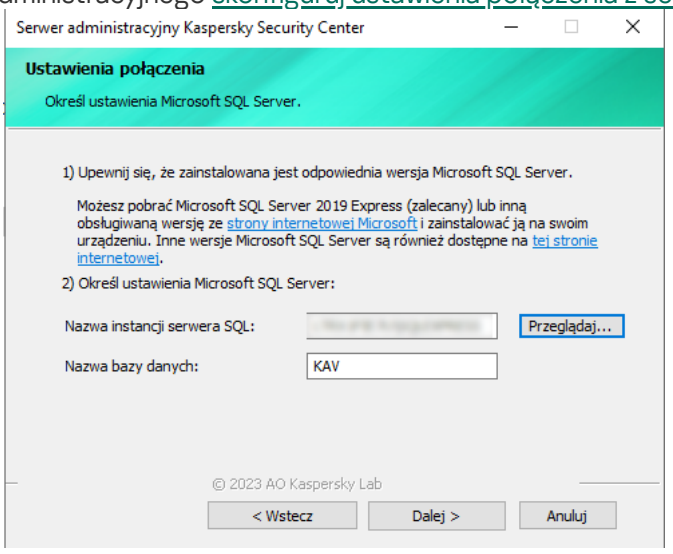
   Nowy Serwer administracyjny może mieć przypisaną nazwę NetBIOS, FQDN i statyczny adres IP. Zależy to od tego, który adres Serwera administracyjnego został ustawiony w pakiecie instalacyjnym Agenta sieciowe w momencie instalacji Agenta sieciowego. Alternatywnie można użyć adresu połączenia, który określa Serwer administracyjny, z którym łączy się Agent sieciowy (możesz uzyskać ten adres na zarządzanych urządzeniach korzystając z narzędzia klnagchk).

5. W razie konieczności, na innym urządzeniu, zainstaluj system zarządzania bazą danych (DBMS), którego będzie używał Serwer administracyjny.

   Bazę danych można zainstalować na nowym urządzeniu razem z Serwerem administracyjnym lub na innym urządzeniu. Upewnij się, że urządzenia spełnia wymagania sprzętowe i programowe. Kiedy wybierasz DBMS, weź pod uwagę liczbę urządzeń obsługiwanych przez Serwer administracyjny.

6. Uruchom instalację Serwera administracyjnego na nowym urządzeniu.

7. Podczas instalacji Serwera administracyjnego skonfiguruj ustawienia połączenia z serwerem bazy danych.



Przykład okna Ustawienia połączenia dla Microsoft SQL Server

W zależności od tego, gdzie chcesz zlokalizować serwer bazy danych, wykonaj jedną z następujących czynności:

- **Zachowaj serwer bazy danych na poprzednim urządzeniu**

  1. Kliknij przycisk **Przeglądaj** obok pola **Nazwa instancji serwera SQL**, a następnie wybierz poprzednią nazwę urządzenia z wyświetlonej listy.

     Pamiętaj, że poprzednie urządzenie musi być dostępne do połączenia z nowym Serwerem administracyjnym.

  2. Wprowadź poprzednią nazwę bazy danych w polu **Nazwa bazy danych**.

- **Przenieś bazę danych na inne urządzenie**

  1. Kliknij przycisk **Przeglądaj** obok pola **Nazwa instancji serwera SQL**, a następnie wybierz nazwę urządzenia z wyświetlonej listy.

  2. Wprowadź nową nazwę bazy danych w polu **Nazwa bazy danych**.

     Należy pamiętać, że nazwa nowej bazy danych musi być zgodna z nazwą bazy danych z poprzedniego urządzenia. Nazwy baz danych muszą być identyczne, abyś mógł korzystać z kopii zapasowej Serwera administracyjnego. Domyślna nazwa bazy danych to *KAV*.

8. Po zakończeniu instalacji odzyskaj dane Serwera administracyjnego na nowym urządzeniu za pomocą narzędzia klbackup.

   Jeśli używasz programu SQL Server jako DBMS na poprzednich i nowych urządzeniach, pamiętaj, że wersja programu SQL Server zainstalowana na nowym urządzeniu musi być taka sama lub nowsza niż wersja programu SQL Server zainstalowana na poprzednim urządzeniu. W przeciwnym razie nie będzie możliwe odzyskanie danych Serwera administracyjnego na nowym urządzeniu.

9. Otwórz Konsolę administracyjną do nawiązywania połączenia z Serwerem administracyjnym.
10. Sprawdź, czy wszystkie zarządzane urządzenia są podłączone do Serwera administracyjnego.
11. Odinstaluj Serwer administracyjny i serwer bazy danych z poprzedniego urządzenia.

Możesz także użyć Kaspersky Security Center Web Console do przeniesienia Serwera administracyjnego i serwera bazy danych na inne urządzenie.

Unikanie konfliktów między kilkoma Serwerami administracyjnymi

Jeśli w sieci posiadasz więcej niż jeden Serwer administracyjny, mogą one widzieć te same urządzenia klienckie. Może to być na przykład spowodowane zainstalowaniem przez Serwer administracyjny aplikacji, która została już zainstalowana przez inny Serwer administracyjny, a także innymi konfliktami. Aby zapobiec instalacji aplikacji na urządzeniu zarządzanym przez inny Serwer administracyjny, należy włączyć opcję **Zainstaluj tylko na urządzeniach zarządzanych przez ten Serwer administracyjny** we właściwościach zadania *Zdalna instalacja aplikacji*.

Jeśli włączysz opcję **Zainstaluj tylko na urządzeniach zarządzanych przez ten Serwer administracyjny**, a następnie uruchomisz zadanie *Zdalna instalacja aplikacji*, zostanie wykonane sprawdzenie w celu ustalenia, czy urządzenia są zarządzane przez inny Serwer administracyjny. W przypadku urządzeń zarządzanych przez inny Serwer administracyjny wartość atrybutu **Zarządzane przez inny Serwer administracyjny** zostanie ustawiona na `true`. Zadanie *Zdalna instalacja aplikacji* nie zostanie zastosowane do tych urządzeń.

Wartości atrybutu **Zarządzane przez inny Serwer administracyjny** są wyświetlane w kolumnie **Zarządzane przez inny Serwer administracyjny** na liście zarządzanych urządzeń i liście nieprzypisanych urządzeń.

Możesz także użyć właściwości **Zarządzane przez inny Serwer administracyjny** jako kryterium dla:

- Wyszukiwania urządzeń
- Wybory urządzeń
- Reguły przenoszenia urządzeń
- Reguł automatycznego znakowania

Aby zresetować atrybut Zarządzane przez inny Serwer administracyjny:

1. W menu głównym Kaspersky Security Center Web Console przejdź do **Wykrywanie i wdrażanie** → **Urządzenia nieprzypisane**.
2. Wybierz wymagane urządzenie, a następnie kliknij przycisk **Usuń atrybut Zarządzane przez inny Serwer administracyjny**.

Atrybut **Zarządzane przez inny Serwer administracyjny** został zresetowany.

Zarządzanie grupami administracyjnymi

Dostępne są tu informacje o sposobie zarządzania grupami administracyjnymi.

Na grupach administracyjnych możesz wykonać następujące akcje:

- Dodać do grup administracyjnych dowolną liczbę grup zagnieżdżonych z jakiegokolwiek poziomu hierarchii.
- Dodać urządzenia do grup administracyjnych.
- Zmienić hierarchię grup administracyjnych przez przeniesienie pojedynczych urządzeń i całych grup do innych grup.
- Usunąć grupy zagnieżdżone i urządzenia z grup administracyjnych.
- Dodać podrzędne i wirtualne Serwery administracyjne do grup administracyjnych.
- Przenieść urządzenia z grup administracyjnych Serwera administracyjnego do grup innego Serwera.
- Wskazać aplikacje Kaspersky, które będą automatycznie instalowane na urządzeniach znajdujących się w grupie.

Możesz wykonać te działania tylko wtedy, gdy posiadasz uprawnienie **Modyfikacja** w obszarze **Zarządzanie grupami administracyjnymi** dla grup administracyjnych, którymi chcesz zarządzać (lub dla Serwera administracyjnego, do którego te grupy należą).

Tworzenie grup administracyjnych

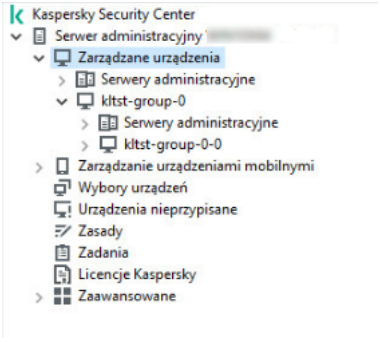
Hierarchia grup administracyjnych jest tworzona w oknie głównym aplikacji Kaspersky Security Center, w folderze **Zarządzane urządzenia**. Grupy administracyjne są wyświetlane w drzewie konsoli jako foldery (zobacz rysunek poniżej).

Natychmiast po zainstalowaniu Kaspersky Security Center, folder **Zarządzane urządzenia** będzie zawierał tylko pusty folder **Serwery administracyjne**.

Ustawienia interfejsu użytkownika określają, czy folder **Serwery administracyjne** jest wyświetlany w drzewie konsoli. Aby wyświetlić ten folder, na pasku menu wybierz **Widok** → **Konfiguracja interfejsu** i w otwartym oknie **Konfiguracja interfejsu** zaznacz pole **Wyświetl podrzędne Serwery administracyjne**.

Podczas tworzenia hierarchii grup administracyjnych możesz dodać urządzenia i maszyny wirtualne do folderu **Zarządzane urządzenia**, a także możesz dodać zagnieżdżone grupy. Możesz dodać podrzędne i wirtualne Serwery administracyjne do folderu **Serwery administracyjne**.

Tak jak w folderze **Zarządzane urządzenia**, każda utworzona grupa początkowo zawiera tylko pusty folder **Serwery administracyjne**, który służy do pracy z podrzędnymi i wirtualnymi Serwerami administracyjnymi tej grupy. Informacje o zasadach i zadaniach dla tej grupy i jej urządzeniach wyświetlane są na zakładkach z odpowiednimi nazwami w obszarze roboczym tej grupy.



Wyświetlanie hierarchii grup administracyjnych

W celu utworzenia grupy administracyjnej:

1. W drzewie konsoli rozwiń folder **Zarządzane urządzenia**.
2. Jeśli chcesz utworzyć podgrupę w istniejącej grupie administracyjnej, w folderze **Zarządzane urządzenia** wybierz podfolder odpowiadający grupie, do której chcesz dodać nową grupę administracyjną.

   Jeśli tworzysz nową grupę administracyjną na najwyższym poziomie hierarchii, możesz pominąć ten krok.
3. Uruchom tworzenie grupy administracyjnej w jeden z następujących sposobów:
   - Korzystając z polecenia **Nowa** → **Grupa** z menu kontekstowego.
   - Klikając przycisk **Nowa grupa**, znajdujący się w obszarze roboczym okna głównego aplikacji, na zakładce **Urządzenia**.
4. W oknie **Nazwa grupy**, które zostanie otwarte, wprowadź nazwę grupy i kliknij **OK**.

W drzewie konsoli pojawi się nowy folder grupy administracyjnej o określonej nazwie.

Aplikacja umożliwia tworzenie hierarchii grup administracyjnych opartej na strukturze Active Directory lub na strukturze sieci domeny. Strukturę grup możesz również utworzyć z pliku tekstowego.

W celu utworzenia struktury grup administracyjnych:

1. W drzewie konsoli wybierz folder **Zarządzane urządzenia**.
2. Z menu kontekstowego folderu **Zarządzane urządzenia** wybierz **Wszystkie zadania → Nowa struktura grupy**.

Zostanie uruchomiony Kreator struktury nowej grupy administracyjnej. Postępuj zgodnie z instrukcjami kreatora.

Przenoszenie grup administracyjnych

Możliwe jest przenoszenie zagnieżdżonych grup administracyjnych w obrębie hierarchii grup.

Grupa administracyjna jest przenoszona wraz z grupami zagnieżdżonymi, podrzędnymi Serwerami administracyjnymi, urządzeniami, zasadami grupy i zadaniami. System zastosuje do grupy wszystkie ustawienia odpowiadające jej nowej pozycji w hierarchii grup administracyjnych.

Nazwa grupy musi być unikatowa w obrębie tego poziomu hierarchii. Jeżeli w folderze, do którego przenosisz grupę administracyjną, istnieje już grupa o takiej nazwie, powinieneś zmienić nazwę przenoszonej grupy. Jeżeli nie zmienisz nazwy przenoszonej grupy, do jej nazwy zostanie automatycznie dodany przyrostek **(<kolejny numer>)**, na przykład: **(1)**, **(2)**.

Nie można zmienić nazwy grupy **Zarządzane urządzenia**, ponieważ jest on wbudowanym elementem Konsoli administracyjnej.

W celu przeniesienia grupy do innego folderu w drzewie konsoli:

1. Wybierz grupę, którą chcesz przenieść.
2. Wykonaj jedną z poniższych czynności:
   - Przenieś grupę, korzystając z menu kontekstowego:
     1. Wybierz **Wytnij** z menu kontekstowego grupy.
     2. Wybierz **Wklej** z menu kontekstowego grupy administracyjnej, do której chcesz przenieść wybraną grupę.
   - Przenieś grupę, korzystając z menu okna głównego:
     a. Z głównego menu wybierz **Akcja → Wytnij**.
     b. Wybierz z drzewa konsoli grupę administracyjną, do której chcesz przenieść wybraną grupę.
     c. Z głównego menu wybierz **Akcja → Wklej**.
   - Przenieść grupę do innej w drzewie konsoli, używając myszy.

Usuwanie grup administracyjnych

Możesz usunąć grupę administracyjną, jeżeli nie zawiera ona podrzędnych Serwerów administracyjnych, grup zagnieżdżonych lub urządzeń klienckich oraz gdy nie utworzono dla niej zasad lub zadań grupowych.

Przed usunięciem grupy administracyjnej należy usunąć z tej grupy wszystkie podrzędne Serwery administracyjne, grupy zagnieżdżone i urządzenia klienckie.

W celu usunięcia grupy:

1. Z drzewa konsoli wybierz grupę administracyjną.
2. Wykonaj jedną z poniższych czynności:
   - Wybierz **Usuń** z menu kontekstowego grupy.
   - Z głównego menu aplikacji wybierz **Akcja** → **Usuń**.
   - Wciśnij klawisz **DELETE**.

Automatyczne tworzenie struktury grup administracyjnych

Kaspersky Security Center umożliwia tworzenie struktury grup administracyjnych przy użyciu kreatora tworzenia hierarchii grup.

Kreator tworzy strukturę grup administracyjnych w oparciu o następujące dane:

- Struktury grup roboczych i domen Windows
- Struktury grup Active Directory
- Zawartość pliku tekstowego utworzonego ręcznie przez administratora

Podczas tworzenia pliku tekstowego muszą być spełnione następujące wymagania:

- Nazwa każdej nowej grupy musi znajdować się w nowej linii, a separator musi rozpoczynać się pustą linią. Puste linie są ignorowane.

  Na przykład:

  Office 1

  Office 2

  Office 3

  W grupie docelowej zostaną utworzone trzy grupy pierwszego poziomu hierarchii.

- Nazwę grupy zagnieżdżonej należy poprzedzić ukośnikiem (/).

  Na przykład:

  Office 1/Division 1/Department 1/Group 1

  W grupie docelowej zostaną utworzone cztery podgrupy zagnieżdżone w sobie.

- Aby utworzyć kilka grup zagnieżdżonych na tym samym poziomie hierarchii, należy określić "pełną ścieżkę do grupy".

  Na przykład:

  Office 1/Division 1/Department 1

  Office 1/Division 2/Department 1

  Office 1/Division 3/Department 1

  Office 1/Division 4/Department 1

  Jedna grupa pierwszego poziomu hierarchii Office 1 zostanie utworzona w grupie docelowej; grupa ta będzie zawierać cztery grupy zagnieżdżone tego samego poziomu hierarchii: "Division 1", "Division 2", "Division 3" i "Division 4". Każda z tych grup będzie zawierać grupę "Department 1".

Utworzenie hierarchii grup administracyjnych poprzez kreator nie ma wpływu na integralność sieci: zamiast zastępowania istniejących grup, dodawane są nowe grupy. Urządzenie klienckie nie może zostać przydzielone do grupy administracyjnej drugi raz, ponieważ urządzenie jest usuwane z grupy **Urządzenia nieprzypisane** po przeniesieniu go do grupy administracyjnej.

Jeśli podczas tworzenia struktury grupy administracyjnej urządzenie nie zostało umieszczone w grupie **Urządzenia nieprzypisane** (zostało zamknięte lub odłączone od sieci), nie zostanie automatycznie przeniesione do grupy administracyjnej. Urządzenia można dodać do grup administracyjnych ręcznie po zakończeniu działania kreatora.

W celu uruchomienia automatycznego tworzenia struktury grup administracyjnych:

1. W drzewie konsoli kliknij folder **Zarządzane urządzenia**.
2. Z menu kontekstowego folderu **Zarządzane urządzenia** wybierz **Wszystkie zadania → Nowa struktura grupy**.

   Zostanie uruchomiony Kreator struktury nowej grupy administracyjnej. Postępuj zgodnie z instrukcjami kreatora.

Automatyczna instalacja aplikacji na urządzeniach w grupie administracyjnej

Możesz określić, które pakiety instalacyjne mają być użyte do automatycznej instalacji zdalnej aplikacji Kaspersky na urządzeniach klienckich w grupie administracyjnej.

W celu skonfigurowania automatycznej instalacji aplikacji na nowych urządzeniach w grupie administracyjnej:

1. W drzewie konsoli wybierz żądaną grupę administracyjną.
2. Otwórz okno właściwości tej grupy administracyjnej.
3. W panelu **Sekcje** wybierz **Automatyczna instalacja**, a w obszarze roboczym wybierz pakiety instalacyjne aplikacji, które mają zostać zainstalowane na nowych urządzeniach.
4. Kliknij **OK**.

Zadania grupowe zostaną utworzone. Te zadania są uruchamiane na urządzeniach klienckich natychmiast po dodaniu ich do grupy administracyjnej.

W przypadku, gdy do automatycznej instalacji wybrano tylko niektóre pakiety instalacyjne danej aplikacji, zadanie instalacji zostanie utworzone tylko dla najnowszej wersji aplikacji.

Zarządzanie urządzeniami klienckimi

Ta sekcja zawiera informacje na temat pracy z urządzeniami klienckimi.

Łączenie urządzenia klienckiego z Serwerem administracyjnym

Połączenie między urządzeniem klienckim a Serwerem administracyjnym jest nawiązywane poprzez Agenta sieciowego zainstalowanego na urządzeniu klienckim.

Po połączeniu urządzenia klienckiego z Serwerem administracyjnym wykonywane są następujące działania:

- Automatyczna synchronizacja danych:
  - Synchronizacja listy aplikacji zainstalowanych na urządzeniu klienckim.
  - Synchronizacja zasad, ustawień aplikacji, zadań oraz ustawień zadań.
- Odebranie aktualnych informacji o stanie aplikacji, wykonywaniu zadań i statystyk działania aplikacji przez Serwer administracyjny.
- Dostarczenie informacji o zdarzeniach na Serwer administracyjny w celu ich przetworzenia.

Automatyczna synchronizacja danych przeprowadzana jest regularnie zgodnie z ustawieniami Agenta sieciowego (przykładowo co piętnaście minut). Możesz określić ten czas ręcznie.

Informacja o zdarzeniu jest dostarczana do Serwera administracyjnego natychmiast po jego wystąpieniu.

Jeżeli Serwer administracyjny jest zdalny (znajduje się poza siecią firmową), urządzenia klienckie mogą łączyć się z nim przez internet.

Aby urządzenia klienckie łączyły się z Serwerem administracyjnym przez Internet, muszą być spełnione następujące warunki:

- Zdalny Serwer administracyjny musi posiadać zewnętrzny adres IP, a port dla ruchu przychodzącego o numerze 13000 musi pozostać otwarty (dla połączenia z Agentami sieciowymi). Zalecane jest także otwarcie portu UDP o numerze 13000 (do odbierania powiadomień o zamknięciu urządzeń).

- Agenty sieciowe powinny zostać zainstalowane na urządzeniach.

- Podczas instalacji Agenta sieciowego na urządzeniach powinieneś określić zewnętrzny adres IP zdalnego Serwera administracyjnego. Jeżeli do instalacji wykorzystywany jest pakiet instalacyjny, zewnętrzny adres IP jest określany ręcznie we właściwościach tego pakietu instalacyjnego, na zakładce **Ustawienia**.

- Aby użyć zdalnego Serwera administracyjnego do zarządzania aplikacjami i zadaniami dla urządzenia, w oknie właściwości tego urządzenia, w sekcji **Ogólne** zaznacz pole **Nie odłączaj od Serwera administracyjnego**. Po zaznaczeniu tego pola, należy zaczekać, aż Serwer administracyjny zsynchronizuje się ze zdalnym urządzeniem. Liczba urządzeń klienckich mających stałe połączenie z Serwerem administracyjnym nie może przekraczać 300.

Aby zwiększyć wydajność zadań zainicjowanych przez zdalny Serwer administracyjny, możesz otworzyć na urządzeniu port o numerze 15000. W tym przypadku, aby uruchomić zadanie, Serwer administracyjny wysyła specjalny pakiet do Agenta sieciowego przez port 15000, bez oczekiwania na zakończenie synchronizacji z urządzeniem.

Kaspersky Security Center pozwala na takie skonfigurowanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym, dzięki któremu połączenie pozostanie aktywne po zakończeniu wszystkich operacji. Stałe połączenie jest wymagane w przypadkach, gdy konieczne jest monitorowanie stanu aplikacji w czasie rzeczywistym, a Serwer administracyjny nie może połączyć się z klientem z jakiegoś powodu (na przykład, połączenie jest chronione przez zaporę sieciową, otwieranie portów na urządzeniu klienckim nie jest dozwolone lub adres IP urządzenia klienckiego nie jest znany). Stałe połączenie między urządzeniem klienckim a Serwerem administracyjnym można nawiązać w oknie właściwości urządzenia, w sekcji **Ogólne**.

Stałe połączenie zalecamy nawiązywać z najważniejszymi urządzeniami. Całkowita liczba jednocześnie utrzymywanych połączeń przez Serwer administracyjny jest ograniczona do 300.

Przy ręcznej synchronizacji system korzysta z pomocniczej metody łączenia, gdzie połączenie jest inicjowane przez Serwer administracyjny. Przed nawiązaniem połączenia na urządzeniu klienckim należy otworzyć port UDP. Serwer administracyjny wysyła żądanie połączenia na port UDP urządzenia klienckiego. W odpowiedzi weryfikowany jest certyfikat Serwera administracyjnego. Jeśli certyfikat Serwera administracyjnego odpowiada kopii certyfikatu przechowywanej na urządzeniu klienckim, rozpoczynane jest nawiązywanie połączenia.

Ręczne uruchamianie synchronizacji jest również wykorzystywane do uzyskiwania aktualnych informacji o stanie aplikacji, wykonywaniu zadań i statystyk działania aplikacji.

Ręczne łączenie urządzenia klienckiego z Serwerem administracyjnym. Narzędzie klmover

Jeżeli chcesz ręcznie połączyć urządzenie klienckie z Serwerem administracyjnym, możesz użyć na urządzeniu klienckim narzędzia klmover.

Podczas instalacji Agenta sieciowego na urządzeniach klienckich narzędzie jest automatycznie kopiowane do folderu instalacyjnego Agenta sieciowego.

W celu ręcznego połączenia urządzenia klienckiego z Serwerem administracyjnym, korzystając z narzędzia klmover:

Na urządzeniu uruchom narzędzie klmover z poziomu wiersza poleceń.

Po uruchomieniu narzędzia klmover z poziomu wiersza poleceń, będzie ono mogło wykonać następujące akcje (w zależności od używanych parametrów):

- Nawiązać połączenie między Agentem sieciowym a Serwerem administracyjnym, używając określonych ustawień;
- Zapisać wyniki działania w dzienniku zdarzeń lub wyświetlić je na ekranie.

Narzędzia klmover nie można używać w przypadku urządzeń klienckich podłączonych do Serwera administracyjnego poprzez bramy połączeń. W przypadku takich urządzeń należy albo ponownie skonfigurować Agenta sieciowego, albo ponownie zainstalować Agenta sieciowego i określić bramę połączenia.

Składnia wiersza poleceń narzędzia:

```
klmover [-logfile <nazwa pliku>] [-address <adres serwera>] [-pn <numer portu>] [-ps
<numer portu SSL>] [-nossl] [-cert <ścieżka do pliku certyfikatu>] [-silent] [-dupfix]
[-virtserv] [-cloningmode]
```

Do uruchomienia narzędzia wymagane są uprawnienia administratora.

Opisy przełączników:

- `-logfile <nazwa pliku>`—Zapisuje wyniki działania narzędzia do pliku raportu.

  Domyślnie informacje są zapisywane w standardowym strumieniu wyjścia (stdout). Jeżeli parametr ten nie zostanie użyty, na ekranie zostaną wyświetlane wiadomości: o błędzie oraz z wynikami.

- `-address <adres serwera>`—Adres Serwera administracyjnego, z którym nawiązywane jest połączenie.

  Jako adres można określić adres IP, nazwę NetBIOS lub nazwę DNS urządzenia.

- `-pn <numer portu>`—Numer portu użytego do nawiązania nieszyfrowanego połączenia z Serwerem administracyjnym.

  Domyślny numer portu to 14000.

- `-ps <numer portu SSL>`—Numer portu SSL, przez który nawiązywane jest połączenie szyfrowane z Serwerem administracyjnym przy użyciu protokołu SSL.

  Domyślny numer portu to 13000.

- `-nossl`—Użycie nieszyfrowanego połączenia z Serwerem administracyjnym.

  Jeżeli parametr ten nie zostanie użyty, Agent sieciowy nawiąże z Serwerem administracyjnym połączenie szyfrowane przy użyciu protokołu SSL.

- `-cert <ścieżka dostępu do pliku certyfikatu>`—Użycie określonego pliku certyfikatu do autoryzacji podczas uzyskiwania dostępu do Serwera administracyjnego.

  Jeżeli parametr ten nie zostanie użyty, Agent sieciowy pobierze certyfikat podczas pierwszego połączenia z Serwerem administracyjnym.

- `-silent`—Uruchamia narzędzie w trybie cichym.

  Użycie tego parametru może być przydatne, gdy, na przykład, narzędzie jest uruchamiane ze skryptu logowania podczas rejestracji użytkownika.

- `-dupfix`—Ten klucz jest używany, gdy Agent sieciowy został zainstalowany w sposób inny niż tradycyjny (z pakietu dystrybucyjnego), na przykład poprzez przywrócenie go z obrazu dysku ISO.

- `-virtserv`— Nazwa wirtualnego Serwera administracyjnego.

- `-cloningmode`— Tryb klonowania dysku Agenta sieciowego.

  Użyj jednego z następujących parametrów, aby skonfigurować tryb klonowania dysku:

  - `-cloningmode` — Zażądaj stanu trybu klonowania dysku.
  - `-cloningmode 1` — Włącz tryb klonowania dysku.
  - `-cloningmode 0` — Wyłącz tryb klonowania dysku.

- `-nauninstpwd <hasło>`—Klucz służy do określenia hasła dezinstalacyjnego Agenta sieciowego.

  Klucz nie jest obowiązkowy.

Na przykład, aby połączyć Agenta sieciowego z Serwerem administracyjnym, uruchom następującą komendę:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Tunelowanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym

Kaspersky Security Center umożliwia tunelowanie połączeń TCP z Konsoli administracyjnej poprzez Serwer administracyjny, a następnie poprzez Agenta sieciowego do określonego portu na zarządzanym urządzeniu. Tunelowanie połączeń jest przeznaczone dla połączenia aplikacji klienckiej na urządzeniu z zainstalowaną Konsolą administracyjną z portem TCP na zarządzanym urządzeniu—jeśli nie jest możliwe bezpośrednie połączenie między Konsolą administracyjną a urządzeniem docelowym.

Na przykład, tunelowanie jest wykorzystywane dla połączeń ze zdalnym pulpitem - zarówno do łączenia się z istniejącą sesją, jak i do tworzenia nowej zdalnej sesji.

Tunelowanie połączeń może zostać włączone także przy użyciu narzędzi zewnętrznych. Na przykład, administrator może uruchomić w ten sposób narzędzie putty, klienta VNC oraz inne narzędzia.

Tunelowanie połączenia pomiędzy zdalnym urządzeniem klienckim a Serwerem administracyjnym jest wymagane, gdy port używany do nawiązania połączenia z Serwerem administracyjnym nie jest dostępny na urządzeniu. Port może być niedostępny na urządzeniu w następujących przypadkach:

- Zdalne urządzenie jest podłączone do sieci lokalnej, która wykorzystuje mechanizm NAT.
- Zdalne urządzenie jest częścią sieci lokalnej Serwera administracyjnego, ale jego port jest zamknięty przez zaporę sieciową.

W celu tunelowania połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym:

1. W drzewie konsoli wybierz folder grupy, która zawiera urządzenie klienckie.
2. Na zakładce **Urządzenia** wybierz urządzenie.
3. Z menu kontekstowego urządzenia wybierz **Wszystkie zadania** → **Tunelowanie połączenia**.
4. W otwartym oknie **Tunelowanie połączenia** utwórz tunel.

Zdalne połączenie z pulpitem urządzenia klienckiego

Administrator może uzyskać zdalny dostęp do pulpitu urządzenia klienckiego poprzez Agenta sieciowego zainstalowanego na urządzeniu klienckim.

Zdalne połączenie z urządzeniem poprzez Agenta sieciowego jest możliwe nawet wtedy, gdy porty TCP i UDP urządzenia klienckiego są zamknięte. Po nawiązaniu połączenia z urządzeniem, administrator uzyskuje pełny dostęp do informacji przechowywanych na tym urządzeniu, dzięki czemu może zarządzać aplikacjami, które są na nim zainstalowane.

W tej sekcji opisano sposób nawiązywania połączenia z urządzeniem klienckim Windows i urządzeniem klienckim macOS za pośrednictwem Agenta sieciowego.

Łączenie z urządzeniami klienckimi Windows

Zdalne połączenie z urządzeniem klienckim Windows można nawiązać w jeden z następujących sposobów:

- Używając standardowego składnika systemu Microsoft Windows o nazwie Podłączanie pulpitu zdalnego.

  Połączenie ze zdalnym pulpitem jest nawiązywane przy użyciu standardowego narzędzia Windows o nazwie mstsc.exe zgodnie z ustawieniami narzędzia.

- Używając technologii udostępniania pulpitu Windows.

Łączenie z urządzeniem klienckim z systemem Windows przy użyciu funkcji Podłączanie pulpitu zdalnego

Połączenie z bieżącą sesją zdalnego pulpitu użytkownika jest nawiązywane bez zgody użytkownika. Po nawiązaniu przez administratora połączenia z sesją, użytkownik urządzenia zostaje odłączony od sesji bez wcześniejszego powiadomienia.

W celu nawiązania połączenia z pulpitem urządzenia klienckiego przy użyciu komponentu Podłączanie pulpitu zdalnego:

1. W drzewie Konsoli administracyjnej wybierz urządzenie, do którego chcesz uzyskać dostęp.
2. Z menu kontekstowego urządzenia wybierz **Wszystkie zadania → Połącz z urządzeniem → Nowa sesja Pulpitu zdalnego**.

   Zostanie uruchomione standardowe narzędzie systemu Windows o nazwie mstsc.exe, które pomoże w nawiązaniu połączenia ze zdalnym pulpitem.
3. Postępuj zgodnie z instrukcjami wyświetlanymi w oknach dialogowych narzędzia.

Po nawiązaniu połączenia z urządzeniem, pulpit jest dostępny w oknie Podłączanie pulpitu zdalnego systemu Microsoft Windows.

Łączenie z urządzeniem klienckim z systemem Windows przy użyciu funkcji Udostępnianie pulpitu w systemie Windows

Podczas łączenia się z istniejącą sesją zdalnego pulpitu użytkownik sesji na urządzeniu otrzymuje od administratora żądanie dotyczące połączenia. W raportach utworzonych przez Kaspersky Security Center nie są zapisywane żadne informacje dotyczące zdalnych działań wykonywanych na urządzeniu ani wyniki tych działań.

Administrator może połączyć się z istniejącą sesją na urządzeniu klienckim bez rozłączania użytkownika w tej sesji. W tym przypadku administrator i użytkownik sesji na urządzeniu klienckim współdzielą dostęp do pulpitu.

Administrator może skonfigurować audyt aktywności użytkownika na zdalnym urządzeniu klienckim. W trakcie audytu aplikacja zapisuje informacje o plikach na urządzeniu klienckim, który został otwarty i/lub zmodyfikowany przez administratora.

W celu nawiązania połączenia z pulpitem urządzenia klienckiego poprzez udostępnianie pulpitu Windows muszą być spełnione następujące warunki:

- Na stacji roboczej administratora powinien być zainstalowany system operacyjny Microsoft Windows Vista lub nowszy. Typ systemu operacyjnego urządzenia, na którym znajduje się Serwer administracyjny nie nakłada żadnych ograniczeń na łączenie poprzez udostępnianie pulpitu Windows.

  Aby sprawdzić, czy funkcja udostępniania pulpitu Windows znajduje się w posiadanej przez Ciebie edycji systemu Windows, upewnij się, że klucz CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} znajduje się w rejestrze systemu Windows.
- System Microsoft Windows Vista lub nowszy jest zainstalowany na urządzeniu klienckim.
- Kaspersky Security Center korzysta z licencji dla Zarządzania lukami i poprawkami.

W celu nawiązania połączenia z pulpitem urządzenia klienckiego poprzez udostępnianie pulpitu Windows:

1. W drzewie Konsoli administracyjnej wybierz urządzenie, do którego chcesz uzyskać dostęp.
2. Z menu kontekstowego urządzenia wybierz **Wszystkie zadania → Połącz z urządzeniem → Udostępnianie pulpitu Windows**.

3. W oknie **Wybierz sesję pulpitu zdalnego**, które zostanie otwarte, wybierz sesję na urządzeniu, do której chcesz się podłączyć.

   W przypadku pomyślnego nawiązania połączenia z urządzeniem, pulpit urządzenia będzie dostępny w oknie **Kaspersky Remote Desktop Session Viewer**.

4. Aby rozpocząć interakcję z urządzeniem, w menu głównym okna **Kaspersky Remote Desktop Session Viewer** wybierz **Akcje** → **Tryb interaktywny**.

Narzędzie **Kaspersky Remote Desktop Session Viewer** wymaga licencji komercyjnej.

Łączenie z urządzeniami klienckimi macOS

Administrator może używać systemu Virtual Network Computing (VNC) do łączenia się z urządzeniami macOS.

Połączenie ze zdalnym pulpitem jest nawiązywane za pośrednictwem klienta VNC zainstalowanego na urządzeniu Serwera administracyjnego. Klient VNC przełącza sterowanie klawiaturą i myszą z urządzenia klienckiego na administratora.

Gdy administrator łączy się ze zdalnym pulpitem, użytkownik nie otrzymuje powiadomień ani próśb o połączenie od administratora. Administrator łączy się z istniejącą sesją na urządzeniu klienckim bez rozłączania użytkownika w tej sesji.

W celu nawiązania połączenia z pulpitem macOS klienta poprzez klienta VNC muszą być spełnione następujące warunki:

- Klient VNC jest zainstalowany na urządzeniu Serwera administracyjnego.
- Zdalne logowanie i zdalne zarządzanie są dozwolone na urządzeniu klienckim.
- Użytkownik zezwolił administratorowi na dostęp do urządzenia klienckiego w ustawieniach **udostępniania** systemu operacyjnego macOS.

Aby połączyć się z pulpitem urządzenia klienckiego za pośrednictwem systemu Virtual Network Computing:

1. W drzewie Konsoli administracyjnej wybierz urządzenie, do którego chcesz uzyskać dostęp.
2. Z menu kontekstowego urządzenia wybierz **Wszystkie zadania** → **Tunelowanie połączenia**.
3. W otwartym oknie **Tunelowanie połączenia** wykonaj następujące czynności:
   a. W sekcji **1. Port sieciowy** określ numer portu sieciowego urządzenia, z którym chcesz się połączyć.

      Domyślnie wykorzystywany jest port 5900.

   b. W sekcji **2. Tunelowanie** kliknij przycisk **Utwórz tunel**.

   c. W sekcji **3. Ustawienia sieciowe** kliknij przycisk **Kopiuj**.
4. Otwórz klienta VNC i wklej skopiowane atrybuty sieciowe do pola tekstowego. Naciśnij **Enter**.
5. W oknie, które zostanie otwarte, przejrzyj szczegóły certyfikatu. Jeśli zgadzasz się na użycie certyfikatu, kliknij przycisk **Tak**.
6. W oknie **Uwierzytelnianie** określ poświadczenia urządzenia klienckiego, a następnie kliknij przycisk **OK**.

Nawiązywanie połączenia z urządzeniami poprzez udostępnianie pulpitu Windows

W celu nawiązania połączenia z urządzeniem poprzez udostępnianie pulpitu Windows:

1. W drzewie konsoli, na zakładce **Urządzenia** wybierz folder **Zarządzane urządzenia**.

   Obszar roboczy tego folderu wyświetla listę urządzeń.

2. Z menu kontekstowego urządzenia, z którym chcesz nawiązać połączenie, wybierz **Połącz z urządzeniem → Udostępnianie pulpitu Windows**.

   Zostanie otwarte okno **Wybierz sesję pulpitu zdalnego**.

3. W oknie **Wybierz sesję pulpitu zdalnego** wybierz sesję pulpitu w celu nawiązania połączenia z urządzeniem.

4. Kliknij **OK**.

Połączenie z urządzeniem zostanie nawiązane.

Konfigurowanie ponownego uruchamiania urządzenia klienckiego

Podczas korzystania, instalowania lub usuwania Kaspersky Security Center konieczne może być ponowne uruchomienie urządzenia. Możesz określić ustawienia ponownego uruchamiania tylko dla urządzeń działających pod kontrolą systemu Windows.

W celu skonfigurowania ponownego uruchamiania urządzenia klienckiego:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której chcesz skonfigurować ponowne uruchamianie.

2. W obszarze roboczym grupy wybierz zakładkę **Zasady**.

3. W obszarze roboczym, na liście zasad wybierz zasadę Agenta sieciowego Kaspersky Security Center, a następnie z menu kontekstowego zasady wybierz **Właściwości**.

4. W oknie ustawień zasady wybierz sekcję **Zarządzanie ponownym uruchamianiem**.

5. Wybierz akcję, jaka ma zostać wykonana, gdy wymagane jest ponowne uruchomienie urządzenia:

   - Wybierz **Nie uruchamiaj ponownie systemu operacyjnego**, aby zablokować automatyczne ponowne uruchamianie.

   - Wybierz **Jeżeli będzie to wymagane, automatycznie uruchom ponownie system operacyjny**, aby zezwolić na automatyczne ponowne uruchomienie.

   - Wybierz **Pytaj użytkownika o akcję**, aby włączyć wyświetlanie pytania o zezwolenie na ponowne uruchomienie.

Można określić częstotliwość wyświetlania pytań o ponowne uruchomienie, włączyć wymuszone ponowne uruchomienie oraz wymuszone zamknięcie aplikacji w zablokowanych sesjach na urządzeniu, zaznaczając odpowiednie pola i ustawienia czasu w polu pokrętła.

6. Aby zapisać wprowadzone zmiany i zamknąć okno właściwości zasady, kliknij **OK**.

Ponowne uruchamianie urządzenia zostanie skonfigurowane.

Audyt działań na zdalnym urządzeniu klienckim

Aplikacja umożliwia przeprowadzenie audytu działań administratora na zdalnych urządzeniach klienckich działających pod kontrolą systemu Windows. W trakcie audytu aplikacja zapisuje na urządzeniu informacje o plikach, które zostały otwarte i/lub zmodyfikowane przez administratora. Audyt działań administratora jest dostępny, gdy są spełnione następujące warunki:

- Licencja Zarządzanie lukami i poprawkami jest w użyciu.
- Administrator posiada uprawnienie do włączania współdzielonego dostępu do pulpitu zdalnego urządzenia.

W celu włączenia audytu działań na zdalnym urządzeniu klienckim:

1. W drzewie konsoli wybierz grupę administracyjną, dla której powinien zostać skonfigurowany audyt działań administratora.
2. W obszarze roboczym grupy wybierz zakładkę **Zasady**.
3. Wybierz zasadę Agenta sieciowego Kaspersky Security Center, a następnie z menu kontekstowego zasady wybierz **Właściwości**.
4. W oknie ustawień zasady wybierz sekcję **Udostępnianie pulpitu Windows**.
5. Zaznacz pole **Włącz audyt**.
6. Na listach **Maski plików, które będą monitorowane podczas odczytu** i **Maski plików, które będą monitorowane podczas modyfikacji** dodaj maski plików, na których wykonywane działania mają być monitorowane przez aplikację podczas audytu.

   Domyślnie aplikacja monitoruje działania wykonywane na plikach z rozszerzeniami .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt i .pdf.

7. Aby zapisać wprowadzone zmiany i zamknąć okno właściwości zasady, kliknij **OK**.

Audyt działań administratora na zdalnym urządzeniu użytkownika z włączonym dostępem do pulpitu został skonfigurowany.

Wpisy dotyczące działań administratora na zdalnym urządzeniu są zapisywane w:

- Raporcie zdarzeń na zdalnym urządzeniu.
- Pliku z rozszerzeniem syslog znajdującym się w folderze Agenta sieciowego na zdalnym urządzeniu (na przykład: C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- Bazie danych zdarzeń programu Kaspersky Security Center.

Sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym

Kaspersky Security Center umożliwia ręczne lub automatyczne sprawdzanie połączeń między urządzeniem klienckim a Serwerem administracyjnym.

Automatyczne sprawdzanie połączeń odbywa się na Serwerze administracyjnym. Ręczne sprawdzanie połączeń wykonywane jest na urządzeniu.

Automatyczne sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym

W celu włączenia automatycznego sprawdzania połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym:

1. W drzewie konsoli wybierz grupę administracyjną, która zawiera urządzenia.
2. W obszarze roboczym grupy administracyjnej, na zakładce **Urządzenia** wybierz urządzenia.
3. Z otwartego menu kontekstowego urządzenia wybierz **Sprawdź dostępność urządzenia**.

Zostanie otwarte okno zawierające informacje o dostępności urządzenia.

Ręczne sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym. Narzędzie klnagchk

Możesz sprawdzić połączenie oraz uzyskać szczegółowe informacje o ustawieniach połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym, korzystając z narzędzia klnagchk. Narzędzie klnagchk znajduje się w folderze instalacyjnym Agenta sieciowego.

Po uruchomieniu narzędzia klnagchk z poziomu wiersza poleceń będzie ono mogło wykonać następujące akcje (w zależności od używanych parametrów):

- Wyświetla na ekranie lub zapisuje w raporcie wartości ustawień używanych do łączenia Agenta sieciowego, zainstalowanego na urządzeniu, z Serwerem administracyjnym.
- Rejestruje w pliku dziennika zdarzeń statystyki Agenta sieciowego (od jego ostatniego uruchomienia) oraz wyniki działania narzędzia lub wyświetlić informacje na ekranie.
- Podejmij próbę nawiązania połączenia pomiędzy Agentem sieciowym a Serwerem administracyjnym.

  Jeżeli próba nawiązania połączenia nie powiedzie się, narzędzie wyśle pakiet ICMP w celu sprawdzenia stanu urządzenia, na którym zainstalowany jest Serwer administracyjny.

W celu sprawdzenia połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym, korzystając z narzędzia klnagchk,

Na urządzeniu z zainstalowanym Agentem sieciowym uruchom narzędzie klnagchk z wiersza poleceń, korzystając z konta administratora lokalnego.

Składnia wiersza poleceń narzędzia:

```
klnagchk [-logfile <nazwa pliku>] [-sp] [-savecert <ścieżka do pliku certyfikatu>] [-restart][-sendhb]
```

Opisy przełączników:

- `-logfile <nazwa pliku>`—Zapisuje do pliku raportu wartości ustawień połączenia pomiędzy Agentem sieciowym a Serwerem administracyjnym oraz wyniki działania narzędzia.

  Domyślnie informacje są zapisywane w standardowym strumieniu wyjścia (stdout). Jeżeli parametr ten nie zostanie użyty, na ekranie zostaną wyświetlane wiadomości: o błędzie, z wynikami oraz ustawieniami.

- `-sp`—Wyświetla hasło używane do autoryzacji użytkownika na serwerze proxy.

  Klucz jest używany, jeśli połączenie z Serwerem administracyjnym jest nawiązywane za pośrednictwem serwera proxy.

- `-savecert <nazwa pliku>`—Zapisuje w określonym pliku certyfikat używany do uzyskiwania dostępu do Serwera administracyjnego.

- `-restart`—Ponowne uruchamia Agenta sieciowego po zakończeniu działania narzędzia.

- `-sendhb`—Rozpoczyna synchronizację Agenta sieciowego z Serwerem administracyjnym.

Po uruchomieniu narzędzie klnagchk uzyskuje dostęp do plików konfiguracyjnych Agenta sieciowego i wyświetla parametry połączenia. Parametry te są określane podczas instalacji Agenta sieciowego oraz w ustawieniach zasady Agenta sieciowego:

- `Current device`—Nazwa urządzenia klienckiego w sieci Windows.

- `Network Agent version`—Pełny numer wersji Agenta sieciowego (z poprawkami) zainstalowanego na urządzeniu.

- `Administration Server address`—Adres Serwera administracyjnego.

- `Use SSL`—Parametr wskazujący, czy podczas łączenia się z Serwerem administracyjnym używane jest bezpieczne połączenie.

  Możliwe wartości:

  - 0 — bezpieczne połączenie nie jest używane.

  - 1 — używane jest bezpieczne połączenie.

- `Compress traffic`—Parametr wskazujący, czy ruch pomiędzy urządzeniem klienckim a Serwerem administracyjnym jest kompresowany.

- `Numbers of the Administration Server SSL ports`—Liczba prawidłowych portów do komunikacji z Serwerem administracyjnym podczas korzystania z bezpiecznego połączenia.

- `Numbers of the Administration Server ports`—Numery prawidłowych portów do komunikacji z Serwerem administracyjnym podczas korzystania ze zwykłego połączenia.

- `Use proxy server`—Parametr wskazujący, czy używany jest serwer proxy.

Możliwe wartości:

- 0 — serwer proxy nie jest używany.
- 1 — używany jest serwer proxy.

- `Address` —Adres i port serwera proxy oddzielone dwukropkiem. Ten parametr jest wyświetlany tylko wtedy, gdy używany jest serwer proxy.
- `User name` —Nazwa użytkownika umożliwiająca dostęp do serwera proxy. Ten parametr jest wyświetlany tylko wtedy, gdy używany jest serwer proxy.
- `Password` —Hasło dostępu do serwera proxy. Ten parametr jest wyświetlany tylko wtedy, gdy używany jest serwer proxy. Aby wyświetlić hasło serwera proxy, musisz użyć klucza `sp` w poleceniu.
- `Administration Server certificate` —Parametr wskazujący, czy urządzenie klienckie posiada certyfikat Serwera administracyjnego. Certyfikat może nie istnieć, jeśli Agent sieciowy nigdy nie nawiązał pomyślnego połączenia z Serwerem administracyjnym.

  Możliwe wartości:

  - `not installed` —Urządzenie klienckie nie posiada certyfikatu Serwera administracyjnego.
  - `available` — Urządzenie klienckie posiada certyfikat Serwera administracyjnego.
- `Open UDP port` —Parametr wskazujący, czy Agent sieciowy używa portu UDP do odbierania żądań synchronizacji z Serwera administracyjnego.

  Możliwe wartości:

  - 0 — Port UDP jest zamknięty dla odbierania żądań synchronizacji z Serwera administracyjnego.
  - 1 — Port UDP jest otwarty do odbierania żądań synchronizacji z Serwera administracyjnego.
- `Numbers of UDP ports` —Numery portów UDP, z których może korzystać Agent sieciowy.
- `Location name` —Lokalizacja sieciowa urządzenia.
- `State of network location` —Parametr wskazujący, czy urządzenie klienckie może zostać przełączone z jednego profilu połączenia Serwera administracyjnego na inny.

  Możliwe wartości:

  - `Enabled` —Profil połączenia Serwera administracyjnego można przełączyć dla urządzenia klienckiego.
  - `Disabled` —Nie można przełączyć profilu połączenia Serwera administracyjnego dla urządzenia klienckiego.
- `Profile to use` —Profil połączenia dla Serwera administracyjnego.
- `Condition` —Adres IP i maska podsieci, do której podłączone jest urządzenie klienckie.
- `Synchronization interval (min)` —Standardowy odstęp między synchronizacjami.
- `Connection timeout (in seconds)` —Limit czasu połączenia.
- `Send / receive timeout (in seconds)` —Limit czasu połączenia dla operacji odczytu i zapisu.

- `Device ID`—Identyfikator urządzenia w sieci. `Device ID` jest unikalny wśród urządzeń klienckich zarządzanych przez konkretny Serwer administracyjny.

- `Locations of connection gateways`—Parametry łączenia urządzenia klienckiego z Serwerem administracyjnym poprzez bramę połączeń.

- `Location of distribution points`—Parametry łączenia urządzenia klienckiego z Serwerem administracyjnym poprzez punkt dystrybucji.

- `Connection with server`—Parametr wskazujący, czy brama połączenia ma ciągłe połączenie z Serwerem administracyjnym. Parametr wyświetlany tylko wtedy, gdy urządzenie klienckie pełni funkcję bramy połączenia.

  Możliwe wartości:

  - `active`—Brama połączenia ma ciągłe połączenie z Serwerem administracyjnym.

  - `inactive`—Brama połączenia nie ma ciągłego połączenia z Serwerem administracyjnym.

- `Connection with server through connection gateway`—Parametr wskazujący, czy połączenie z Serwerem administracyjnym przez bramę połączenia zostało nawiązane prawidłowo. Parametr wyświetlany tylko wtedy, gdy urządzenie klienckie pełni funkcję bramy połączenia.

  Możliwe wartości:

  - `active`—Połączenie z Serwerem administracyjnym poprzez bramę połączenia jest nawiązane prawidłowo.

  - `inactive`—Połączenie z Serwerem administracyjnym przez bramę połączenia jest nawiązane nieprawidłowo.

Ponadto dane wyjściowe narzędzia klnagchk mogą zawierać jeden z następujących wierszy:

- `Administration Server is installed on this device`—Narzędzie klnagchk jest uruchomione na urządzeniu Serwera administracyjnego.

- `This device has been assigned a connection gateway but is not yet registered on Administration Server`—Narzędzie klnagchk jest uruchamiane na urządzeniu, na którym jest zainstalowany Agent sieciowy, w trybie bramy połączenia. Skonfigurowana brama połączenia czeka na połączenie z Serwerem administracyjnym, ale Serwer administracyjny nie wyświetla urządzenia wśród zarządzanych urządzeń. Należy zapewnić, że Serwer administracyjny zainicjuje połączenie z bramą połączenia.

- `This device is a connection gateway`—Narzędzie klnagchk jest uruchamiane na urządzeniu pełniącym rolę bramy połączenia.

- `Acts as a distribution point`—Narzędzie klnagchk jest uruchamiane na urządzeniu pełniącym funkcję punktu dystrybucji.

Narzędzie klnagchk sprawdza stan usługi Agenta sieciowego. Jeśli usługa nie jest uruchomiona, narzędzie zostanie zatrzymane. Jeśli usługa jest uruchomiona, narzędzie wyświetla następujące statystyki połączeń:

- `Total number of synchronization requests`—Liczba prób połączenia urządzenia klienckiego z Serwerem administracyjnym.

- `The number of successful synchronization request`—Liczba pomyślnych prób połączenia urządzenia klienckiego z Serwerem administracyjnym.

- `Total number of synchronizations`—Liczba prób synchronizacji ustawień urządzenia klienckiego z ustawieniami Serwera administracyjnego.

- `The number of successful synchronizations`—Liczba udanych prób synchronizacji ustawień urządzenia klienckiego z Serwerem administracyjnym.

- `Date/time of the last request for synchronization`—Data i godzina ostatniego połączenia.

Podczas analizowania połączenia pomiędzy Serwerem administracyjnym a Agentem sieciowym należy użyć parametrów `Total number of synchronization requests` i `The number of successful synchronization request`. Ustawienia urządzenia klienckiego synchronizują się z ustawieniami Serwera administracyjnego tylko wtedy, gdy ustawienia Serwera administracyjnego zostały zmienione (na przykład, jeśli dodano nowe zadania lub zmodyfikowano ustawienia zasady). W przeciwnym razie wartości parametrów `Total number of synchronizations` i `The number of successful synchronizations` pozostają niezmienione.

Aby uzyskać więcej informacji na temat rozwiązywania problemów z połączeniem agenta sieciowego z Serwerem administracyjnym, zapoznaj się z sekcją Często zadawane pytania dotyczące Kaspersky Security Center.

Informacje o sprawdzaniu czasu połączenia pomiędzy urządzeniem a Serwerem administracyjnym

Po wyłączeniu urządzenia, Agent sieciowy powiadamia Serwer administracyjny o tym zdarzeniu. W Konsoli administracyjnej to urządzenie jest wyświetlane jako wyłączone. Jednakże Agent sieciowy nie może powiadamiać Serwera administracyjnego o wszystkich tego typu zdarzeniach. Dlatego też Serwer administracyjny okresowo analizuje atrybut **Połączono z Serwerem administracyjnym** (wartość tego atrybutu jest wyświetlana w Konsoli administracyjnej, we właściwościach urządzenia, w sekcji **Ogólne**) dla każdego urządzenia i porównuje go z interwałem synchronizacji z aktualnych ustawień Agenta sieciowego. Jeśli urządzenie nie odpowiedziało w ponad trzech pomyślnych interwałach synchronizacji, to urządzenie zostanie oznaczone jako wyłączone.

Identyfikowanie urządzeń klienckich na Serwerze administracyjnym

Urządzenia klienckie są identyfikowane w oparciu o ich nazwy. Nazwa urządzenia musi być unikatowa w obrębie wszystkich urządzeń połączonych z Serwerem administracyjnym.

Nazwa urządzenia jest przesyłana do Serwera administracyjnego podczas przeszukiwania sieci Windows i po wykryciu w niej nowego urządzenia lub przy pierwszym połączeniu Agenta sieciowego, zainstalowanego na urządzeniu, z Serwerem administracyjnym. Domyślnie nazwa odpowiada nazwie urządzenia w sieci Windows (nazwa NetBIOS). Jeśli na Serwerze administracyjnym jest już zarejestrowane urządzenie o tej nazwie, do nazwy nowego urządzenia zostanie dodany przyrostek z liczbą, na przykład: **<Nazwa>-1**, **<Nazwa>-2**. Pod tą nazwą urządzenie jest dodawane do grupy administracyjnej.

Przenoszenie urządzeń do grupy administracyjnej

Możesz przenosić urządzenia z jednej grupy administracyjnej do innej, jeśli posiadasz uprawnienie **Modyfikacja** w obszarze **Zarządzanie grupami administracyjnymi** dla źródłowej i docelowej grupy administracyjnej (lub dla Serwera administracyjnego, do którego te grupy należą).

W celu dodania jednego lub kilku urządzeń do wybranej grupy administracyjnej:

1. W drzewie konsoli rozwiń folder **Zarządzane urządzenia**.

2. W folderze **Zarządzane urządzenia** wybierz podfolder odpowiadający grupie, w której zostaną umieszczone urządzenia klienckie.

   Jeżeli chcesz dodać urządzenia do grupy **Zarządzane urządzenia**, możesz pominąć ten krok.

3. W obszarze roboczym wybranej grupy administracyjnej, na zakładce **Urządzenia** uruchom proces dodawania urządzeń do grupy w jeden z następujących sposobów:

   - Dodając urządzenia do grupy poprzez kliknięcie przycisku **Przenieś urządzenia do grupy** znajdującego się w oknie z informacjami dla listy urządzeń
   - Wybierając **Utwórz** → **Urządzenie** z menu kontekstowego listy urządzeń

   Zostanie uruchomiony Kreator przenoszenia urządzeń. Postępując zgodnie z jego poleceniami, wybierz metodę przenoszenia urządzeń do grupy i utwórz listę urządzeń, które mają zostać dodane do grupy.

   Jeżeli ręcznie tworzysz listę urządzeń, jako adres urządzenia możesz określić adres IP (lub zakres IP), nazwę NetBIOS lub nazwę DNS. Do listy możesz przenieść ręcznie tylko urządzenia, dla których informacje zostały już dodane do bazy danych Serwera administracyjnego przy podłączeniu urządzenia lub po wyszukiwaniu urządzeń.

   W celu zaimportowania listy urządzeń z pliku, należy wskazać plik TXT zawierający listę adresów urządzeń, które mają zostać dodane. Każdy adres musi znajdować się w oddzielnym wierszu.

Po zakończeniu pracy kreatora, wybrane urządzenia zostaną włączone do grupy administracyjnej i będą wyświetlane na liście urządzeń pod nazwami wygenerowanymi przez Serwer administracyjny.

Możesz przenieść urządzenie do wybranej grupy administracyjnej, przeciągając je z folderu **Urządzenia nieprzypisane** do folderu tej grupy administracyjnej.

Zmienianie Serwera administracyjnego dla urządzeń klienckich

Można zmienić Serwer administracyjny zarządzający urządzeniami klienckimi na inny, używając zadania *Zmiana Serwera administracyjnego*.

W celu zmiany Serwera administracyjnego zarządzającego urządzeniami klienckimi na inny Serwer:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. W obszarze roboczym tego folderu kliknij przycisk **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. W kroku **Wybierz typ zadania** kreatora, wybierz węzeł **Serwer administracyjny Kaspersky Security Center**, rozwiń folder **Zaawansowane**, a następnie wybierz zadanie **Zmiana Serwera administracyjnego**.
4. W oknie, które zostanie otwarte, kliknij przycisk **OK**, aby potwierdzić akceptację warunków zmiany Serwera administracyjnego dla urządzeń klienckich.

5. W kroku **Ustawienia** kreatora wybierz Serwer administracyjny, którego chcesz używać do zarządzania wybranymi urządzeniami:

   - **Zmień na inny główny Serwer administracyjny**

     Aby przenieść urządzenia klienckie na inny główny Serwer administracyjny, należy określić następujące ustawienia połączenia z Serwerem administracyjnym:

     1. W polu **Serwer administracyjny** podaj adres nowego głównego Serwera administracyjnego.

     2. W polu **Port** podaj numer portu, za pomocą którego ma zostać nawiązane połączenie z Serwerem administracyjnym.

        Domyślny numer portu to 14000.

     3. W polu **Port SSL** określ numer portu SSL na głównym Serwerze administracyjnym.

        Domyślny numer portu to 13000.

     4. W razie potrzeby zaznacz pole wyboru **Użyj serwera proxy**.

        Jeżeli to pole wyboru będzie odznaczone, do połączenia urządzenia z Serwerem administracyjnym wykorzystywane jest połączenie bezpośrednie.

        Jeżeli to pole wyboru jest zaznaczone, określ parametry serwera proxy:

        - **Adres serwera proxy**

        - **Port serwera proxy**

        Jeżeli Twój serwer proxy wymaga uwierzytelnienia, w polach **Nazwa użytkownika** i **Hasło**, określ poświadczenia konta, w ramach którego nawiązywane jest połączenie z serwerem proxy. Zalecamy określenie poświadczeń konta, które ma minimalne uprawnienia wymagane tylko do uwierzytelnienia serwera proxy.

     5. W razie potrzeby prześlij nowy certyfikat Serwera administracyjnego.

   - **Zmień na inny wirtualny Serwer na głównym Serwerze**

     Wybierz tę opcję, aby przenieść urządzenia klienckie na wirtualny Serwer administracyjny na bieżącym głównym Serwerze administracyjnym. Aby to zrobić, w polu **Nazwa wirtualnego Serwera administracyjnego** podaj nazwę wymaganego wirtualnego Serwera administracyjnego.

   W razie potrzeby określ czas oczekiwania przed ponownym uruchomieniem Agenta sieciowego.

6. W tym kroku kreatora wybierz urządzenia, do których zostanie przypisane zadanie:

   - **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**. W tym przypadku zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

   - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**. Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

- **Przypisz zadanie do wyboru urządzeń**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonym wyborze. Możesz określić predefiniowany lub niestandardowy wybór, który utworzyłeś.

- **Przypisz zadanie do grupy administracyjnej**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonej grupie administracyjnej.

7. W kroku **Wybieranie konta do uruchomienia zadania** kreatora określ ustawienia konta:

   - **Konto domyślne**

     Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

     Domyślnie opcja ta jest zaznaczona.

   - **Określ konto**

     Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

     - **Konto**

       Konto, z poziomu którego zadanie jest uruchamiane.

     - **Hasło**

       Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

8. W kroku **Konfiguruj terminarz zadania** kreatora możesz utworzyć terminarz uruchomienia zadania. Jeśli to konieczne, określ następujące ustawienia:

   - **Zaplanowane uruchomienie:**

     Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

     - **Codziennie (czas letni nie jest obsługiwany)**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

       Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

       Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

     - **Według dni tygodnia**

       Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

       Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

     - **Co miesiąc**

       Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

       W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

       Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Raz**

  Zadanie zostanie uruchomione raz, w określonym dniu i o określonej godzinie (domyślnie w dniu utworzenia zadania).

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Natychmiast**

  Zadanie jest uruchamiane natychmiast po tym, jak urządzenie stanie się widoczne w sieci lub zostanie uwzględnione w zakresie zadania.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

9. W tym kroku kreatora należy podać nazwę zadania, które tworzysz.

10. W kroku **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

    Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu wykonywania zadania, urządzenia klienckie, dla których zostało ono utworzone, zostaną przekazane Serwerowi administracyjnemu określonemu w ustawieniach zadania.

Jeśli Serwer administracyjny obsługuje szyfrowanie i ochronę danych, a Ty tworzysz zadanie *Zmiana Serwera administracyjnego*, zostanie wyświetlone ostrzeżenie. Ostrzeżenie informuje, że jeśli jakiekolwiek zaszyfrowane dane są przechowywane na urządzeniach, po rozpoczęciu przez nowy Serwer zarządzania urządzeniami, użytkownicy będą mieli dostęp tylko do zaszyfrowanych danych, z którymi wcześniej pracowali. W innych przypadkach dostęp do zaszyfrowanych danych będzie niemożliwy. Szczegółowe opisy scenariuszy, w których dostęp do zaszyfrowanych danych nie jest zapewniany, znajdują się w Pomocy Kaspersky Endpoint Security for Windows.

Przenoszenie urządzeń podłączonych do Serwera administracyjnego przez bramy połączeń na inny Serwer administracyjny

Możesz przenieść urządzenia podłączone do Serwera administracyjnego przez bramy połączeń na inny Serwer administracyjny. Może to być na przykład konieczne w przypadku instalacji innej wersji Serwera administracyjnego i braku konieczności ponownej instalacji Agenta sieciowego na urządzeniach, gdyż mogłoby to być czasochłonne.

Polecenia opisane w instrukcji muszą być uruchamiane na urządzeniach klienckich z poziomu konta z uprawnieniami administratora.

Aby przenieść urządzenie podłączone poprzez bramę połączenia do innego Serwera administracyjnego:

1. Uruchom narzędzie klmover z parametrem `-address <adres serwera>`, aby przełączyć się na nowy Serwer administracyjny.
2. Uruchom polecenie `klnagchk -nagwait -tl 4`.
3. Uruchom następujące polecenia, aby ustawić nową bramę połączenia:
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<ip lub nazwa bramy>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Gdzie `<gateway ip or name>` to adres bramy połączenia dostępny z Internetu.
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` to numer portu TCP, na którym nasłuchuje brama połączenia.
4. Uruchom polecenie `klnagchk -restart -tl 4`, aby uruchomić usługę Agenta sieciowego.

Urządzenie zostaje przeniesione na nowy Serwer administracyjny i podłączone poprzez nową podłączoną bramę.

Klastry i grupy serwerów

Kaspersky Security Center obsługuje technologię klastra. Jeśli Agent sieciowy wyśle na Serwer administracyjny informacje potwierdzające, że aplikacja zainstalowana na urządzeniu klienckim jest częścią grupy serwerów, to urządzenie klienckie staje się węzłem klastra. Klaster zostanie dodany jako odrębny obiekt w folderze **Zarządzane urządzenia** w drzewie konsoli z ikoną serwera ().

Możemy wyróżnić kilka typowych cech klastra:

- Klaster i każdy z jego węzłów są zawsze w tej samej grupie administracyjnej.
- Jeśli administrator spróbuje przenieść węzeł klastra, węzeł wróci do swojej oryginalnej lokalizacji.
- Jeśli administrator spróbuje przenieść klaster do innej grupy, wszystkie jego węzły zostaną przeniesione wraz z nim.

Zdalne włączanie, wyłączanie i ponowne uruchamianie urządzeń klienckich

Kaspersky Security Center pozwala na zdalne zarządzanie urządzeniami klienckimi: włączanie, wyłączanie i ponowne uruchamianie.

W celu zdalnego zarządzania urządzeniami klienckimi:

1. Nawiąż połączenie z Serwerem administracyjnym, który zarządza urządzeniami.
2. Utwórz zadanie zarządzania urządzeniami przy użyciu jednej z następujących metod:
   - Jeżeli chcesz włączyć, wyłączyć lub uruchomić ponownie urządzenia znajdujące się w wybranej grupie administracyjnej, utwórz zadanie dla wybranej grupy.
   - Jeżeli chcesz włączyć, wyłączyć lub uruchomić ponownie urządzenia znajdujące się w różnych grupach administracyjnych lub nie należące do żadnej z grup, utwórz zadanie dla wskazanych urządzeń.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora. W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania wybierz węzeł **Kaspersky Security Center**, otwórz folder **Zaawansowane** i wybierz zadanie **Zarządzaj urządzeniami**.
3. Uruchom utworzone zadanie.

Po zakończeniu zadania, polecenie (włącz, wyłącz lub uruchom ponownie) zostanie wykonane na wybranych urządzeniach.

Informacje o korzystaniu z ciągłego połączenia pomiędzy zarządzanym urządzeniem a Serwerem administracyjnym

Domyślnie Kaspersky Security Center nie oferuje stałego połączenia pomiędzy zarządzanymi urządzeniami a Serwerem administracyjnym. Agenty sieciowe na zarządzanych urządzeniach okresowo nawiązują połączenie i synchronizują się z Serwerem administracyjnym. Odstęp pomiędzy tymi sesjami synchronizacji jest zdefiniowany w zasadzie Agenta sieciowego i domyślnie wynosi 15 minut. Jeśli wymagana jest wczesna synchronizacja (na przykład, aby wymusić zastosowanie zasady), Serwer administracyjny wysyła podpisany pakiet sieciowy do Agenta sieciowego na porcie UDP o numerze 15000 (Serwer administracyjny może wysłać ten pakiet poprzez sieć IPv4 lub IPv6). Jeśli z jakiegoś powodu nie jest możliwe nawiązanie połączenia poprzez UDP między Serwerem administracyjnym a zarządzanym urządzeniem, synchronizacja zostanie uruchomiona przy kolejnym rutynowym nawiązaniu połączenia między Agentem sieciowym a Serwerem administracyjnym w obrębie interwału synchronizacji.

Jednakże niektórych operacji nie można jednak wykonać bez wcześniejszego nawiązania połączenia między Agentem sieciowym a Serwerem administracyjnym. Operacje te obejmują uruchamianie i zatrzymywanie zadań lokalnych, odbieranie statystyk dla zarządzanej aplikacji i tworzenie tunelu. Aby te operacje były możliwe, musisz włączyć opcję **Nie odłączaj od Serwera administracyjnego** na zarządzanym urządzeniu.

Informacje o wymuszonej synchronizacji

Chociaż Kaspersky Security Center automatycznie synchronizuje stan, ustawienia, zadania i zasady dla zarządzanych urządzeń, to w niektórych przypadkach administrator musi dokładnie wiedzieć, czy dla określonego urządzenia w danym momencie została już przeprowadzona synchronizacja.

W menu kontekstowym zarządzanych urządzeń w Konsoli administracyjnej urządzenia element menu **Wszystkie zadania** zawiera polecenie **Wymuś synchronizację**. Jeśli Kaspersky Security Center 15.1 wykona to polecenie, Serwer administracyjny podejmie próbę nawiązania połączenia z urządzeniem. Jeśli ta próba zakończy się pomyślnie, zostanie wykonana wymuszona synchronizacja. W innym przypadku synchronizacja zostanie wymuszona dopiero po kolejnym zaplanowanym połączeniu nawiązanym pomiędzy Agentem sieciowym a Serwerem administracyjnym.

Informacje o terminarzu połączenia

W oknie właściwości Agenta sieciowego, w sekcji **Łączność**, w podsekcji **Terminarz połączeń** możesz określić przedziały czasu, w trakcie których Agent sieciowy prześle dane do Serwera administracyjnego.

Połącz, gdy jest to konieczne. Jeśli ta opcja jest zaznaczona, połączenie jest nawiązywane, gdy Agent sieciowy musi wysłać dane na Serwer administracyjny.

Połącz w określonych przedziałach czasu. Jeśli ta opcja jest zaznaczona, Agent sieciowy łączy się z Serwerem administracyjnym w określonym czasie. Możesz dodać kilka przedziałów czasu.

Wysyłanie wiadomości na urządzenia użytkowników

W celu wysyłania wiadomości do użytkowników urządzeń:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. Utwórz zadanie wysyłania wiadomości dla użytkowników urządzeń na jeden z następujących sposobów:
   - Jeśli chcesz wysłać wiadomość do użytkowników urządzeń należących do wybranej grupy administracyjnej, utwórz zadanie dla wybranej grupy.
   - Jeżeli chcesz wysłać wiadomość do użytkowników urządzeń należących do różnych grup administracyjnych lub nie będących w żadnej grupie administracyjnej, utwórz zadanie dla wskazanych urządzeń.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.
3. W oknie Typ zadania kreatora tworzenia nowego zadania wybierz węzeł **Serwer administracyjny Kaspersky Security Center**, otwórz folder **Zaawansowane** i wybierz zadanie **Wyślij wiadomość do użytkownika**. Zadanie wysyłania wiadomości do użytkownika jest dostępne tylko dla urządzeń działających pod kontrolą systemu Windows. Wiadomości możesz wysyłać także z poziomu menu kontekstowego w folderze **Konta użytkowników**.
4. Uruchom utworzone zadanie.

   Po zakończeniu wykonywania zadania utworzona wiadomość zostanie wysłana do użytkowników wybranych urządzeń. Zadanie wysyłania wiadomości do użytkownika jest dostępne tylko dla urządzeń działających pod kontrolą systemu Windows. Wiadomości możesz wysyłać także z poziomu menu kontekstowego w folderze **Konta użytkowników**.

Zarządzanie Kaspersky Security for Virtualization

Kaspersky Security Center obsługuje opcję łączenia maszyn wirtualnych z Serwerem administracyjnym. Maszyny wirtualne są chronione przez Kaspersky Security for Virtualization. Więcej informacji można znaleźć w dokumentacji dla tej aplikacji.

Konfigurowanie przełączania stanów urządzeń

Możesz zmienić warunki, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia.

W celu włączenia zmiany stanu urządzenia na Krytyczny:

1. Otwórz okno właściwości w jeden z następujących sposobów:
   - W folderze **Zasady**, w menu kontekstowym zasady Serwera administracyjnego wybierz **Właściwości**.
   - Z menu kontekstowego grupy administracyjnej wybierz **Właściwości**.
2. W oknie **Właściwości**, które zostanie otwarte, w panelu **Sekcje** wybierz **Stan urządzenia**.

3. W sekcji **Ustaw stan Krytyczny, jeśli** zaznacz pole obok warunku na liście.

   Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

4. Kliknij dwukrotnie nazwę wybranego warunku i w otwartym oknie ustaw wymaganą wartość dla warunku.

   Nie można ustawić wartości dla następujących warunków: Aplikacja zabezpieczająca nie jest zainstalowana, Zainstalowane są niekompatybilne aplikacje, Wykryto luki w oprogramowaniu, Ustawienia urządzenia mobilnego nie są zgodne z zasadą, Wykryto nieprzetworzone incydenty związane z bezpieczeństwem, Stan urządzenia zdefiniowany przez aplikację, Zarządzanie urządzeniem nie jest możliwe, Aplikacja zabezpieczająca nie jest uruchomiona, Licencja utraciła ważność.

   W przypadku warunku **Wymagane jest ponowne uruchomienie** można określić powody ponownego uruchomienia. Zalecamy zaznaczenie pól wyboru obok wszystkich powodów z listy.

5. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Krytyczne*.

W celu włączenia zmiany stanu urządzenia na Ostrzeżenie:

1. Otwórz okno właściwości w jeden z następujących sposobów:

   - W folderze **Zasady**, w menu kontekstowym zasady Serwera administracyjnego wybierz **Właściwości**.
   - Z menu kontekstowego grupy administracyjnej wybierz **Właściwości**.

2. W oknie **Właściwości**, które zostanie otwarte, w panelu **Sekcje** wybierz **Stan urządzenia**.

3. W prawej części, w sekcji **Ustaw stan Ostrzeżenie, jeśli** zaznacz pole obok warunku na liście.

   Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

4. Kliknij dwukrotnie nazwę wybranego warunku i w otwartym oknie ustaw wymaganą wartość dla warunku.

   Nie można ustawić wartości dla następujących warunków: Aplikacja zabezpieczająca nie jest zainstalowana, Zainstalowane są niekompatybilne aplikacje, Wykryto luki w oprogramowaniu, Ustawienia urządzenia mobilnego nie są zgodne z zasadą, Wykryto nieprzetworzone incydenty związane z bezpieczeństwem, Stan urządzenia zdefiniowany przez aplikację, Zarządzanie urządzeniem nie jest możliwe, Aplikacja zabezpieczająca nie jest uruchomiona, Licencja utraciła ważność.

   W przypadku warunku **Wymagane jest ponowne uruchomienie** można określić powody ponownego uruchomienia. Zalecamy zaznaczenie pól wyboru obok wszystkich powodów z listy.

5. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Ostrzeżenie*.

Znakowanie urządzeń i przeglądanie przydzielonych znaczników

Kaspersky Security Center umożliwia znakowanie urządzeń. *Znacznik* to identyfikator urządzenia, który może zostać użyty do grupowania, opisywania lub wyszukiwania urządzeń. Znaczniki przydzielone do urządzeń mogą być użyte do tworzenia wyborów, wyszukiwania urządzeń i rozdzielania urządzeń pomiędzy grupami administracyjnymi.

Urządzenia można znakować ręcznie lub automatycznie. Oznacz urządzenie ręcznie we właściwościach urządzenia; możesz skorzystać z ręcznego znakowania, jeśli musisz oznaczyć pojedyncze urządzenie. Automatyczne znakowanie jest wykonywane przez Serwer administracyjny zgodnie z określonymi regułami znakowania.

We właściwościach Serwera administracyjnego możesz skonfigurować automatyczne znakowanie dla urządzeń zarządzanych przez ten Serwer administracyjny. Urządzenia są znakowane automatycznie, gdy spełnione są określone reguły. Każdemu znacznikowi odpowiada pojedyncza reguła. Reguły są stosowane do właściwości sieciowych urządzenia, systemu operacyjnego, aplikacji zainstalowanych na urządzeniu i innych właściwości urządzenia. Na przykład, możesz skonfigurować regułę, która przypisze znacznik *Win* do wszystkich urządzeń działających pod kontrolą systemu Windows. Następnie możesz użyć tego znacznika podczas tworzenia wyboru urządzeń; pomoże to w sortowaniu wszystkich urządzeń z systemem Windows i przypisaniu do nich zadania.

Możesz także użyć znaczników jako warunków aktywacji profilu zasad na zarządzanym urządzeniu w celu zastosowania określonych profili zasad tylko na urządzeniach z określonymi znacznikami. Na przykład, jeśli urządzenie oznaczone jako *Kurier* pojawi się w grupie administracyjnej *Użytkownicy* i jeśli została włączona aktywacja odpowiedniego profilu zasad przez znacznik *Kurier*, wówczas profil utworzony dla grupy *Użytkownicy* nie zostanie zastosowany do tego urządzenia—ale profil profilu zasad zostanie zastosowany. Profil zasad może zezwolić temu urządzeniu na uruchamianie niektórych aplikacji, których uruchamianie zostało zablokowane przez profil.

Możesz utworzyć kilka reguł znakowania. Do jednego urządzenia może zostać przypisanych kilka znaczników, jeśli utworzyłeś kilka reguł znakowania i jeśli odpowiednie warunki tych reguł są spełnione w tym samym czasie. Listę wszystkich przydzielonych znaczników można przejrzeć we właściwościach urządzenia. Każda reguła znakowania może zostać włączona lub wyłączona. Jeśli reguła jest włączona, jest ona stosowana do urządzenia zarządzanego przez Serwer administracyjny. Jeśli aktualnie nie korzystasz z reguły, ale możesz potrzebować jej w przyszłości, nie musisz jej usuwać, możesz po prostu odznaczyć pole **Włącz regułę**. W tej sytuacji reguła zostanie wyłączona; nie będzie używana, aż do ponownego zaznaczenia pola **Włącz regułę**. Konieczność wyłączenia reguły bez jej usuwania może być w przypadku, gdy chcesz tymczasowo wykluczyć regułę z listy reguł znakowania, a potem będziesz chciał znowu włączyć ją do listy.

Automatyczne znakowanie urządzeń

Możesz tworzyć i modyfikować reguły automatycznego znakowania w oknie właściwości Serwera administracyjnego.

W celu automatycznego znakowania urządzeń:

1. W drzewie konsoli wybierz węzeł z nazwą Serwera administracyjnego, dla którego musisz określić reguły znakowania.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Reguły znakowania**.
4. W sekcji **Reguły znakowania** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Nowa reguła**.
5. W oknie **Nowa reguła** skonfiguruj ogólne właściwości reguły:

   - Określ nazwę reguły.

     Nazwa reguły nie może zawierać więcej niż 255 znaków oraz nie może zawierać żadnych znaków specjalnych (takich jak `"*<>?\:|`).

   - Włącz lub wyłącz regułę, korzystając z pola **Włącz regułę**.

     Domyślnie zaznaczone jest pole **Włącz regułę**.

- W polu **Znacznik** wprowadź nazwę znacznika.

  Nazwa znacznika nie może zawierać więcej niż 255 znaków oraz nie może zawierać żadnych znaków specjalnych (takich jak `"*<>?\:|`).

6. W sekcji **Warunki** kliknij przycisk **Dodaj**, aby dodać nowy warunek, lub kliknij przycisk **Właściwości**, aby zmodyfikować istniejący warunek.

   Zostanie otwarte okno kreatora nowego warunku reguły automatycznego znakowania.

7. W oknie **Warunek przypisywania znacznika** zaznacz pola obok warunków, które mają mieć wpływ na znakowanie. Możesz określić kilka warunków.

8. W zależności od wybranego warunku przypisywania znaczników, kreator wyświetli okna, w których można skonfigurować odpowiednie warunki. Skonfiguruj wyzwalanie reguły według następujących warunków:

   - **Użycie komputera lub połączenie z określoną siecią**—właściwości sieci urządzenia, takie jak nazwa urządzenia w sieci Windows, a także uwzględnienie urządzenia w domenie lub podsieci IP.

     Jeśli dla bazy danych używanej z Kaspersky Security Center ustawione jest sortowanie z rozróżnianiem wielkości liter, zachowaj wielkość liter podczas określania nazwy DNS urządzenia. W przeciwnym razie reguła automatycznego tagowania nie będzie działać.

   - **Użycie Active Directory**—obecność urządzenia w jednostce organizacyjnej Active Directory i członkostwo urządzenia w grupie Active Directory.

   - **Określone aplikacje**—obecność Agenta sieciowego na urządzeniu oraz typ, wersja i architektura systemu operacyjnego.

   - **Maszyny wirtualne**—uwzględnienie urządzenia w określonym typie maszyn wirtualnych.

   - **Zainstalowano aplikację z rejestru aplikacji**—obecność aplikacji różnych producentów na urządzeniu.

9. Po skonfigurowaniu warunku, wprowadź jego nazwę, a następnie zamknij okno kreatora.

   Jeśli to konieczne, dla jednej reguły możesz ustawić kilka warunków. W tej sytuacji znacznik zostanie przypisany do urządzenia, jeśli spełnia przynajmniej jeden warunek. Dodane warunki będą wyświetlane w oknie właściwości reguły.

10. Kliknij **OK** w oknie **Nowa reguła**, a następnie kliknij **OK** w oknie właściwości Serwera administracyjnego.

Nowo utworzone reguły są wymuszone na urządzeniach zarządzanych przez wybrany Serwer administracyjny. Jeśli ustawienia urządzenia spełniają warunki reguły, do urządzenia zostanie przydzielony znacznik.

Przeglądanie i konfigurowanie znaczników przydzielonych do urządzenia

Możesz wyświetlić listę wszystkich znaczników, które zostały przypisane do urządzenia, a także przejść do konfiguracji reguł automatycznego znakowania w oknie właściwości urządzenia.

W celu wyświetlenia i skonfigurowania znaczników przypisanych do urządzenia:

1. W drzewie konsoli otwórz folder **Zarządzane urządzenia**.

2. W obszarze roboczym folderu **Zarządzane urządzenia** wybierz urządzenie, dla którego chcesz wyświetlić przypisane znaczniki.

3. Z menu kontekstowego urządzenia mobilnego wybierz **Właściwości**.

4. W oknie właściwości urządzenia wybierz sekcję **Znaczniki**.

   Zostanie wyświetlona lista znaczników przypisanych do wybranego urządzenia, a także sposób, w jaki każdy znacznik został przypisany: ręcznie lub zgodnie z regułą.

5. Jeśli to konieczne, wykonaj następujące czynności:

   - Aby przejść do konfiguracji reguł znakowania, kliknij odnośnik **Ustaw reguły automatycznego znakowania** (tylko dla systemu Windows).
   - Aby zmienić nazwę znacznika, zaznacz go i kliknij przycisk **Zmień nazwę**.
   - Aby usunąć nazwę znacznika, zaznacz go i kliknij przycisk **Usuń**.
   - Aby ręcznie dodać znacznik, wprowadź go w polu znajdującym się w dolnej części sekcji **Znaczniki** i kliknij przycisk **Dodaj**.

6. Jeśli w sekcji **Znaczniki** wprowadziłeś jakiekolwiek zmiany, kliknij przycisk **Zastosuj**, aby te zmiany zostały zastosowane.

7. Kliknij **OK**.

Jeśli we właściwościach urządzenia usunąłeś znacznik lub zmieniłeś jego nazwę, ta zmiana nie będzie wpływać na reguły znakowania, które zostały skonfigurowane we właściwościach Serwera administracyjnego. Zmiana zostanie zastosowana tylko na tym urządzeniu, w którego właściwościach została wprowadzona.

Zdalna diagnostyka urządzeń klienckich. Narzędzie do zdalnej diagnostyki Kaspersky Security Center

Narzędzie do zdalnej diagnostyki programu Kaspersky Security Center (zwane dalej narzędziem do zdalnej diagnostyki) zostało zaprojektowane do zdalnego wykonywania na urządzeniach klienckich następujących działań:

- Włączania i wyłączania śledzenia, zmieniania poziomu śledzenia, pobierania pliku śledzenia.
- Pobierania informacji o systemie i ustawień aplikacji.
- Pobierania dzienników zdarzeń.
- Generowania pliku zrzutu dla aplikacji.
- Uruchamiania diagnostyki i pobierania jej raportów.
- Uruchamiania i zatrzymywania działania aplikacji.

Możesz użyć dzienników zdarzeń i raportów diagnostycznych pobranych z urządzenia klienckiego do samodzielnego rozwiązania problemów. Dodatkowo, specjalista z działu pomocy technicznej Kaspersky może poprosić o pobranie plików śledzenia, plików zrzutu pamięci, dzienników zdarzeń, a także raportów diagnostycznych z urządzenia klienckiego w celu przeprowadzenia dalszej analizy w Kaspersky.

Narzędzie do zdalnej diagnostyki jest automatycznie instalowane na urządzeniu wraz z Konsolą administracyjną.

Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim

W celu połączenia narzędzia do zdalnej diagnostyki z urządzeniem klienckim:

1. Z drzewa konsoli wybierz dowolną grupę administracyjną.
2. W obszarze roboczym, na zakładce **Urządzenia**, z menu kontekstowego dowolnego urządzenia wybierz **Narzędzia użytkownika → Zdalna diagnostyka**.

   Zostanie otwarte okno główne narzędzia do zdalnej diagnostyki.
3. W pierwszym polu okna głównego narzędzia do zdalnej diagnostyki określ narzędzia, których chcesz użyć do nawiązania połączenia z urządzeniem:

   - **Dostęp przy użyciu sieci Microsoft Windows**.
   - **Dostęp przy użyciu Serwera administracyjnego**.
4. Jeżeli w pierwszym polu okna głównego narzędzia zaznaczyłeś opcję **Dostęp przy użyciu sieci Microsoft Windows**, wykonaj następujące czynności:

   - W polu **Urządzenie** określ adres urządzenia, z którym chcesz się połączyć

     Jako adresu urządzenia użyj adresu IP, nazwy NetBIOS lub nazwy DNS.

     Domyślną wartością jest adres urządzenia, z którego menu kontekstowego uruchomiono narzędzie.
   - Określ konto, z którego nawiązywane jest połączenie z urządzeniem:

     - **Połącz jako bieżący użytkownik** (wybrane domyślnie). Nawiąż połączenie, korzystając z konta bieżącego użytkownika.
     - **Do połączenia użyj nazwy użytkownika i hasła**. Nawiąż połączenie, korzystając z określonego konta użytkownika. Określ **Nazwę użytkownika** i **Hasło** żądanego konta.

     Połączenie z urządzeniem jest możliwe tylko z poziomu konta lokalnego administratora urządzenia.
5. Jeżeli w pierwszym polu okna głównego narzędzia zaznaczyłeś opcję **Dostęp przy użyciu Serwera administracyjnego**, wykonaj następujące czynności:

   - W polu **Serwer administracyjny** określ adres Serwera administracyjnego, z którego zamierzasz połączyć się z urządzeniem.

     Jako adresu serwera użyj adresu IP, nazwy NetBIOS lub nazwy DNS.

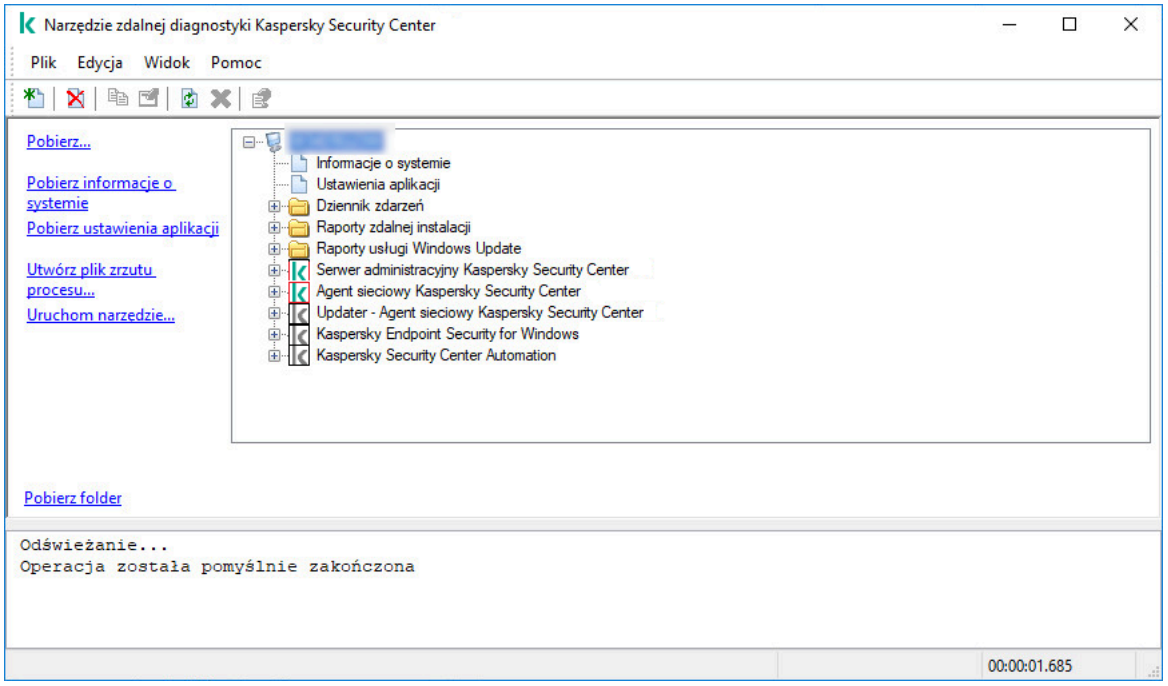
     Domyślną wartością jest adres Serwera administracyjnego, z którego uruchomiono narzędzie.
   - Jeśli jest to wymagane, zaznacz pola **Użyj SSL**, **Kompresuj ruch** oraz **Urządzenie należy do podrzędnego Serwera administracyjnego**.

     Jeżeli zaznaczone jest pole **Urządzenie należy do podrzędnego Serwera administracyjnego**, w polu **Urządzenie należy do podrzędnego Serwera administracyjnego** możesz podać nazwę podrzędnego Serwera administracyjnego, który zarządza urządzeniem, klikając przycisk **Przeglądaj**.

6. Aby połączyć się z urządzeniem, kliknij przycisk **Zaloguj się**.

Możesz przeprowadzić autoryzację z użyciem weryfikacji dwuetapowej, jeśli jest ona włączona dla Twojego konta.

Zostanie otwarte okno przeznaczone do zdalnej diagnostyki urządzenia (patrz rysunek poniżej). Lewa część okna zawiera odnośniki do działań diagnostyki urządzenia. W prawej części okna znajduje się drzewo obiektów urządzenia, którymi może zarządzać narzędzie. Dolna część okna wyświetla postęp wykonywania działań narzędzia.



Narzędzie do zdalnej diagnostyki. Okno Zdalna diagnostyka urządzeń

Narzędzie do zdalnej diagnostyki zapisuje pliki pobrane z urządzeń na pulpicie urządzenia, z którego zostało uruchomione.

Generowania pliku zrzutu dla aplikacji

Plik zrzutu dla aplikacji umożliwia przeglądanie parametrów aplikacji uruchomionej na urządzeniu klienckim w danym momencie. Ten plik zawiera również informacje o modułach, które zostały załadowane dla aplikacji.

Zbieranie zrzutów pamięci z urządzeń z systemem Linux nie jest obsługiwane.

Do zbierania zrzutów za pomocą zdalnej diagnostyki używane jest narzędzie kldumper. Narzędzie to jest przeznaczone do zbierania zrzutów procesów aplikacji Kaspersky na prośbę specjalistów pomocy technicznej. Szczegółowe informacje na temat wymagań dotyczących korzystania z narzędzia kldumper można znaleźć w bazie wiedzy Kaspersky Security Center.

Tworzenie pliku zrzutu dla aplikacji:

1. W obszarze roboczym folderu **Zarządzane urządzenia**, na karcie **Urządzenia** otwórz menu kontekstowe odpowiedniego urządzenia, a następnie wybierz opcję **Narzędzia użytkownika** → **Zdalna diagnostyka**.

   Zostanie otwarte okno **Narzędzie zdalnej diagnostyki Kaspersky Security Center**.

2. Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim.

   Zostanie otwarte okno przeznaczone do zdalnej diagnostyki urządzenia.

3. W lewej części okna kliknij łącze **Utwórz plik zrzutu procesu**.

4. W sekcji **Generowanie plik zrzutu procesu** określ plik wykonywalny aplikacji, dla której chcesz wygenerować plik zrzutu.

5. Kliknij przycisk **OK**.

Pobierane jest archiwum z plikiem zrzutu dla określonej aplikacji.

Jeśli wskazana aplikacja nie jest uruchomiona na urządzeniu klienckim, folder „result" zawarty w pobranym archiwum będzie pusty.

Jeśli określona aplikacja jest uruchomiona, ale pobieranie kończy się niepowodzeniem z powodu błędu lub folder „wynik" zawarty w pobranym archiwum jest pusty, zapoznaj się z Bazą wiedzy Kaspersky Security Center.

Włączanie i wyłączanie śledzenia, pobieranie pliku śledzenia

W celu włączenia śledzenia na zdalnym urządzeniu:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem.

2. Z drzewa obiektów urządzenia wybierz aplikację, dla której chcesz włączyć śledzenie.

   > Śledzenie może być włączane i wyłączane dla aplikacji posiadających funkcję autoochrony tylko wtedy, gdy urządzenie jest połączone przy użyciu narzędzi Serwera administracyjnego.

   Jeśli chcesz włączyć śledzenie dla Agenta sieciowego, możesz to zrobić podczas tworzenia zadania Zainstaluj wymagane aktualizacje i napraw luki. W tym przypadku Agent sieciowy zapisze informacje o śledzeniu nawet wtedy, gdy śledzenie jest wyłączone dla Agenta sieciowego w narzędziu do zdalnej diagnostyki.

3. W celu włączenia śledzenia:

   a. W lewej części okna narzędzia do zdalnej diagnostyki kliknij **Włącz śledzenie**.

   b. W otwartym oknie **Wybierz poziom śledzenia** zalecane jest zachowanie domyślnych wartości ustawień. Jeśli jest to wymagane, specjalista z pomocy technicznej przeprowadzi Cię przez proces konfiguracji. Dostępne są następujące ustawienia:

      - **Poziom śledzenia**

        Poziom śledzenia definiuje ilość szczegółów, jaką plik śledzenia zawiera.

- **Śledzenie na podstawie rotacji** (dostępne tylko dla Kaspersky Endpoint Security)

  Aplikacja nadpisuje informacje o śledzeniu, aby zapobiec nadmiernemu zwiększeniu rozmiaru pliku śledzenia. Określ maksymalną liczbę plików, jaka będzie używana do przechowywania informacji o śledzeniu, a także maksymalny rozmiar każdego pliku. Jeśli zostanie zapisana maksymalna liczba plików śledzenia o maksymalnym rozmiarze, najstarszy plik śledzenia zostanie usunięty, aby mógł zostać zapisany nowy plik śledzenia.

c. Kliknij **OK**.

4. W przypadku Kaspersky Endpoint Security specjalista z pomocy technicznej może poprosić o włączenie śledzenia Xperf dla informacji o działaniu systemu.

   W celu włączenia śledzenia Xperf:

   a. W lewej części okna narzędzia do zdalnej diagnostyki kliknij **Włącz śledzenie Xperf**.

   b. W otwartym oknie **Wybierz poziom śledzenia**, w zależności od odpowiedzi od specjalisty z pomocy technicznej, wybierz jeden z następujących poziomów śledzenia:

      - **Niski**

        Plik śledzenia tego typu zawiera minimalną ilość informacji o systemie.

        Domyślnie opcja ta jest zaznaczona.

      - **Głęboki**

        Plik śledzenia tego typu zawiera bardziej szczegółowe informacje niż pliki śledzenia typu *Niski* i specjaliści z pomocy technicznej mogą poprosić o nie, gdy plik śledzenia typu *Niski* nie jest wystarczający do oceny działania. *Głęboki* plik śledzenia zawiera informacje techniczne o systemie, w tym informacje o sprzęcie, systemie operacyjnym, listę uruchomionych i zakończonych procesów i aplikacji, zdarzeń użytych do oceny działania, a także zdarzeń z Narzędzia do oceny wydajności systemu Windows.

   c. Wybierz jeden z następujących typów śledzenia:

      - **Podstawowy**

        Informacje o śledzeniu są otrzymywane podczas działania aplikacji Kaspersky Endpoint Security.

        Domyślnie opcja ta jest zaznaczona.

      - **Po ponownym uruchomieniu**

        Informacje o śledzeniu są otrzymywane, gdy system operacyjny jest uruchamiany na zarządzanym urządzeniu. Ten typ śledzenia jest efektywny, gdy problem, który wpływa na działanie systemu, pojawi się po włączeniu urządzenia, a przed uruchomieniem Kaspersky Endpoint Security.

   d. Możesz także zostać poproszony o włączenie opcji **Śledzenie na podstawie rotacji**, aby zapobiec nadmiernemu zwiększeniu rozmiaru pliku śledzenia. Następnie określ maksymalny rozmiar pliku śledzenia. Jeśli plik osiągnie maksymalny rozmiar, najstarsze informacje śledzenia zostaną nadpisane nowymi informacjami.

   e. Kliknij **OK**.

   W niektórych przypadkach, aby włączyć śledzenie, konieczne jest ponowne uruchomienie aplikacji zabezpieczającej i jej zadania.

Narzędzie do zdalnej diagnostyki włączy śledzenie wybranej aplikacji.

W celu pobrania pliku śledzenia aplikacji:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".

2. W węźle aplikacji, w folderze **Pliki śledzenia** wybierz żądany plik.

3. W lewej części okna narzędzia do zdalnej diagnostyki kliknij **Pobierz cały plik**.

   W przypadku plików o dużym rozmiarze można pobrać ich ostatnio utworzone części.

   Podświetlony plik śledzenia może zostać usunięty. Plik może zostać usunięty po wyłączeniu śledzenia.

Wybrany plik jest pobierany do lokalizacji określonej w dolnej części okna.

W celu wyłączenia śledzenia na zdalnym urządzeniu:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".

2. W drzewie obiektów urządzenia wybierz aplikację, dla której chcesz wyłączyć śledzenie.

   > Śledzenie może być włączane i wyłączane dla aplikacji posiadających funkcję autoochrony tylko wtedy, gdy urządzenie jest połączone przy użyciu narzędzi Serwera administracyjnego.

3. W lewej części okna narzędzia do zdalnej diagnostyki kliknij **Wyłącz śledzenie**.

Narzędzie do zdalnej diagnostyki wyłączy śledzenie wybranej aplikacji.

Pobierania ustawień aplikacji

W celu pobrania ustawień aplikacji ze zdalnego urządzenia:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".

2. W drzewie obiektów okna narzędzia do zdalnej diagnostyki wybierz węzeł z nazwą urządzenia, znajdujący się na najwyższej pozycji.

3. W lewej części okna narzędzia do zdalnej diagnostyki wybierz żądane działanie z następujących opcji:

   - **Pobierz informacje o systemie**
   - **Pobierz ustawienia aplikacji**
   - **Utwórz plik zrzutu procesu**

     W oknie, które zostanie otwarte po kliknięciu tego odnośnika, określ plik wykonywalny aplikacji, dla której chcesz wygenerować plik zrzutu pamięci.

- **Uruchom narzędzie**

  W oknie, które zostanie otwarte po kliknięciu tego odnośnika, określ plik wykonywalny narzędzia, które chcesz uruchomić, oraz ustawienia jego uruchamiania.

Narzędzie zostanie pobrane i uruchomione na urządzeniu.

Pobierania dzienników zdarzeń

W celu pobrania dziennika zdarzeń ze zdalnego urządzenia:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".

2. W folderze **Dzienniki zdarzeń systemowych** drzewa obiektów urządzenia wybierz odpowiedni raport.

3. Pobierz wybrany dziennik, klikając odnośnik **Pobierz dziennik zdarzeń <nazwa dziennika zdarzeń>** w lewej części okna narzędzia do zdalnej diagnostyki.

Wybrany dziennik zdarzeń jest pobierany do lokalizacji określonej w dolnym panelu.

Pobieranie kilku elementów informacji diagnostycznych

Narzędzie do zdalnej diagnostyki Kaspersky Security Center umożliwia pobranie kilku elementów informacji diagnostycznych, w tym dzienników zdarzeń, informacji o systemie, plików śledzenia i plików zrzutów.

W celu pobrania informacji diagnostycznych ze zdalnego urządzenia:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".

2. W lewej części okna narzędzia do zdalnej diagnostyki kliknij **Pobierz**.

3. Zaznacz pola obok elementów, które chcesz pobrać.

4. Kliknij **Uruchom**.

Każdy wybrany element zostanie pobrany do lokalizacji określonej w dolnym panelu.

Uruchamianie diagnostyki i pobieranie wyników

W celu uruchomienia diagnostyki aplikacji na zdalnym urządzeniu i pobrania wyników:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".

2. Z drzewa obiektów urządzenia wybierz żądaną aplikację.

3. Uruchom diagnostykę, klikając odnośnik **Uruchom diagnostykę**, dostępny w lewej części okna narzędzia do zdalnej diagnostyki.

   W drzewie obiektów, w węźle wybranej aplikacji pojawi się raport z diagnostyki.

4. W drzewie obiektów wybierz nowo utworzony raport z diagnostyki i pobierz go, klikając odnośnik **Pobierz folder**.

Wybrany raport jest pobierany do lokalizacji określonej w dolnym panelu.

Uruchamianie, zatrzymywanie i ponowne uruchamianie aplikacji

Aplikacje mogą być uruchamiane, zatrzymywane i ponownie uruchamiane tylko wtedy, gdy połączyłeś urządzenie przy użyciu narzędzi Serwera administracyjnego.

W celu uruchomienia, zatrzymania lub ponownego uruchomienia aplikacji:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".

2. Z drzewa obiektów urządzenia wybierz żądaną aplikację.

3. W lewej części okna narzędzia do zdalnej diagnostyki wybierz działanie:

   - **Zatrzymaj aplikację**
   - **Uruchom aplikację ponownie**
   - **Uruchom aplikację**

W zależności od wybranej akcji, aplikacja zostanie uruchomiona, zatrzymana lub uruchomiona ponownie.

Urządzenia chronione UEFI

Urządzenie chronione UEFI to urządzenia z programem lub aplikacją Kaspersky dla UEFI zintegrowanymi na poziomie BIOS-u. Zintegrowana ochrona zapewnia bezpieczeństwo urządzenia od momentu uruchomienia systemu, natomiast ochrona na urządzeniach bez zintegrowanego oprogramowania zaczyna działać dopiero po uruchomieniu aplikacji zabezpieczającej. Kaspersky Security Center obsługuje zarządzanie tymi urządzeniami.

W celu zmodyfikowania ustawień połączenia urządzeń chronionych UEFI:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.

2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.

3. W oknie właściwości Serwera administracyjnego wybierz **Ustawienia połączenia z serwerem** → **Porty dodatkowe**.

4. W sekcji **Porty dodatkowe** zmodyfikuj odpowiednie ustawienia:

   - **Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS**

     Urządzenia chronione UEFI mogą nawiązywać połączenie z Serwerem administracyjnym.

- **Port dla urządzeń chronionych UEFI i urządzeń KasperskyOS**

  Możesz zmienić numer portu, jeśli opcja **Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS** jest włączona. Domyślny numer portu to 13294.

5. Kliknij **OK**.

Ustawienia zarządzanego urządzenia

W celu sprawdzenia ustawień zarządzanego urządzenia:

1. W drzewie konsoli wybierz folder **Zarządzane urządzenia**.
2. W obszarze roboczym folderu wybierz urządzenie.
3. Z otwartego menu kontekstowego urządzenia wybierz **Właściwości**.

Zostanie otwarte okno właściwości wybranego urządzenia z wybraną sekcją **Ogólne**.

Ogólne

Sekcja **Ogólne** wyświetla ogólne informacje o urządzeniu klienckim. Informacje są dostarczane w oparciu o dane otrzymane podczas ostatniej synchronizacji urządzenia klienckiego z Serwerem administracyjnym:

- **Nazwa**

  W tym polu możesz wyświetlić i zmodyfikować nazwę urządzenia klienckiego w grupie administracyjnej.

- **Opis**

  W tym polu możesz wprowadzić dodatkowy opis urządzenia klienckiego.

- **Domena Windows**

  Domena lub grupa robocza Windows, która zawiera urządzenie.

- **Nazwa NetBIOS**

  Nazwa urządzenia klienckiego w sieci Windows.

- **Nazwa DNS**

  Nazwa domeny DNS urządzenia klienckiego.

- **Adres IP**

  Adres IP urządzenia.

- **Grupa**

  Grupa administracyjna zawierająca urządzenie klienckie.

- **Ostatnia aktualizacja**

  Data ostatniej aktualizacji antywirusowych baz danych lub aplikacji na urządzeniu.

- **Ostatnio dostępny**

  Data i godzina, gdy urządzenie było ostatnio widoczne w sieci.

- **Połączono z Serwerem administracyjnym**

  Data i godzina ostatniego połączenia Agenta sieciowego, zainstalowanego na urządzeniu klienckim, z Serwerem administracyjnym.

- **Nie odłączaj od Serwera administracyjnego**

  Jeśli ta opcja jest włączona, utrzymywana jest ciągła łączność pomiędzy zarządzanym urządzeniem a Serwerem administracyjnym. Możesz użyć tej opcji, jeśli nie używasz serwerów push, które zapewniają taką łączność.

  Jeśli ta opcja jest wyłączona, a serwery push nie są używane, zarządzane urządzenie będzie nawiązywało połączenie z Serwerem administracyjnym jedynie w celu synchronizacji danych lub przesłania informacji.

  Maksymalna całkowita liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego** to 300.

  Ta opcja jest wyłączona domyślnie na zarządzanych urządzeniach. Ta opcja jest włączona domyślnie na urządzeniu, na którym jest zainstalowany Serwer administracyjny i pozostaje włączona nawet w przypadku próby jej wyłączenia.

Ochrona

Sekcja **Ochrona** zawiera informacje o bieżącym stanie ochrony antywirusowej na urządzeniu klienckim:

- **Stan urządzenia**

  Stan urządzenia klienckiego przypisany w oparciu o kryteria zdefiniowane przez administratora dla stanu ochrony antywirusowej na urządzeniu i aktywności urządzenia w sieci.

- **Wszystkie problemy**

  Ta tabela zawiera pełną listę problemów wykrytych przez zarządzane aplikacje zainstalowane na urządzeniu klienckim. Każdemu problemowi towarzyszy stan, który aplikacja sugeruje przypisać do urządzenia dla tego problemu.

- **Ochrona w czasie rzeczywistym**

  To pole wyświetla bieżący stan ochrony urządzenia klienckiego w czasie rzeczywistym.

  Jeśli stan zmieni się na urządzeniu, nowy stan zostanie wyświetlony w oknie właściwości urządzenia dopiero po zsynchronizowaniu urządzenia klienckiego z Serwerem administracyjnym.

- **Ostatnie skanowanie na żądanie**

  Data i godzina ostatniego skanowania w poszukiwaniu szkodliwego oprogramowania przeprowadzonego na urządzeniu klienckim.

- **Łączna liczba wykrytych zagrożeń**

  Całkowita liczba zagrożeń wykrytych na urządzeniu klienckim od momentu zainstalowania aplikacji zabezpieczającej (pierwsze skanowanie) lub od momentu ostatniego zresetowania licznika zagrożeń.

- **Aktywne zagrożenia**

  Liczba nieprzetworzonych plików na urządzeniu klienckim.

  To pole ignoruje liczbę nieprzetworzonych plików na urządzeniach mobilnych.

- **Stan szyfrowania dysku**

  Bieżący stan szyfrowania plików na lokalnych dyskach urządzenia. Opis statusów znajduje się w pomocy Kaspersky Endpoint Security for Windows.

Aplikacje

Sekcja **Aplikacje** wyświetla wszystkie aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim. Ta sekcja zawiera przyciski Start () i Stop () umożliwiające uruchamianie i zatrzymywanie wybranej aplikacji Kaspersky (z wyłączeniem Agenta sieciowego). Przyciski te są włączone, jeśli port UDP 15000 jest dostępny na zarządzanym urządzeniu do otrzymywania powiadomień push z Serwera administracyjnego. Jeśli zarządzane urządzenie nie jest dostępne dla powiadomień push, ale włączony jest tryb ciągłego połączenia z Serwerem administracyjnym (włączona jest opcja **Nie odłączaj od Serwera administracyjnego** w sekcji **Ogólne**), przyciski uruchom i zatrzymaj są również dostępne. Sekcja **Aplikacje** zawiera również następujące przyciski:

- **Zdarzenia**

  Kliknięcie tego przycisku wyświetla listę zdarzeń, które wystąpiły na urządzeniu klienckim podczas działania aplikacji, oraz wyświetla wyniki zadania dla tej aplikacji.

- **Statystyki**

  Kliknięcie tego przycisku wyświetla bieżące informacje statystyczne dotyczące aplikacji.

- **Właściwości**

  Po kliknięciu tego przycisku można zobaczyć informacje o aplikacji oraz skonfigurować aplikację.

Zadania

W zakładce **Zadania** możesz zarządzać zadaniami urządzenia klienckiego: przeglądać listę istniejących zadań, tworzyć nowe zadania, usuwać, uruchamiać i zatrzymywać zadania, a także modyfikować ustawienia zadań i przeglądać wyniki ich wykonania. Lista zadań jest tworzona w oparciu o dane otrzymane w czasie ostatniej synchronizacji komputera klienckiego z Serwerem administracyjnym. Serwer administracyjny żąda od urządzenia klienckiego szczegółów dotyczących stanu zadania.

Przyciski uruchom (), zatrzymaj () i usuń () są włączone, jeśli port UDP 15000 jest dostępny na zarządzanym urządzeniu do odbioru powiadomień push z Serwera administracyjnego. Jeśli zarządzane urządzenie nie jest dostępne dla powiadomień push, ale włączony jest tryb ciągłego połączenia z Serwerem administracyjnym (włączona jest opcja **Nie odłączaj od Serwera administracyjnego** w sekcji **Ogólne**), dostępne są również przyciski uruchom, zatrzymaj i usuń.

Jeżeli połączenie nie zostanie nawiązane, status zadania nie będzie wyświetlany, a przyciski będą nieaktywne.

Zdarzenia

Zakładka **Zdarzenia** wyświetla zdarzenia zarejestrowane na Serwerze administracyjnym dla wybranego urządzenia klienckiego.

Możesz eksportować, kopiować i usuwać zdarzenia urządzenia.

Znaczniki

W zakładce **Znaczniki** możesz zarządzać listą słów kluczowych, które są używane podczas wyszukiwania urządzeń klienckich: przejrzeć listę istniejących znaczników, przypisać znaczniki z listy, skonfigurować reguły automatycznego oznaczania oraz dodać nowe znaczniki i zmienić nazwy starszych znaczników, a także usunąć znaczniki.

Informacje o systemie

Sekcja **Ogólne informacje o systemie** zawiera informacje o aplikacji zainstalowanej na urządzeniu klienckim.

Rejestr aplikacji

W sekcji **Rejestr aplikacji** możesz przejrzeć rejestr aplikacji zainstalowanych na urządzeniu klienckim i ich uaktualnień, a także możesz skonfigurować wyświetlanie rejestru aplikacji.

Informacje o zainstalowanych aplikacjach są dostępne, jeśli Agent sieciowy zainstalowany na urządzeniu klienckim prześle żądane informacje do Serwera administracyjnego. Możesz skonfigurować przesyłanie informacji do Serwera administracyjnego w oknie właściwości Agenta sieciowego lub jego zasady, w sekcji **Repozytoria**.

- **Wyświetl tylko niekompatybilne aplikacje zabezpieczające**

  Jeśli ta opcja jest włączona, lista aplikacji zawiera tylko te aplikacje zabezpieczające, które są niekompatybilne z aplikacjami firmy Kaspersky.

  Domyślnie opcja ta jest wyłączona.

- **Pokaż uaktualnienia**

  Jeśli ta opcja jest włączona, lista aplikacji zawiera nie tylko aplikacje, ale także zainstalowane dla nich pakiety aktualizacyjne.

  Aby wyświetlić listę aktualizacji, potrzebne jest 100 KB ruchu. Jeśli zamkniesz listę i otworzysz ją ponownie, będziesz musiał ponownie poświęcić 100 KB ruchu internetowego.

  Domyślnie opcja ta jest wyłączona.

- **Eksportuj do pliku**

  Kliknij ten przycisk, aby wyeksportować listę aplikacji zainstalowanych na urządzeniu do pliku CSV lub TXT.

- **Historia**

  Kliknij ten przycisk, aby przejrzeć zdarzenia dotyczące instalacji aplikacji na urządzeniu. Wyświetlane są następujące informacje:

  - Data i godzina zainstalowania aplikacji na urządzeniu
  - Nazwa aplikacji
  - Wersja aplikacji

- **Właściwości**

  Kliknij ten przycisk, aby przejrzeć właściwości aplikacji wybranej na liście aplikacji zainstalowanych na urządzeniu. Wyświetlane są następujące informacje:

  - Nazwa aplikacji
  - Wersja aplikacji
  - Producent aplikacji

Pliki wykonywalne

Sekcja **Pliki wykonywalne** wyświetla pliki wykonywalne wykryte na urządzeniu klienckim.

Rejestrze sprzętu

W sekcji **Rejestr sprzętu** możesz wyświetlić informacje o sprzęcie zainstalowanym na urządzeniu klienckim. Możesz przejrzeć informacje dla urządzeń z systemem Windows oraz urządzeń z systemem Linux.

Upewnij się, że narzędzie lshw jest zainstalowane na urządzeniach z systemem Linux, z których chcesz pobrać szczegółowe informacje o sprzęcie. Szczegóły dot. sprzętu przechwycone z maszyn wirtualnych mogą być niekompletne, w zależności od używanego hiperwizora.

Jeżeli Agent sieciowy jest zainstalowany na urządzeniu z systemem Windows, wysyła on do Serwera administracyjnego następujące informacje o sprzęcie urządzenia:

- Pamięć RAM
- Urządzenia pamięci masowej
- Płyta główna
- Procesor
- Karty sieciowe
- Monitory

- Karta graficzna
- Karta dźwiękowa

Jeżeli Agent sieciowy jest zainstalowany na urządzeniu z systemem Linux lub macOS, wysyła on do Serwera administracyjnego następujące informacje o sprzęcie urządzenia, jeżeli informacje te są dostarczane przez system operacyjny:

- Całkowita ilość pamięci RAM
- Całkowita pojemność urządzeń pamięci masowej
- Płyta główna
- Procesor
- Karty sieciowe

Sesje

Sekcja **Sesje** wyświetla wyłącznie w odniesieniu do urządzeń Windows informacje dotyczące właściciela urządzenia klienckiego, a także kont użytkowników, którzy pracowali na wybranym urządzeniu klienckim.

Informacje o użytkownikach domeny są generowane w oparciu o dane Active Directory. Szczegóły dotyczące użytkowników lokalnych są dostępne w Menedżerze konta zabezpieczeń Windows, zainstalowanym na urządzeniu klienckim.

- **Właściciel urządzenia**

  Pole **Właściciel urządzenia** wyświetla nazwę użytkownika, z którym administrator może się skontaktować, gdy zajdzie potrzeba wykonania określonych działań na urządzeniu klienckim.

  Użyj przycisków **Przypisz** i **Właściwości**, aby wybrać właściciela urządzenia oraz wyświetlić informacje o użytkowniku, który został wskazany jako właściciel urządzenia.

  Użyj przycisku z czerwonym krzyżykiem, aby usunąć aktualnego właściciela urządzenia.

Lista wyświetla konta użytkowników, którzy korzystają z urządzenia klienckiego.

- **Nazwa**

  Nazwa urządzenia w sieci Windows.

- **Nazwa uczestnika**

  Nazwa (domena lub nazwa lokalna) użytkownika, który logował się do systemu tego urządzenia.

- **Konto**

  Konto użytkownika, który logował się na tym urządzeniu.

- **E-mail**

  Adres e-mail użytkownika.

- **Telefon**

  Numer telefonu użytkownika.

Incydenty związane z bezpieczeństwem

Na zakładce **Incydenty związane z bezpieczeństwem** możesz przejrzeć, zmodyfikować i utworzyć incydenty związane z bezpieczeństwem dla urządzenia klienckiego. Problemy bezpieczeństwa mogą być tworzone automatycznie poprzez zarządzane aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim, a także ręcznie przez administratora. Na przykład, jeśli niektórzy użytkownicy regularnie przenoszą szkodliwe oprogramowanie ze swoich nośników wymiennych na urządzenia, administrator może utworzyć problem bezpieczeństwa. W treści problemu bezpieczeństwa administrator może dostarczyć krótki opis przypadku oraz zalecane działania (na przykład działania dyscyplinarne wobec użytkownika), a także dodać odsyłacz.

Problem bezpieczeństwa, dla którego zostały wykonane wszystkie wymagane działania, nazywane jest *przetworzonym*. Obecność nieprzetworzonych problemów bezpieczeństwa może zostać wybrana jako warunek zmiany stanu urządzenia na *Krytyczny* lub *Ostrzeżenie*.

Ta sekcja zawiera listę problemów bezpieczeństwa, które zostały utworzone dla urządzenia. Problemy bezpieczeństwa są klasyfikowane według priorytetu i typu. Typ incydentu związanego z bezpieczeństwem jest definiowany przez aplikację Kaspersky, która utworzyła incydent związany z bezpieczeństwem. Możesz podświetlić przetworzone zdarzenia na liście, zaznaczając pole w kolumnie **Przetworzone**.

Luki w oprogramowaniu

Sekcja **Luki w oprogramowaniu** zawiera informacje o lukach w aplikacjach firm trzecich zainstalowanych na urządzeniach klienckich. Do wyszukiwania luk po nazwie możesz użyć pola wyszukiwania znajdującego się nad listą.

- **Eksportuj do pliku**

  Kliknij przycisk **Eksportuj do pliku**, aby zapisać listę luk do pliku. Domyślnie aplikacja eksportuje listę luk do pliku CSV.

- **Pokaż tylko luki, które można naprawić**

  Jeśli ta opcja jest włączona, sekcja wyświetla luki, które można naprawić przy użyciu poprawki.

  Jeśli ta opcja jest wyłączona, sekcja wyświetla luki, które można wyeliminować przy użyciu poprawki, oraz luki, dla których nie opublikowano poprawki.

  Domyślnie opcja ta jest włączona.

- **Właściwości**

  Na liście wybierz lukę w oprogramowaniu i kliknij przycisk **Właściwości**, aby przejrzeć właściwości wybranej luki w oprogramowaniu w oddzielnym oknie. W oknie możesz wykonać następujące czynności:

  - Zignoruj lukę w oprogramowaniu na tym zarządzanym urządzeniu (w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console).
  - Przejrzyj listę zalecanych poprawek dla luki.
  - Ręcznie określ aktualizacje oprogramowania, aby naprawić lukę (w Konsoli administracyjnej lub w Kaspersky Security Center Web Console).

- Przejrzyj instancje luki.
- Przejrzyj listę istniejących zadań, aby naprawić lukę i utworzyć nowe zadania w celu wyeliminowania luki.

Dostępne aktualizacje

Sekcja ta wyświetla listę aktualizacji oprogramowania znajdujących się na tym urządzeniu, ale jeszcze nie zainstalowanych. Informacje o opcjonalnych aktualizacjach Microsoft Windows nie są wysyłane do Serwera administracyjnego.

- **Pokaż zainstalowane aktualizacje**

  Jeśli ta opcja jest włączona, lista wyświetla uaktualnienia, które nie zostały zainstalowane oraz te, które zostały już zainstalowane na urządzeniu klienckim.

  Domyślnie opcja ta jest wyłączona.

Zasady aktywne

Ta sekcja wyświetla listę zasad aplikacji firmy Kaspersky aktualnie przypisanych do tego urządzenia.

- **Eksportuj do pliku**

  Kliknij przycisk **Eksportuj do pliku**, aby zapisać listę aktywnych zasad do pliku. Domyślnie aplikacja eksportuje listę zasad do pliku CSV.

Aktywne profile zasad

- **Aktywne profile zasad**

  Lista umożliwia przejrzenie informacji o istniejących profilach zasad, które są aktywne na urządzeniach klienckich. Aby odszukać aktywne profile zasad na liście, można użyć paska wyszukiwania znajdującego się nad listą, w którym należy wprowadzić nazwę zasady lub nazwę profilu zasad.

- **Eksportuj do pliku**

  Kliknij przycisk **Eksportuj do pliku**, aby zapisać listę aktywnych profili zasad do pliku. Domyślnie aplikacja eksportuje listę profili zasad do pliku CSV.

Punkty dystrybucji

Ta sekcja zawiera listę punktów dystrybucji, z którymi urządzenie komunikuje się.

- **Eksportuj do pliku**

  Kliknij przycisk **Eksportuj do pliku**, aby zapisać do pliku listę punktów dystrybucji, z którymi urządzenie komunikuje się. Domyślnie aplikacja eksportuje listę urządzeń do pliku CSV.

- **Właściwości**

  Kliknij przycisk **Właściwości**, aby przejrzeć i skonfigurować punkt dystrybucji, z którym urządzenie komunikuje się.

Ogólne ustawienia zasady

Ogólne

W sekcji **Ogólne** możesz zmodyfikować stan zasady oraz określić dziedziczenie ustawień zasady:

- W sekcji **Stan zasady** możesz wybrać jeden z trybów zasady:

  - **Zasada aktywna**

    Jeśli wybrano tę opcję, zasada jest aktywna.

    Domyślnie opcja ta jest zaznaczona.

  - **Zasada użytkownika mobilnego**

    Jeżeli ta opcja jest zaznaczona, zasada stanie się aktywna, gdy urządzenie znajdzie się poza siecią korporacyjną.

  - **Zasada nieaktywna**

    Jeśli ta opcja jest zaznaczona, zasada stanie się nieaktywna, ale wciąż będzie przechowywana w folderze **Zasady**. Jeśli jest to wymagane, zasadę można aktywować.

- W grupie ustawień **Dziedziczenie ustawień** możesz skonfigurować dziedziczenie zasady:

  - **Dziedzicz ustawienia z zasady nadrzędnej**

    Jeśli ta opcja jest włączona, wartości ustawień zasady są dziedziczone z zasady grupy najwyższego poziomu, są więc zablokowane.

    Domyślnie opcja ta jest włączona.

  - **Wymuś dziedziczenie ustawień w zasadach podrzędnych**

    Jeśli ta opcja jest włączona, po zastosowaniu zmian w zasadzie zostaną wykonane następujące czynności:

    - Wartości ustawień zasady zostaną rozesłane do zasad podgrup administracyjnych, czyli do zasad podrzędnych.

    - Opcja **Dziedzicz ustawienia z zasady nadrzędnej** będzie automatycznie włączona w podsekcji **Dziedziczenie ustawień** sekcji **Ogólne** okna właściwości każdej zasady podrzędnej.

    Jeśli ta opcja jest włączona, ustawienia zasad podrzędnych są zablokowane.

    Domyślnie opcja ta jest wyłączona.

Konfiguracja zdarzenia

Sekcja **Konfiguracja zdarzenia** umożliwia skonfigurowanie zapisywania zdarzeń oraz powiadamiania o zdarzeniach. Zdarzenia są grupowane według istotności na następujących zakładkach:

- **Krytyczny**

  Zakładka **Krytyczny** nie jest wyświetlana we właściwościach zasady Agenta sieciowego.

- **Błąd funkcjonalny**
- **Ostrzeżenie**
- **Informacja**

Na każdej zakładce, lista wyświetla typy zdarzeń oraz domyślny okres przechowywania zdarzeń na Serwerze administracyjnym (w dniach). Kliknięcie przycisku **Właściwości** umożliwia określenie ustawień zapisywania zdarzeń oraz powiadomień o zdarzeniach wybranych z listy. Domyślnie, podstawowe ustawienia powiadamiania, określone dla całego Serwera administracyjnego, są używane dla wszystkich typów zdarzeń. Jednakże możesz zmienić określone ustawienia dla żądanych typów zdarzeń.

Na przykład, na zakładce **Ostrzeżenie** możesz skonfigurować typ zdarzenia **Wystąpił incydent związany z bezpieczeństwem**. Takie zdarzenia mogą mieć miejsce, na przykład, gdy wolne miejsce na dysku punktu dystrybucji jest mniejsze niż 2 GB (co najmniej 4 GB są wymagane do zdalnego instalowania aplikacji i pobierania aktualizacji). Aby skonfigurować zdarzenie **Wystąpił incydent związany z bezpieczeństwem**, wybierz je i kliknij przycisk **Właściwości**. Następnie możesz określić, gdzie mają być przechowywane zdarzenia i jak o nich powiadamiać.

Jeśli Agent sieciowy wykrył problem bezpieczeństwa, możesz nim zarządzać za pomocą ustawień zarządzanego urządzenia.

Aby wybrać kilka typów zdarzeń, użyj klawisza **Shift** lub **Ctrl**; aby wybrać wszystkie typy, użyj przycisku **Wybierz wszystkie**.

Ustawienia zasady Agenta sieciowego

W celu skonfigurowania zasady Agenta sieciowego:

1. Z drzewa konsoli wybierz folder **Zasady**.
2. W obszarze roboczym folderu wybierz zasadę Agenta sieciowego.
3. Z otwartego menu kontekstowego zasady wybierz **Właściwości**.

Zostanie otwarte okno właściwości zasady Agenta sieciowego.

Zobacz tabelę porównawczą, w której szczegółowo opisano, jak poniższe ustawienia mają zastosowanie w zależności od używanego systemu operacyjnego.

Ogólne

W sekcji **Ogólne** możesz zmodyfikować stan zasady oraz określić dziedziczenie ustawień zasady:

- W sekcji **Stan zasady** możesz wybrać jeden z trybów zasady:
  - **Zasada aktywna**

    Jeśli wybrano tę opcję, zasada jest aktywna.

    Domyślnie opcja ta jest zaznaczona.
  - **Zasada użytkownika mobilnego**

    Jeżeli ta opcja jest zaznaczona, zasada stanie się aktywna, gdy urządzenie znajdzie się poza siecią korporacyjną.
  - **Zasada nieaktywna**

    Jeśli ta opcja jest zaznaczona, zasada stanie się nieaktywna, ale wciąż będzie przechowywana w folderze **Zasady**. Jeśli jest to wymagane, zasadę można aktywować.
- W grupie ustawień **Dziedziczenie ustawień** możesz skonfigurować dziedziczenie zasady:
  - **Dziedzicz ustawienia z zasady nadrzędnej**

    Jeśli ta opcja jest włączona, wartości ustawień zasady są dziedziczone z zasady grupy najwyższego poziomu, są więc zablokowane.

    Domyślnie opcja ta jest włączona.
  - **Wymuś dziedziczenie ustawień w zasadach podrzędnych**

    Jeśli ta opcja jest włączona, po zastosowaniu zmian w zasadzie zostaną wykonane następujące czynności:
    - Wartości ustawień zasady zostaną rozesłane do zasad podgrup administracyjnych, czyli do zasad podrzędnych.
    - Opcja **Dziedzicz ustawienia z zasady nadrzędnej** będzie automatycznie włączona w podsekcji **Dziedziczenie ustawień** sekcji **Ogólne** okna właściwości każdej zasady podrzędnej.

    Jeśli ta opcja jest włączona, ustawienia zasad podrzędnych są zablokowane.

    Domyślnie opcja ta jest wyłączona.

Konfiguracja zdarzenia

Sekcja **Konfiguracja zdarzenia** umożliwia skonfigurowanie zapisywania zdarzeń oraz powiadamiania o zdarzeniach. Zdarzenia są grupowane według istotności na następujących zakładkach:

- **Krytyczny**

  Zakładka **Krytyczny** nie jest wyświetlana we właściwościach zasady Agenta sieciowego.
- **Błąd funkcjonalny**

- **Ostrzeżenie**
- **Informacja**

Na każdej zakładce, lista wyświetla typy zdarzeń oraz domyślny okres przechowywania zdarzeń na Serwerze administracyjnym (w dniach). Kliknięcie przycisku **Właściwości** umożliwia określenie ustawień zapisywania zdarzeń oraz powiadomień o zdarzeniach wybranych z listy. Domyślnie, podstawowe ustawienia powiadamiania, określone dla całego Serwera administracyjnego, są używane dla wszystkich typów zdarzeń. Jednakże możesz zmienić określone ustawienia dla żądanych typów zdarzeń.

Na przykład, na zakładce **Ostrzeżenie** możesz skonfigurować typ zdarzenia **Wystąpił incydent związany z bezpieczeństwem**. Takie zdarzenia mogą mieć miejsce, na przykład, gdy wolne miejsce na dysku punktu dystrybucji jest mniejsze niż 2 GB (co najmniej 4 GB są wymagane do zdalnego instalowania aplikacji i pobierania aktualizacji). Aby skonfigurować zdarzenie **Wystąpił incydent związany z bezpieczeństwem**, wybierz je i kliknij przycisk **Właściwości**. Następnie możesz określić, gdzie mają być przechowywane zdarzenia i jak o nich powiadamiać.

Jeśli Agent sieciowy wykrył problem bezpieczeństwa, możesz nim zarządzać za pomocą ustawień zarządzanego urządzenia.

Aby wybrać kilka typów zdarzeń, użyj klawisza **Shift** lub **Ctrl**; aby wybrać wszystkie typy, użyj przycisku **Wybierz wszystkie**.

Ustawienia

W sekcji **Ustawienia** możesz skonfigurować zasadę Agenta sieciowego:

- **Rozsyłaj pliki tylko poprzez punkty dystrybucji**

  Jeśli ta opcja jest włączona, Agenty sieciowe na zarządzanych urządzeniach pobierają uaktualnienia tylko z punktów dystrybucji.

  Jeśli ta opcja jest wyłączona, Agenty sieciowe na zarządzanych urządzeniach pobierają uaktualnienia z punktów dystrybucji lub z Serwera administracyjnego.

  > Należy pamiętać, że aplikacje zabezpieczające na zarządzanych urządzeniach pobierają uaktualnienia ze źródła ustawionego w zadaniu aktualizacji dla każdej aplikacji zabezpieczającej. Jeśli włączysz opcję **Rozsyłaj pliki tylko poprzez punkty dystrybucji**, upewnij się, że Kaspersky Security Center jest ustawiony jako źródło uaktualnień w zadaniach aktualizacji.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar kolejki zdarzeń, w MB**

  W tym polu możesz określić maksymalny rozmiar przestrzeni dyskowej zajmowanej przez kolejkę zdarzenia.

  Domyślna wartość to 2 megabajty (MB).

- **Aplikacja może pobierać rozszerzone dane zasad na urządzenie**

  Agent sieciowy zainstalowany na zarządzanym urządzeniu przesyła informacje o zastosowanej zasadzie aplikacji zabezpieczającej (na przykład, Kaspersky Endpoint Security for Windows). Przesłane informacje możesz przejrzeć w interfejsie aplikacji zabezpieczającej.

Agent sieciowy przesyła następujące informacje:

- Czas dostarczenia zasady na zarządzane urządzenie.
- Nazwę aktywnej zasady w momencie dostarczenia zasady na zarządzane urządzenie.
- Nazwę zasady użytkowania mobilnego w momencie dostarczenia jej do zarządzanego urządzenia (niedostępna dla Agenta sieciowego dla systemu Linux).
- Nazwę i pełną ścieżkę do grupy administracyjnej, która zawierała zarządzane urządzenie w momencie dostarczenia zasady na zarządzane urządzenie.
- Listę aktywnych profili zasad wraz z ich nazwami i priorytetami w momencie dostarczenia zasad do zarządzanego urządzenia.

Możesz użyć informacji, aby zapewnić, że poprawna zasada zostanie zastosowana do urządzenia oraz aby rozwiązać problemy. Domyślnie opcja ta jest wyłączona.

- **Chroń usługę Agenta sieciowego przed nieuprawnionym usuwaniem, zatrzymywaniem i zmianami ustawień**

  Gdy ta opcja pozostaje aktywna, po zainstalowaniu Agenta sieciowego na zarządzanym urządzeniu, składnik nie może zostać usunięty ani ponownie skonfigurowany bez wymaganych uprawnień. Usługa Agenta sieciowego nie może zostać zatrzymana. Ta opcja nie ma wpływu na kontrolery domeny.

  Włącz tę opcję, aby chronić Agenta sieciowego na stacjach roboczych obsługiwanych z uprawnieniami lokalnego administratora.

  Domyślnie opcja ta jest wyłączona.

- **Użyj hasła dezinstalacyjnego**

  Jeśli ta opcja jest włączona, klikając przycisk **Modyfikuj**, można określić hasło do narzędzia klmover i zdalnej dezinstalacji Agenta sieciowego.

  Domyślnie opcja ta jest wyłączona.

Repozytoria

W sekcji **Repozytoria** możesz wybrać typy obiektów, których szczegóły zostaną wysłane z Agenta sieciowego na Serwer administracyjny:

- **Szczegóły aktualizacji Windows Update**

  Jeśli ta opcja jest włączona, informacje o aktualizacjach Microsoft Windows Update, które powinny zostać zainstalowane na urządzeniach klienckich, są przesyłane do Serwera administracyjnego.

  Czasami, nawet wtedy, gdy opcja jest wyłączona, aktualizacje są wyświetlanie we właściwościach urządzenia w sekcji **Dostępne aktualizacje**. To może mieć miejsce, gdy, na przykład, urządzenia w organizacji zawierają luki, które mogłyby zostać wyeliminowane przez te aktualizacje.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

  Informacje o opcjonalnych aktualizacjach Microsoft Windows nie są wysyłane do Serwera administracyjnego.

- **Szczegóły luk w oprogramowaniu oraz odpowiednich aktualizacji**

  Jeśli ta opcja jest włączona, informacje o lukach w oprogramowaniu innej firmy (w tym oprogramowaniu firmy Microsoft), wykrytych na zarządzanych urządzeniach, oraz o aktualizacjach oprogramowania, które eliminują luki innych firm (nie dotyczy oprogramowania firmy Microsoft) są wysyłane do Serwera administracyjnego.

Wybranie tej opcji (**Szczegóły luk w oprogramowaniu oraz odpowiednich aktualizacji**) zwiększy obciążenie sieci, obciążenie dysku Serwera administracyjnego oraz zużycie zasobów Agenta sieciowego.

Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

Aby zarządzać aktualizacjami oprogramowania firmy Microsoft, użyj opcji **Szczegóły aktualizacji Windows Update**.

- **Szczegóły rejestru sprzętu**

  Agent sieciowy zainstalowany na urządzeniu wysyła informacje o sprzęcie urządzenia do Serwera administracyjnego. Możesz przejrzeć szczegóły sprzętu we właściwościach urządzenia.

  Upewnij się, że narzędzie lshw jest zainstalowane na urządzeniach z systemem Linux, z których chcesz pobrać szczegółowe informacje o sprzęcie. Szczegóły dot. sprzętu przechwycone z maszyn wirtualnych mogą być niekompletne, w zależności od używanego hiperwizora.

- **Szczegóły zainstalowanych aplikacji**

  Jeśli ta opcja jest włączona, informacje o aplikacjach zainstalowanych na urządzeniach klienckich są przesyłane do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Dołącz informacje o poprawkach**

  Informacje o poprawkach aplikacji zainstalowanych na urządzeniach klienckich są wysyłane do Serwera administracyjnego. Włączenie tej opcji może zwiększyć obciążenie na Serwerze administracyjnym oraz DBMS, a także spowodować zwiększenie rozmiaru bazy danych.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

Jeśli modyfikacja niektórych ustawień w tej sekcji jest zablokowana przez zasadę Agenta sieciowego, nie można ich modyfikować.

Okno Aktualizacje oprogramowania i luki

W sekcji **Aktualizacje oprogramowania i luki** możesz skonfigurować wyszukiwanie i rozsyłanie aktualizacji systemu Windows, a także włączyć skanowanie plików wykonywalnych w poszukiwaniu luk:

- **Użyj Serwera administracyjnego jako serwera WSUS**

  Jeśli ta opcja jest włączona, aktualizacje systemu Windows są pobierane na Serwer administracyjny. Serwer administracyjny dostarcza pobrane aktualizacje usłudze Windows Update na urządzeniach klienckich w trybie scentralizowanym przy użyciu Agentów sieciowych.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie używany do pobierania aktualizacji systemu Windows. W tym przypadku urządzenia klienckie same pobierają aktualizacje systemu Windows.

  Domyślnie opcja ta jest wyłączona.

- Pod sekcją **Zezwalaj użytkownikom na zarządzanie instalowaniem aktualizacji Windows Update** możesz ograniczyć aktualizacje Windows, które użytkownicy mogą ręcznie instalować na swoich urządzeniach przy użyciu Windows Update.

Na urządzeniach działających pod kontrolą systemu Windows 10, jeśli usługa Windows Update już wykryła aktualizacje dla urządzenia, nowa opcja, którą wybierzesz w sekcji **Zezwalaj użytkownikom na zarządzanie instalowaniem aktualizacji Windows Update**, zostaną zastosowane dopiero po zainstalowaniu wykrytych aktualizacji.

Wybierz element z listy rozwijalnej:

- **Zezwalaj użytkownikom na instalację wszystkich dostępnych aktualizacji Windows Update**

  Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach.

  Wybierz tę opcję, jeśli nie chcesz uczestniczyć w instalacji aktualizacji.

  Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

- **Zezwalaj użytkownikom na instalację wszystkich zatwierdzonych aktualizacji Windows Update**

  Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach i które zostały zatwierdzone przez Ciebie.

  Na przykład, możesz chcieć najpierw sprawdzić instalację aktualizacji w środowisku testowym i upewnić się, że nie wpływają negatywnie na działanie urządzeń, a następnie zezwolić na instalację tylko tych zatwierdzonych aktualizacji.

  Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

- **Nie zezwalaj użytkownikom na instalowanie aktualizacji Windows Update**

  Użytkownicy nie mogą ręcznie zainstalować aktualizacji Microsoft Windows Update na swoich urządzeniach. Wszystkie stosowane aktualizacje są instalowane w sposób skonfigurowany przez Ciebie.

  Wybierz tę opcję, jeśli chcesz zarządzać instalacją aktualizacji w sposób scentralizowany.

  Na przykład, możesz chcieć zoptymalizować terminarz aktualizacji, aby sieć nie została przeciążona. Możesz skonfigurować terminarz aktualizacji po godzinach, aby nie przeszkadzały w pracy użytkowników.

- W grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** możesz wybrać tryb wyszukiwania aktualizacji:

  - **Aktywny**

    Jeśli ta opcja jest zaznaczona, Serwer administracyjny z pomocą Agenta sieciowego przesyła żądanie z Agenta Windows Update na urządzeniu klienckim do źródła uaktualnień: Serwery Windows Update lub WSUS. Następnie Agent sieciowy przesyła informacje z usługi Windows Update Agent do Serwera administracyjnego.

    Opcja zaczyna działać tylko wtedy, gdy zaznaczona jest opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

Domyślnie opcja ta jest zaznaczona.

- **Pasywny**

  Jeżeli ta opcja jest zaznaczona, Agent sieciowy co jakiś czas przesyła informacje od Serwera administracyjnego dotyczące aktualizacji pobranych przy ostatniej synchronizacji agenta usługi Windows Update ze źródłem uaktualnień. Jeśli nie zostanie przeprowadzona synchronizacja agenta usługi Windows Update ze źródłem uaktualnień, informacje o aktualizacjach Serwera administracyjnego będą przestarzałe.

  Wybierz tę opcję, jeśli chcesz uzyskać aktualizacje z pamięci podręcznej źródła uaktualnień.

- **Wyłączony**

  Jeśli ta opcja jest zaznaczona, Serwer administracyjny nie żąda informacji dotyczących aktualizacji.

  Wybierz tę opcję, gdy, na przykład, chcesz najpierw przetestować aktualizacje na swoim lokalnym urządzeniu.

- **Skanuj pliki wykonywalne w poszukiwaniu luk podczas ich uruchamiania**

  Jeśli ta opcja jest włączona, pliki wykonywalne są skanowane w poszukiwaniu luk podczas ich uruchamiania.

  Domyślnie opcja ta jest włączona.

Zarządzanie ponownym uruchomieniem

W sekcji **Zarządzanie ponownym uruchamianiem** możesz określić działanie, jakie zostanie wykonane, jeśli system operacyjny urządzenia zarządzanego musi być uruchomiony ponownie, gdy korzystasz, instalujesz lub dezinstalujesz aplikację:

- **Nie uruchamiaj ponownie systemu operacyjnego**

  System operacyjny nie zostanie uruchomiony ponownie.

- **Jeżeli będzie to wymagane, automatycznie uruchom ponownie system operacyjny**

  Jeśli jest to konieczne, system operacyjny zostanie automatycznie uruchomiony ponownie.

- **Pytaj użytkownika o akcję**

  Aplikacja pyta użytkownika o pozwolenie na ponowne uruchomienie systemu operacyjnego.

  Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja pyta użytkownika o pozwolenie na ponowne uruchomienie systemu operacyjnego z częstotliwością określoną w polu znajdującym się obok pola do zaznaczenia. Domyślnie częstotliwość wyświetlania pytania wynosi 5 minut.

    Jeśli ta opcja jest wyłączona, aplikacja nie ponawia pytania o pozwolenie na ponowne uruchomienie systemu.

    Domyślnie opcja ta jest włączona.

  - **Wymuś restart po (min)**

    Jeśli ta opcja jest włączona, po wyświetleniu pytania, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu czasu określonego w polu znajdującym się obok pola do zaznaczenia.

    Jeśli ta opcja jest wyłączona, aplikacja nie wymusza ponownego uruchomienia systemu.

    Domyślnie opcja ta jest włączona.

- **Czas oczekiwania przed wymuszeniem zamknięcia aplikacji dla zablokowanych sesji (min)**

  Wymuszone zamknięcie aplikacji ma miejsce, gdy urządzenie użytkownika jest zablokowane (automatycznie po określonym czasie nieaktywności lub ręcznie).

  Jeśli ta opcja jest włączona, wymuszone zamknięcie aplikacji na zablokowanym urządzeniu odbywa się po minięciu czasu określonego w polu wejściowym.

  Jeśli ta opcja jest wyłączona, aplikacje nie będą zamykane na zablokowanym urządzeniu.

  Domyślnie opcja ta jest wyłączona.

Udostępnianie pulpitu Windows

W sekcji **Udostępnianie pulpitu Windows** możesz włączyć i skonfigurować audyt działań administratora wykonywanych na zdalnym urządzeniu podczas współdzielenia dostępu do pulpitu:

- **Włącz audyt**

  Jeśli ta opcja jest włączona, audyt działań administratora na zdalnym urządzeniu jest włączony. Wpisy dotyczące działań administratora na zdalnym urządzeniu są zapisywane w:

  - Raporcie zdarzeń na zdalnym urządzeniu
  - W pliku z rozszerzeniem syslog, znajdującym się w folderze instalacyjnym Agenta sieciowego na zdalnym urządzeniu
  - W bazie danych zdarzeń programu Kaspersky Security Center

  Audyt działań administratora jest dostępny, gdy są spełnione następujące warunki:

  - Licencja Zarządzanie lukami i poprawkami jest w użyciu
  - Administrator posiada uprawnienie do włączania współdzielonego dostępu do pulpitu zdalnego urządzenia

  Jeśli ta opcja jest wyłączona, audyt działań administratora na zdalnym urządzeniu jest wyłączony.

  Domyślnie opcja ta jest wyłączona.

- **Maski plików, które będą monitorowane podczas odczytu**

  Lista zawiera maski plików. Jeśli audyt jest włączony, aplikacja monitoruje odczytywanie plików przez administratora, które odpowiadają maskom, i zapisuje informacje o odczycie plików. Lista jest dostępna, jeśli pole **Włącz audyt** jest zaznaczone. Możesz zmodyfikować maski plików i dodać nowe do listy. Każda nowa maska pliku powinna być określona na liście w nowym wierszu.

  Domyślnie określone są następujące maski plików:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Maski plików, które będą monitorowane podczas modyfikacji**

  Lista zawiera maski plików na zdalnym urządzeniu. Jeśli audyt jest włączony, aplikacja monitoruje zmiany wprowadzone przez administratora w plikach, które odpowiadają maskom, i zapisuje informacje o tych modyfikacjach. Lista jest dostępna, jeśli pole **Włącz audyt** jest zaznaczone. Możesz zmodyfikować maski plików i dodać nowe do listy. Każda nowa maska pliku powinna być określona na liście w nowym wierszu.

  Domyślnie określone są następujące maski plików:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Zarządzaj poprawkami i aktualizacjami

W sekcji **Zarządzaj poprawkami i aktualizacjami** możesz skonfigurować pobieranie i dystrybucję uaktualnień oraz instalację poprawek na zarządzanych urządzeniach:

- **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**

  Jeśli ta opcja jest włączona, poprawki Kaspersky ze stanem zatwierdzenia *Niezdefiniowane* będą automatycznie instalowane na zarządzanych urządzeniach natychmiast po pobraniu z serwerów aktualizacji.

  Jeśli ta opcja jest wyłączona, poprawki Kaspersky, które zostały pobrane i oznaczone jako *Niezdefiniowane*, zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzone*.

  Domyślnie opcja ta jest włączona.

- **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)**

  Jeśli ta opcja jest włączona, tryb offline pobierania aktualizacji jest używany. Jeśli Serwer administracyjny pobierze uaktualnienia, powiadomi Agenta sieciowego (na urządzeniach, na których jest zainstalowany) o uaktualnieniach, które będą wymagane dla zarządzanych aplikacji. Jeśli Agent sieciowy otrzyma informacje o tych uaktualnieniach, pobierze odpowiednie pliki z Serwera administracyjnego z wyprzedzeniem. Przy pierwszym nawiązaniu połączenia z Agentem sieciowym, Serwer administracyjny inicjuje pobranie aktualizacji. Jeśli Agent sieciowy pobierze wszystkie uaktualnienia na urządzenie klienckie, staną się one dostępne dla aplikacji na tym urządzeniu.

  Jeśli zarządzana aplikacja na urządzeniu klienckim spróbuje uzyskać dostęp do Agenta sieciowego w celu uzyskania uaktualnień, Agent sieciowy sprawdzi, czy posiada wszystkie wymagane uaktualnienia. Jeśli uaktualnienia zostały pobrane z Serwera administracyjnego nie więcej niż 25 godzin przed zażądaniem ich przez zarządzaną aplikację, Agent sieciowy nie nawiąże połączenia z Serwerem administracyjnym, ale dostarczy zarządzanej aplikacji uaktualnienia z lokalnej pamięci podręcznej. Połączenie z Serwerem administracyjnym może nie zostać nawiązane, gdy Agent sieciowy dostarcza uaktualnienia aplikacji na urządzeniach klienckich, ale połączenie nie jest wymagane w celu przeprowadzenia aktualizacji.

  Jeśli ta opcja jest wyłączona, tryb offline pobierania aktualizacji nie jest używany. Uaktualnienia są rozsyłane zgodnie z terminarzem zadania pobierania aktualizacji.

  Domyślnie opcja ta jest włączona.

Łączność

Sekcja **Łączność** zawiera trzy zagnieżdżone podsekcje:

- **Sieć**
- **Profile połączenia** (tylko dla systemów Windows i macOS)
- **Terminarz połączeń**

W podsekcji **Sieć** możesz skonfigurować połączenie z Serwerem administracyjnym, włączyć korzystanie z portu UDP oraz określić jego numer. Dostępne są następujące opcje:

- W grupie ustawień **Połączenie z Serwerem administracyjnym** możesz skonfigurować połączenie z Serwerem administracyjnym oraz określić przedziału czasu dla synchronizacji pomiędzy urządzeniami klienckimi a Serwerem administracyjnym:

  - **Kompresuj ruch sieciowy**

    Jeżeli ta opcja jest włączona, prędkość transferu danych przez Agenta sieciowego zostaje zwiększona poprzez zmniejszenie ilości przesyłanych informacji i tym samym zmniejszenie obciążenia Serwera administracyjnego.

    > Obciążenie procesora komputera klienckiego może się zwiększyć.

    Domyślnie pole to jest zaznaczone.

  - **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows**

    Jeżeli ta opcja jest włączona, porty niezbędne do pracy Agenta sieciowego, zostaną dodane do listy wykluczeń Zapory sieciowej systemu Microsoft Windows.

    Domyślnie opcja ta jest włączona.

  - **Użyj SSL**

    Jeśli ta opcja jest włączona, połączenie z Serwerem administracyjnym jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

    Domyślnie opcja ta jest włączona.

  - **Użyj bramy połączenia na punkcie dystrybucji (jeśli jest dostępny) w domyślnych ustawieniach połączenia**

    Jeśli ta opcja jest włączona, brama połączenia na punkcie dystrybucji jest używana z ustawieniami określonymi we właściwościach grupy administracyjnej.

    Domyślnie opcja ta jest włączona.

- **Użyj portu UDP**

  Jeśli chcesz, żeby Agent Sieciowy nawiązywał połączenie z Serwerem administracyjnym poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **Numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z Serwerem administracyjnym to 15000.

- **Numer portu UDP**

  W tym polu możesz wprowadzić numer portu UDP. Domyślny numer portu to 15000.

  Używany jest system dziesiętny.

  Jeżeli na urządzeniu klienckim zainstalowany jest system Windows XP Service Pack 2, wówczas wbudowana zapora sieciowa będzie blokowała port UDP o numerze 15000. Port ten należy otworzyć ręcznie.

- **Użyj punktu dystrybucji do wymuszenia nawiązania połączenia z Serwerem administracyjnym**

  Wybierz tę opcję, jeśli w oknie ustawień punktu dystrybucji zaznaczyłeś opcję **Użyj tego punktu dystrybucji jako serwera push**. W przeciwnym razie punkt dystrybucji nie będzie działał jako serwer push.

W podsekcji **Profile połączenia** możesz określić ustawienia lokalizacji sieciowej, skonfigurować profile połączenia dla Serwera administracyjnego, a także włączyć tryb użytkownika mobilnego, gdy Serwer administracyjny jest niedostępny.

- **Ustawienia lokalizacji sieciowej**

  Ustawienia lokalizacji sieciowej definiują cechy sieci, do której podłączone jest urządzenie klienckie, i określają reguły przełączania Agenta sieciowego z jednego profilu połączenia Serwera administracyjnego do innego, gdy te cechy sieci zostaną zmienione.

- **Profile połączeń Serwera administracyjnego**

  W tej sekcji możesz dodawać i wyświetlać profile połączenia Agenta sieciowego z Serwerem administracyjnym. W tej sekcji możesz także utworzyć reguły przełączania Agenta sieciowego na inne Serwery administracyjne, gdy wystąpią następujące zdarzenia:

  - Gdy urządzenie klienckie zostanie podłączone do innej sieci lokalnej
  - Gdy zostanie zerwane połączenie między urządzeniem a siecią lokalną organizacji
  - Gdy adres bramy połączenia zostanie zmieniony lub adres serwera DNS zostanie zmodyfikowany

  > Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows i macOS.

- **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny**

  Jeśli ta opcja jest włączona, w przypadku połączenia przez ten profil, aplikacje zainstalowane na urządzeniu klienckim będą używać profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

  Jeżeli ta opcja jest wyłączona, aplikacje będą używać zasad aktywnych.

  Domyślnie opcja ta jest wyłączona.

W podsekcji **Terminarz połączeń** możesz określić przedziały czasu, w trakcie których Agent sieciowy wysyła dane do Serwera administracyjnego:

- **Połącz, gdy jest to konieczne**

  Jeśli ta opcja jest zaznaczona, połączenie jest nawiązywane, gdy Agent sieciowy musi wysłać dane na Serwer administracyjny.

  Domyślnie opcja ta jest zaznaczona.

- **Połącz w określonych przedziałach czasu**

  Jeśli ta opcja jest zaznaczona, Agent sieciowy łączy się z Serwerem administracyjnym w określonym czasie. Możesz dodać kilka przedziałów czasu.

Punkty dystrybucji

Sekcja **Punkty dystrybucji** zawiera cztery zagnieżdżone podsekcje:

- **Przeszukiwanie sieci**
- **Ustawienia połączenia internetowego**
- **KSN Proxy**
- **Aktualizacje**

W podsekcji **Przeszukiwanie sieci** możesz skonfigurować automatyczne przeszukiwanie sieci. Można włączyć trzy typy przeszukiwania, czyli przeszukiwanie sieci, przeszukiwanie zakresu adresów IP i przeszukiwanie Active Directory:

- **Włącz przeszukiwanie sieci**

  Jeśli ta opcja jest włączona, Serwer administracyjny automatycznie przeszuka sieć zgodnie z terminarzem skonfigurowanym po kliknięciu odnośników **Ustaw terminarz szybkiego przeszukiwania** i **Ustaw terminarz pełnego przeszukiwania**.

  Jeżeli ta opcja jest wyłączona, Serwer administracyjny przeszukuje sieć z częstotliwością określoną w polu **Częstotliwość przeszukiwania sieci (min)**.

  Interwał wykrywania urządzeń dla Agenta sieciowego w wersjach przed 10.2 może zostać skonfigurowany w polach **Częstotliwość pobierania informacji z domen Windows (min)** (w przypadku szybkiego przeszukiwania sieci z domen Windows) i **Częstotliwość przeszukiwania sieci (min)** (w przypadku pełnego przeszukiwania sieci z domen Windows).

  Domyślnie opcja ta jest wyłączona.

- **Włącz przeszukiwanie zakresu IP**

  Jeśli opcja jest włączona, punkt dystrybucji automatycznie przeszuka zakresy IP zgodnie z terminarzem skonfigurowanym po kliknięciu przycisku **Ustaw terminarz przeszukiwania**.

  Jeśli ta opcja jest wyłączona, Serwer punkt dystrybucji nie będzie przeszukiwał zakresów IP.

  Częstotliwość przeszukiwania zakresu IP dla Agenta sieciowego w wersjach poprzedzających 10.2 może być skonfigurowana w polu **Interwał przeszukiwania (min)**. Pole jest dostępne, jeśli opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

- **Użyj przeszukiwania Zeroconf (tylko na platformach Linux; ręcznie określone zakresy adresów IP zostaną zignorowane)**

  Jeśli ta opcja jest włączona, punkt dystrybucji automatycznie przeszukuje sieć za pomocą urządzeń IPv6, używając zero-configuration networking (zwany również *Zeroconf*). W takim przypadku włączone przeszukiwanie zakresu adresów IP jest ignorowane, ponieważ punkt dystrybucji przeszukuje całą sieć.

  W celu rozpoczęcia korzystania z Zeroconf, muszą być spełnione następujące warunki:

  - Punkt dystrybucji musi działać pod systemem Linux.
  - Musisz zainstalować narzędzie avahi-browse na punkcie dystrybucji.

  Jeśli ta opcja jest wyłączona, punkt dystrybucji nie przeszukuje sieci z urządzeniami IPv6.

  Domyślnie opcja ta jest wyłączona.

- **Włącz przeszukiwanie Active Directory**

  Jeśli ta opcja jest włączona, punkt dystrybucji automatycznie przeszuka Active Directory zgodnie z terminarzem skonfigurowanym po kliknięciu odnośnika **Ustaw terminarz przeszukiwania**.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie przeszukiwał Active Directory.

  Częstotliwość przeszukiwania Active Directory dla Agenta sieciowego w wersjach poprzedzających 10.2 może być skonfigurowana w polu **Interwał przeszukiwania (min)**. Pole jest dostępne, jeśli ta opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

Jeśli Twoje punkty dystrybucji korzystają z serwera proxy podczas łączenia się z Internetem, w podsekcji **Ustawienia połączenia internetowego** możesz określić następujące ustawienia:

- **Użyj serwera proxy**

  Jeśli to pole wyboru jest zaznaczone, do łączenia punktów dystrybucji z serwerami aktualizacji Kaspersky używany jest internetowy serwer proxy. W polach można skonfigurować połączenie z serwerem proxy.

  Domyślnie pole to nie jest zaznaczone.

- **Adres serwera proxy**

  Adres serwera proxy.

- **Numer portu**

  Numer portu używanego do nawiązywania połączenia.

- **Pomiń serwer proxy dla adresów lokalnych**

  Jeśli ta opcja jest włączona, żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

  Domyślnie opcja ta jest wyłączona.

- **Uwierzytelnianie na serwerze proxy**

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  Domyślnie pole to nie jest zaznaczone.

- **Nazwa użytkownika**

  Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy.

- **Hasło**

  Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

W podsekcji **KSN Proxy** możesz skonfigurować aplikację, aby używała punkt dystrybucji do przesyłania żądań KSN z zarządzanych urządzeń:

- **Włącz KSN Proxy po stronie punktu dystrybucji**

  Usługa KSN proxy jest uruchamiana na urządzeniu, które jest używane jako punkt dystrybucji. Użyj tej funkcji do redystrybucji i optymalizacji ruchu w sieci.

  Punkt dystrybucji wysyła statystyki KSN, które zostały wymienione w Oświadczeniu Kaspersky Security Network, do Kaspersky.

Domyślnie opcja ta jest wyłączona. Włączenie tej opcji działa, jeśli opcje **Użyj Serwera administracyjnego jako serwera proxy** i **Zgadzam się na korzystanie z Kaspersky Security Network** zostały włączone w oknie właściwości Serwera administracyjnego.

Możesz przypisać węzeł klastra aktywny-pasywny do punktu dystrybucji i włączyć serwer proxy KSN na tym węźle.

- **Przesyłaj żądania KSN do Serwera administracyjnego**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do chmury KSN lub KPSN. Żądania KSN wygenerowane na samym punkcie dystrybucji są także wysyłane bezpośrednio do chmury KSN lub KPSN.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej), nie mogą uzyskać bezpośredniego dostępu do KPSN. Jeśli chcesz ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do KPSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 12 (lub późniejszej), mogą uzyskać bezpośredni dostęp do KPSN.

- **Port TCP**

  Numer portu TCP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny numer portu to 13111.

- **Użyj portu UDP**

  Jeśli chcesz, żeby Agent Sieciowy nawiązywał połączenie z Serwerem administracyjnym poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **Numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z Serwerem administracyjnym to 15000.

W podsekcji **Aktualizacje** możesz określić, czy Agent sieciowy powinien pobierać pliki diff poprzez włączenie lub wyłączenie opcji **Pobierz pliki diff** (domyślnie, ta opcja jest włączona).

Historia rewizji

W sekcji **Historia rewizji** możesz przejrzeć historię rewizji zasady Agenta sieciowego. Możesz porównać rewizje, przejrzeć rewizje i wykonać zaawansowane działania, takie jak zapisanie rewizji do pliku, wycofać rewizję oraz dodać i zmodyfikować opisy rewizji.

Zarządzanie kontami użytkowników

Ta sekcja dostarcza informacje o rolach i kontach użytkowników obsługiwanych przez aplikację. Sekcja zawiera także instrukcje dotyczące tworzenia kont i ról użytkowników Kaspersky Security Center.

Kaspersky Security Center umożliwia zarządzanie kontami użytkowników i grupami kont. Aplikacja obsługuje trzy typy kont:

- Konta pracowników firmy. Serwer administracyjny pobiera dane kont tych użytkowników domeny podczas przeszukiwania kontrolera domeny organizacji.
- Konta lokalnych użytkowników. Konta lokalne na zarządzanych urządzeniach, a także konta lokalne na urządzeniu, na którym zainstalowany jest Serwer administracyjny.
- Konta użytkowników wewnętrznych Kaspersky Security Center. Możesz tworzyć konta użytkowników wewnętrznych. Konta te są używane wyłącznie w Kaspersky Security Center.

Praca z kontami użytkowników

Kaspersky Security Center umożliwia zarządzanie kontami użytkowników i grupami kont. Aplikacja obsługuje dwa typy kont:

- Konta pracowników firmy. Serwer administracyjny pobiera dane kont tych użytkowników podczas przeszukiwania sieci firmowej.
- Konta wewnętrznych użytkowników. Te konta są stosowane, gdy używane są wirtualne Serwery administracyjne. Konta użytkowników wewnętrznych są tworzone i używane tylko w obrębie Kaspersky Security Center.

Listę kont użytkowników można wyświetlić na jeden z następujących sposobów:

- W drzewie konsoli przejdź do **Zaawansowane** → **Konta użytkowników**.
- W drzewie konsoli przejdź do **Zarządzane urządzenia** → **Urządzenia** tab → <device name> link → sekcja **Sesje**.

  Sekcja **Sesje** powinna wyświetlać konta użytkowników z aktywnymi sesjami na urządzeniach z systemem Windows.

Lista kont użytkowników wyświetla się prawidłowo, jeżeli spełnione są następujące wymagania:

- Użyj Agenta sieciowego w tej samej wersji, co Serwer administracyjny lub nowszej.
- Włączono przeszukiwanie usługi Active Directory w celu wyświetlania kont użytkowników domeny.
- Na zarządzanych urządzeniach z systemem Windows uruchomiona jest usługa **Serwer (LanmanServer)**.

Na kontach użytkowników i grupach kont można wykonać następujące działania:

- Skonfigurować dla użytkowników uprawnienia dostępu do funkcji aplikacji przy użyciu ról.
- Wysłać wiadomości do użytkowników za pośrednictwem poczty elektronicznej i SMS-ów.
- Przeglądać listę urządzeń mobilnych użytkownika.
- Dostarczyć i zainstalować certyfikaty na urządzenia mobilne użytkownika.
- Wyświetl listę certyfikatów wydanych dla użytkownika.
- Wyłączyć weryfikację dwuetapową dla konta użytkownika.

Dodawanie konta użytkownika wewnętrznego

W celu dodania nowego konta użytkownika wewnętrznego do Kaspersky Security Center:

1. W drzewie konsoli otwórz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. W obszarze roboczym kliknij przycisk **Dodaj użytkownika**.

3. W otwartym oknie **Nowy użytkownik** określ ustawienia nowego konta użytkownika:

   - Nazwa użytkownika ()

     > Należy ostrożnie wpisywać nazwę użytkownika. Nie będziesz mógł jej zmienić po zapisaniu zmian.

   - **Opis**
   - **Pełna nazwa**
   - **Główny adres e-mail**
   - **Główny numer telefonu**
   - **Hasło** dla połączenia użytkownika z Kaspersky Security Center

     Hasło musi być zgodne z następującymi regułami:

     - Hasło musi zawierać od 8 do 256 znaków.
     - Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
       - Wielkie litery (A-Z)
       - Małe litery (a-z)
       - Cyfry (0-9)
       - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków "." i "@", gdy "." jest umieszczane przed "@".

     Aby zobaczyć wprowadzone hasło, kliknij i przytrzymaj przycisk **Pokaż**.

     > Liczba prób wprowadzenia hasła jest ograniczona. Domyślnie jest to 10 prób. Możesz zmienić dozwoloną liczbę prób wprowadzenia hasła, jak opisano to w sekcji „Zmienianie liczby dozwolonych prób wprowadzenia hasła”.

Jeśli użytkownik wprowadzi nieprawidłowe hasło określoną liczbę razy, konto użytkownika zostanie zablokowane na jedną godzinę. Na liście kont użytkowników, ikona użytkownika () zablokowanego konta będzie ciemna (niedostępna). Możesz odblokować konto użytkownika tylko poprzez zmianę hasła.

- Jeśli to konieczne, zaznacz pole **Wyłącz konto**, aby zabronić użytkownikowi możliwość łączenia z aplikacją. Możesz wyłączyć konto, na przykład, jeśli chcesz je utworzyć teraz, ale aktywować później.
- Zaznacz pole **Poproś o hasło podczas modyfikowania ustawień konta**, jeśli chcesz włączyć dodatkową opcję ochrony konta użytkownika przed nieautoryzowaną modyfikacją. Jeżeli ta opcja jest włączona, modyfikowanie ustawień konta użytkownika wymaga autoryzacji użytkownika za pomocą uprawnienia Modyfikuj listy ACL obiektów obszaru funkcyjnego **Funkcje ogólne: Uprawnienia użytkownika**.

4. Kliknij **OK**.

Nowo utworzone konto użytkownika będzie wyświetlane w obszarze roboczym folderu **Konta użytkowników**.

Edytowanie konta użytkownika wewnętrznego

W celu edytowania konta użytkownika wewnętrznego w Kaspersky Security Center:

1. W drzewie konsoli otwórz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. W obszarze roboczym kliknij dwukrotnie konto użytkownika wewnętrznego, które chcesz edytować.
3. W otwartym oknie **Właściwości: <nazwa użytkownika>** zmień ustawienia konta użytkownika:
   - **Opis**
   - **Pełna nazwa**
   - **Główny adres e-mail**
   - **Główny numer telefonu**
   - **Hasło** dla połączenia użytkownika z Kaspersky Security Center

     Hasło musi być zgodne z następującymi regułami:

     - Hasło musi zawierać od 8 do 256 znaków.
     - Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
       - Wielkie litery (A-Z)
       - Małe litery (a-z)
       - Cyfry (0-9)
       - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków "." i "@", gdy "." jest umieszczane przed "@".

Aby zobaczyć wprowadzone hasło, kliknij i przytrzymaj przycisk **Pokaż**.

Liczba prób wprowadzenia hasła jest ograniczona. Domyślnie jest to 10 prób. Możesz zmienić dozwoloną liczbę prób wprowadzenia hasła, jak opisano to w sekcji „Zmienianie liczby dozwolonych prób wprowadzenia hasła".

Jeśli użytkownik wprowadzi nieprawidłowe hasło określoną liczbę razy, konto użytkownika zostanie zablokowane na jedną godzinę. Na liście kont użytkowników, ikona użytkownika () zablokowanego konta będzie ciemna (niedostępna). Możesz odblokować konto użytkownika tylko poprzez zmianę hasła.

- Jeśli to konieczne, zaznacz pole **Wyłącz konto**, aby zabronić użytkownikowi możliwość łączenia z aplikacją. Możesz wyłączyć konto, na przykład, gdy pracownik opuści teren firmy.
- Wybierz opcję **Poproś o hasło podczas modyfikowania ustawień konta**, jeśli chcesz włączyć dodatkową opcję ochrony konta użytkownika przed nieautoryzowaną modyfikacją. Jeżeli ta opcja jest włączona, modyfikowanie ustawień konta użytkownika wymaga autoryzacji użytkownika za pomocą uprawnienia Modyfikuj listy ACL obiektów obszaru funkcyjnego **Funkcje ogólne: Uprawnienia użytkownika**.

4. Kliknij **OK**.

Edytowane konto użytkownika będzie wyświetlane w obszarze roboczym folderu **Konta użytkowników**.

Zmienianie liczby dozwolonych prób wprowadzenia hasła

Użytkownik Kaspersky Security Center może wprowadzić niepoprawne hasło ograniczoną liczbę razy. Po osiągnięciu limitu, konto użytkownika zostaje zablokowane na godzinę.

Domyślnie, maksymalna liczba dozwolonych prób wprowadzenia hasła to 10. Możesz zmienić liczbę dozwolonych prób wprowadzenia hasła w sposób opisany w tej sekcji.

W celu zmiany liczny dozwolonych prób wprowadzenia hasła:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).
2. Przejdź do gałęzi:
   - W systemach 32-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - W systemach 64-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
3. Jeśli brakuje wartości SrvSplPpcLogonAttempts, utwórz ją. Typ wartości to DWORD.
   Domyślnie, po zainstalowaniu Kaspersky Security Center, ta wartość nie zostaje utworzona.
4. Określ żądaną liczbę prób w wartości SrvSplPpcLogonAttempts.

5. Kliknij **OK**, aby zachować zmiany.

6. Uruchom ponownie usługę Serwera administracyjnego.

Maksymalna liczba dozwolonych prób wprowadzenia hasła zostanie zmieniona.

Konfigurowanie sprawdzania unikatowości nazwy użytkownika wewnętrznego

Możesz skonfigurować sprawdzanie unikatowości nazwy użytkownika wewnętrznego Kaspersky Security Center podczas dodawania nazwy do aplikacji. Sprawdzanie unikatowości nazwy użytkownika wewnętrznego może zostać przeprowadzone tylko na wirtualnym Serwerze administracyjnym lub na głównym Serwerze administracyjnym, dla którego będzie tworzone konto użytkownika, lub na wszystkich wirtualnych Serwerach administracyjnych i na głównym Serwerze administracyjnym. Domyślnie unikatowość nazwy użytkownika wewnętrznego jest sprawdzana na wszystkich wirtualnych Serwerach administracyjnych i na głównym Serwerze administracyjnym.

W celu sprawdzenia unikatowości nazwy użytkownika wewnętrznego na wirtualnym Serwerze administracyjnym lub na głównym Serwerze administracyjnym:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).

2. Przejdź do gałęzi:

   - W systemach 32-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

   - W systemach 64-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. Dla klucza LP_InterUserUniqVsScope (DWORD) ustaw wartość 00000001.

   0 jest domyślną wartością określoną dla tego klucza.

4. Uruchom ponownie usługę Serwera administracyjnego.

Unikatowość nazwy będzie sprawdzana na wirtualnym Serwerze administracyjnym, na którym został utworzony użytkownik wewnętrzny, lub na głównym Serwerze administracyjnym, jeśli użytkownik wewnętrzny został utworzony na głównym Serwerze administracyjnym.

W celu sprawdzenia unikatowości nazwy użytkownika wewnętrznego na wszystkich wirtualnych Serwerach administracyjnych lub na głównym Serwerze administracyjnym:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).

2. Przejdź do gałęzi:

   - Dla systemów 64-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

   - Dla systemów 32-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Dla klucza LP_InterUserUniqVsScope (DWORD) ustaw wartość 00000000.

   0 jest domyślną wartością określoną dla tego klucza.

4. Uruchom ponownie usługę Serwera administracyjnego.

Unikatowość nazwy będzie sprawdzana na wszystkich wirtualnych Serwerach administracyjnych i na głównym Serwerze administracyjnym.

Dodawanie grupy bezpieczeństwa

Możesz dodawać grupy bezpieczeństwa (grupy użytkowników), przeprowadzać elastyczną konfigurację dostępu grup i grupy bezpieczeństwa do różnych funkcji aplikacji. Grupom bezpieczeństwa można przypisać nazwy, które odpowiadają ich przeznaczeniu. Na przykład, nazwa może odpowiadać miejscu w biurze, w którym znajdują się użytkownicy, lub nazwie jednostki organizacyjnej firmy, do której należą użytkownicy.

Jeden użytkownik może należeć do kilku grup bezpieczeństwa. Konto użytkownika zarządzane przez wirtualny Serwer administracyjny może należeć tylko do grup bezpieczeństwa tego Serwera wirtualnego i może posiadać uprawnienia dostępu tylko w obrębie tego Serwera wirtualnego.

W celu dodania grupy bezpieczeństwa:

1. Z drzewa konsoli wybierz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. Kliknij przycisk **Dodaj grupę zabezpieczeń**.

   Zostanie otwarte okno **Dodaj grupę zabezpieczeń**.

3. W oknie **Dodaj grupę zabezpieczeń**, w sekcji **Ogólne** określ nazwę grupy.

   Nazwa grupy nie może zawierać więcej niż 255 znaków oraz znaków specjalnych, takich jak: *, <, >, ?, \, :, |. Nazwa grupy musi być unikatowa.

   Opis grupy można wpisać w polu **Opis**. Uzupełnienie pola **Opis** nie jest obowiązkowe.

4. Kliknij **OK**.

Dodana grupa bezpieczeństwa pojawi się w folderze **Konta użytkowników** drzewa konsoli. Możesz dodawać użytkowników do nowo utworzonej grupy.

Dodawanie użytkownika do grupy

W celu dodania użytkownika do grupy:

1. Z drzewa konsoli wybierz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. Na liście grup i kont użytkowników wskaż grupę, do której chcesz dodać użytkownika.

3. W oknie właściwości grupy wybierz sekcję **Użytkownicy grupy** i kliknij przycisk **Dodaj**.

   Zostanie otwarte okno z listą użytkowników.

4. Na liście wskaż użytkownika, którego chcesz włączyć do grupy.

5. Kliknij **OK**.

Użytkownik zostaje dodany do grupy i wyświetlony na liście użytkowników grupy.

Konfigurowanie praw dostępu do funkcji aplikacji. Kontrola dostępu oparta o rolę

Kaspersky Security Center oferuje możliwości dla dostępu opartego na roli do funkcji Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky.

Możesz skonfigurować uprawnienia dostępu do funkcji aplikacji dla użytkowników Kaspersky Security Center w jeden z następujących sposobów:

- Konfigurując uprawnienia dla każdego użytkownika lub grupy użytkowników indywidualnie.
- Tworząc standardowe role użytkownika z predefiniowanym zestawem uprawnień i przypisując te role do użytkowników w zależności od ich zakresu obowiązków.

Rola użytkownika (zwana również rolą) jest predefiniowanym zestawem uprawnień dostępu do funkcji Kaspersky Security Center lub zarządzanych aplikacji firmy Kaspersky. Rola może zostać przydzielona użytkownikowi lub grupie użytkowników.

Stosowanie ról użytkownika jest przeznaczone do uproszczenia i skrócenia rutynowych procedur konfigurowania uprawnień dostępu użytkowników do funkcji aplikacji. Uprawnienia dostępu w obrębie roli są konfigurowane zgodnie ze 'standardowymi' zadaniami i zakresem obowiązków użytkowników.

Rolom użytkownika można przypisać nazwy, które odpowiadają ich przeznaczeniu. Możesz utworzyć nieograniczoną liczbę ról w aplikacji.

Możesz użyć predefiniowanych ról użytkownika z już skonfigurowanym zestawem uprawnień lub utworzyć nowe role i samodzielnie skonfigurować wymagane uprawnienia.

Prawa dostępu do funkcji aplikacji

Poniższa tabela przedstawia funkcje Kaspersky Security Center wraz z prawami dostępu do zarządzania powiązanymi zadaniami, raportami, ustawieniami i wykonywania powiązanych działań użytkownika.

Aby wykonać czynności użytkownika wymienione w tabeli, użytkownik musi mieć określone uprawnienia obok akcji.

Prawa do **Odczyt**, **Zapis** i **Wykonywanie** mają zastosowanie do każdego zadania, raportu lub ustawienia. Oprócz tych praw użytkownik musi mieć uprawnienie **Wykonywanie działań dla wyborów urządzeń**, aby zarządzać zadaniami, raportami lub ustawieniami wyborów urządzeń.

Wszystkie zadania, raporty, ustawienia i pakiety instalacyjne, których brakuje w tabeli, należą do obszaru funkcjonalnego **Funkcje ogólne: Podstawowa funkcjonalność**.

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
Funkcje ogólne: Zarządzanie grupami administracyjnymi	**Zapis**	• Dodaj urządzenie do grupy administracyjnej: **Zapis** • Usuń urządzenie z grupy administracyjnej: **Zapis** • Dodaj grupę administracyjną do innej grupy administracyjnej: **Zapis** • Usuń grupę administracyjną z innej grupy administracyjnej: **Zapis**	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
Funkcje ogólne: Uzyskuj dostęp do obiektów bez względu na ich listy ACL	**Odczyt**	Uzyskaj dostęp do Odczyt do wszystkich obiektów: **Odczyt**	Brak	Brak	Brak
Funkcje ogólne Podstawowa funkcjonalność	• **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Reguły przenoszenia urządzeń (tworzenie, modyfikowanie lub usuwanie) dla Serwera wirtualnego: **Zapis**, **Wykonywanie działań dla wyborów urządzeń** • Uzyskaj niestandardowy certyfikat protokołu Mobile (LWNGT): **Odczyt** • Ustaw certyfikat niestandardowy protokołu Mobile (LWNGT): **Zapis** • Uzyskaj listę sieci zdefiniowaną przez NLA: **Odczyt** • Dodaj, zmodyfikuj lub usuń listę sieci zdefiniowaną przez NLA: **Zapis** • Wyświetl listę kontroli dostępu grup: **Odczyt** • Wyświetl dziennik zdarzeń aplikacji Kaspersky: **Odczyt** • Wyświetl klucz odzyskiwania, aby przywrócić dostęp do dysku twardego zaszyfrowanego za pomocą Szyfrowania dysków funkcją BitLocker: **Wykonywanie**	• „Pobierz aktualizacje do repozytorium serwera administracyjnego” • „Dostarczaj raporty” • „Roześlij pakiet instalacyjny” • „Zdalnie zainstaluj aplikację na podrzędnych Serwerach administracyjnych”	• „Raport o stanie ochrony” • „Raport o zagrożeniach” • „Raport o najbardziej zainfekowanych urządzeniach” • „Raport o stanie antywirusowych baz danych” • „Raport o błędach” • „Raport o atakach sieciowych” • „Raport podsumowujący o zainstalowanych aplikacjach zabezpieczających systemy pocztowe” • „Raport podsumowujący o aplikacjach zabezpieczających styk sieci z internetem” • „Raport podsumowujący o typach zainstalowanych aplikacji” • „Raport o użytkownikach zainfekowanych urządzeń” • „Raport incydentów” • „Raport o zdarzeniach” • „Raport aktywności punktów dystrybucji” • „Raport o podrzędnych Serwerach administracyjnych” • „Raport zdarzeń Kontroli urządzeń” • „Raport o lukach” • „Raport o zabronionych aplikacjach” • „Raport Kontroli sieci” • „Raport o stanie szyfrowania zarządzanych urządzeń" • „Raport o stanie szyfrowania urządzeń pamięci masowej"	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
				• „Raport o błędach podczas szyfrowania plików" • „Raport o zablokowanym dostępie do zaszyfrowanych plików" • „Raport o uprawnieniach dostępu do zaszyfrowanych urządzeń" • „Raport o obowiązujących uprawnieniach użytkowników" • „Raport na temat praw"	
Funkcje ogólne: Usunięte obiekty	• **Odczyt** • **Zapis**	• Wyświetl usunięte obiekty w Koszu: **Odczyt** • Usuń obiekty z Kosza: **Zapis**	Brak	Brak	Brak
Funkcje ogólne: Przetwarzanie zdarzeń	• **Usuń zdarzenia** • **Edycja ustawień powiadamiania o zdarzeniach** • **Edycja ustawień rejestrowania zdarzeń** • **Zapis**	• Zmień ustawienia rejestracji zdarzeń: **Edycja ustawień rejestrowania zdarzeń** • Zmień ustawienia powiadomień o zdarzeniach: **Edycja ustawień powiadamiania o zdarzeniach** • Usuń zdarzenia: **Usuń zdarzenia**	Brak	Brak	Ustawienia: • Ustawienia epidemii wirusa: liczba wykryć wirusów wymagana do utworzenia zdarzenia epiden wirusa • Ustawienia epidemii wirusa: czas na ocenę wykrycia wirusów • Maksymalna liczb zdarzeń przechowywanyc w bazie danych • Okres przechowywania zdarzeń z usuniętych urządzeń
Funkcje ogólne: Operacje na Serwerze administracyjnym	• **Odczyt** • **Zapis** • **Wykonywanie** • **Modyfikacja list ACL obiektu** • **Wykonywanie działań dla wyborów urządzeń**	• Określ porty Serwera administracyjnego dla połączenia agenta sieciowego: **Zapis** • Określ porty Serwera proxy aktywacji uruchomionego na serwerze administracyjnym Serwer administracyjny: **Zapis** • Określ porty serwera proxy aktywacji dla urządzeń przenośnych uruchomionych na Serwerze administracyjnym: **Zapis**	• „Tworzenie kopii zapasowych danych Serwera administracyjnego" • „Konserwacja baz danych"	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		• Określ porty serwera sieciowego do dystrybucji samodzielnych pakietów: **Zapis** • Określ porty serwera sieciowego do dystrybucji profili MDM: **Zapis** • Określ porty SSL Serwera administracyjnego do połączenia przez Kaspersky Security Center Web Console: **Zapis** • Określ porty serwera administracyjnego Serwer administracyjny dla połączenia mobilnego: **Zapis** • Zmienianie maksymalnej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego: **Zapis** • Określ maksymalną liczbę zdarzeń, które mogą być wysłane przez Serwer administracyjny: **Zapis** • Określ przedział czasu, w którym zdarzenia mogą być wysyłane przez Serwer administracyjny: **Zapis**			
Funkcje ogólne: Wdrażanie aplikacji Kaspersky	• **Zarządzanie poprawkami Kaspersky** • **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	Zaakceptuj lub odrzuć instalację poprawki: **Zarządzanie poprawkami Kaspersky**	Brak	• „Raport użycia klucza licencyjnego przez wirtualny Serwer administracyjny” • „Raport o wersjach oprogramowania Kaspersky” • „Raport o niekompatybilnych aplikacjach” • „Raport o wersjach aktualizacji modułu oprogramowania Kaspersky” • „Raport wdrażania ochrony”	Pakiet instalacyjny: „Kaspersky”
Funkcje ogólne: Zarządzanie kluczami licencyjnymi	• **Eksportuj plik klucza** • **Zapis**	• Eksportuj plik klucza: **Eksportuj plik klucza** • Zmodyfikuj ustawienia klucza	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		licencyjnego Serwera administracyjnego: **Zapis**			
Funkcje ogólne: Wymuszone zarządzanie raportami	• **Odczyt** • **Zapis**	• Twórz raporty niezależnie od ich list ACL: **Zapis** • Wykonywanie raportów niezależnie od ich list ACL: **Odczyt**	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
Funkcje ogólne: Hierarchia Serwerów administracyjnych	**Skonfiguruj hierarchię Serwerów administracyjnych**	Zarejestruj, zaktualizuj lub usuń podrzędne Serwery administracyjne: **Skonfiguruj hierarchię Serwerów administracyjnych**	Brak	Brak	Brak
Funkcje ogólne: Uprawnienia użytkownika	**Modyfikacja list ACL obiektu**	• Zmień właściwości Zabezpieczenia dowolnego obiektu: **Modyfikacja list ACL obiektu** • Zarządzaj rolami użytkowników: **Modyfikacja list ACL obiektu** • Zarządzaj użytkownikami wewnętrznymi: **Modyfikacja list ACL obiektu** • Zarządzaj grupami zabezpieczeń: **Modyfikacja list ACL obiektu** • Zarządzaj aliasami: **Modyfikacja list ACL obiektu**	Brak	Brak	Brak
Funkcje ogólne: Wirtualne Serwery administracyjne	• **Zarządzaj wirtualnymi Serwerami administracyjnymi** • **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Pobierz listę wirtualnych serwerów administracyjnych Serwery administracyjne: **Odczyt** • Uzyskaj informacje na temat wirtualnego Serwera administracyjnego: **Odczyt** • Utwórz, zaktualizuj lub usuń wirtualny Serwer administracyjny: **Zarządzaj wirtualnymi Serwerami administracyjnymi** • Przenieś wirtualny Serwer administracyjny do innej grupy: **Zarządzaj wirtualnymi Serwerami administracyjnymi** • Ustaw uprawnienia do administracyjnego Serwera wirtualnego: **Zarządzaj wirtualnymi Serwerami administracyjnymi**	Brak	„Raport o wynikach instalacji aktualizacji oprogramowania firm trzecich”	Brak
Funkcje ogólne: Zarządzanie kluczem szyfrowania	• **Odczyt** • **Zapis**	• Eksportuj klucze szyfrowania: **Odczyt** • Zaimportuj klucze	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		szyfrowania: **Zapis**			
Zarządzanie urządzeniami mobilnymi: Ogólny	• **Podłącz nowe urządzenia** • **Przesyłanie do urządzeń mobilnych jedynie informacji o poleceniach** • **Przesyłanie poleceń do urządzeń mobilnych** • **Zarządzanie certyfikatami** • **Odczyt** • **Zapis**	• Uzyskaj dane przywracania Usługi zarządzania kluczami: **Odczyt** • Usuń certyfikaty użytkownika: **Zarządzanie certyfikatami** • Uzyskaj część publiczną certyfikatu użytkownika: **Odczyt** • Sprawdź, czy infrastruktura klucza publicznego jest włączona: **Odczyt** • Sprawdź konto infrastruktury klucza publicznego: **Odczyt** • Uzyskaj szablony infrastruktury klucza publicznego: **Odczyt** • Uzyskaj szablony infrastruktury klucza publicznego za pomocą certyfikatu rozszerzonego użycia klucza: **Odczyt** • Sprawdź, czy certyfikat infrastruktury klucza publicznego został odwołany: **Odczyt** • Zaktualizuj ustawienia wydawania certyfikatów użytkownika: **Zarządzanie certyfikatami** • Uzyskaj ustawienia wydawania certyfikatu użytkownika: **Odczyt** • Pobierz pakiety według nazwy i wersji aplikacji: **Odczyt** • Ustaw lub anuluj certyfikat użytkownika: **Zarządzanie certyfikatami** • Odnów certyfikat użytkownika: **Zarządzanie certyfikatami**	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		• Ustaw tag certyfikatu użytkownika: **Zarządzanie certyfikatami** • Uruchom generację pakietu instalacyjnego MDM; anuluj generowanie pakietu instalacyjnego MDM: **Podłącz nowe urządzenia**			
Zarządzanie systemami: Łączność	• **Uruchom sesje Pulpitu zdalnego** • **Połączenie z istniejącymi sesjami Pulpitu zdalnego** • **Rozpocznij tunelowanie** • **Zapisz pliki z urządzeń na stacji roboczej administratora** • **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Utwórz sesję udostępniania pulpitu: **Uruchom sesje Pulpitu zdalnego** • Utwórz sesję RDP: **Połączenie z istniejącymi sesjami Pulpitu zdalnego** • Utwórz tunel: **Rozpocznij tunelowanie** • Zapisz listę sieci partnerskiej: **Zapisz pliki z urządzeń na stacji roboczej administratora**	Brak	„Raport o użytkownikach urządzenia”	Brak
Zarządzanie systemami: Inwentarz sprzętu	• **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Pobierz lub wyeksportuj obiekt spisu sprzętu: **Odczyt** • Dodaj, ustaw lub usuń obiekt spisu sprzętu: **Zapis**	Brak	• „Raport rejestru sprzętu” • „Raport o zmianach konfiguracji” • „Raport o sprzęcie”	Brak
Zarządzanie systemami: Network Access Control	• **Odczyt** • **Zapis**	• Wyświetl ustawienia CISCO: **Odczyt** • Zmień ustawienia CISCO: **Zapis**	Brak	Brak	Brak
Zarządzanie systemami: Wdrażanie systemu operacyjnego	• **Instalacja serwerów PXE** • **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Zainstaluj serwer PXE: **Instalacja serwerów PXE** • Wyświetl listę serwerów PXE: **Odczyt** • Rozpocznij lub zatrzymaj proces instalacji na klientach PXE: **Wykonywanie** • Zarządzaj sterownikami dla WinPE i obrazów systemu operacyjnego: **Zapis**	„Utwórz pakiet instalacyjny na podstawie obrazu systemu operacyjnego urządzenia odniesienia”	Brak	Pakiet instalacyjny: „Obraz systemu operacyjnego”
Zarządzanie systemami: Zarządzanie lukami i poprawkami	• **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Wyświetl właściwości poprawki trzeciej firmy: **Odczyt** • Zmień właściwości poprawki trzeciej firmy: **Zapis**	• „Wykonać synchronizację Windows Update” • „Instalacja aktualizacji Windows Update”	„Raport o aktualizacjach oprogramowania”	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
			• „Napraw luki" • „Zainstaluj wymagane aktualizacje i napraw luki"		
Zarządzanie systemami: Zdalna instalacja	• **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Przejrzyj właściwości pakietu instalacyjnego Zarządzanie lukami i poprawkami innych firm: **Odczyt** • Zmień właściwości pakietu instalacyjnego Zarządzanie lukami i poprawkami innych firm: **Zapis**	Brak	Brak	Pakiety instalacyjne: • „Aplikacja niestandardowa" • „Pakiet VAPM"
Zarządzanie systemami: Inwentaryzacja oprogramowania	• **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	Brak	Brak	• „Raport o zainstalowanych aplikacjach" • „Raport o rejestrze aplikacji" • „Raport o stanie grup licencjonowanych aplikacji" • „Raport dotyczący kluczy licencyjnych oprogramowania innych firm"	Brak

Informacje o rolach użytkowników

Role użytkowników przypisane do użytkowników Kaspersky Security Center zapewniają im zestawy praw dostępu do funkcji aplikacji.

Użytkownikom utworzonym na Serwerze wirtualnym nie można przypisać roli na Serwerze administracyjnym.

Możesz użyć predefiniowanych ról użytkownika z już skonfigurowanym zestawem uprawnień lub utworzyć nowe role. W takim przypadku należy samodzielnie ustawić zakres roli i przypisać uprawnienia dostępu do funkcji Kaspersky Security Center. Niektóre z predefiniowanych ról użytkowników dostępnych w Kaspersky Security Center mogą być powiązane z określonymi stanowiskami pracy, na przykład **Audytor**, **Specjalista ds. zabezpieczeń**, **Opiekun** (te role są obecne w Kaspersky Security Center od wersji 11). Prawa dostępu do tych ról są wstępnie skonfigurowane zgodnie ze standardowymi zadaniami i zakresem obowiązków powiązanych stanowisk. Poniższa tabela pokazuje jak role mogą zostać powiązane z określonymi stanowiskami pracy:

Przykłady ról dla określonych stanowisk pracy

Rola	Komentarz
Audytor	Zezwala na wszystkie operacje przeglądania i wykonywania wszelkich utworzonych zadań na wybranych urządzeniach podłączonych do Serwera administracyjnego za pośrednictwem Agenta sieciowego z uprawnieniami administratora lokalnego (root w przypadku Linux). Zalecamy ostrożne przyznawanie tych praw ograniczonej grupie użytkowników, którzy potrzebują ich do wykonywania swoich obowiązków służbowych.

Opiekun	Zezwala na wszystkie działania przeglądania, ale nie zezwala na pozostałe działania. Możesz przypisać tę rolę do specjalisty ds. zabezpieczeń i innych menadżerów zarządzających bezpieczeństwem IT w Twojej firmie.
Specjalista ds. zabezpieczeń	Zezwala na wszystkie działania przeglądania, zezwala na zarządzanie raportami; przydziela ograniczone uprawnienia w obszarze **Zarządzanie systemami**: **Łączność**. Możesz przypisać tę rolę do specjalisty zarządzającego bezpieczeństwem IT w Twojej firmie.

Poniższa tabela przedstawia prawa dostępu przypisane do każdej predefiniowanej roli użytkownika.

Prawa dostępu do predefiniowanych ról użytkowników

Rola	Opis
Administrator serwera administracyjnego	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Funkcje ogólne**: • **Podstawowa funkcjonalność** • **Przetwarzanie zdarzeń** • **Hierarchia Serwerów administracyjnych** • **Wirtualne Serwery administracyjne** • **Zarządzanie poprawkami i lukami**: • **Łączność** • **Inwentaryzacja sprzętu** • **Inwentaryzacja oprogramowania** Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.
Operator serwera administracyjnego	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych: • **Funkcje ogólne**: • **Podstawowa funkcjonalność** • **Wirtualne Serwery administracyjne** • **Zarządzanie poprawkami i lukami**: • **Łączność** • **Inwentaryzacja sprzętu** • **Inwentaryzacja oprogramowania**
Audytor	Zezwala na wszystkie operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Usunięte obiekty** • **Wymuszone zarządzanie raportami** Tę rolę można przypisać do osoby, która przeprowadza audyt w Twojej organizacji.

Rola	Opis
Administrator instalacji	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Funkcje ogólne**: • **Podstawowa funkcjonalność** • **Wdrażanie oprogramowania Kaspersky** • **Zarządzanie kluczami licencyjnymi** • **Zarządzanie poprawkami i lukami**: • **Wdrażanie systemu operacyjnego** • **Zarządzanie lukami i poprawkami** • **Instalacja zdalna** • **Inwentaryzacja oprogramowania** Przyznaje uprawnienia do **odczytu** i **wykonywania** w obszarze funkcjonalnym **Funkcje ogólne: Wirtualne serwery administracyjne**.
Operator instalacji	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych: • **Funkcje ogólne**: • **Podstawowa funkcjonalność** • **Zdalna instalacja oprogramowania Kaspersky** (zapewnia również **Zarządzanie poprawkami Kaspersky** bezpośrednio w tym obszarze) • **Wirtualne Serwery administracyjne** • **Zarządzanie poprawkami i lukami**: • **Wdrażanie systemu operacyjnego** • **Zarządzanie lukami i poprawkami** • **Instalacja zdalna** • **Inwentaryzacja oprogramowania**
Administrator Kaspersky Endpoint Security	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.
Operator Kaspersky Endpoint Security	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje
Główny administrator	Zezwala na wszystkie operacje w obszarach funkcjonalnych, z *wyjątkiem* następujących obszarów w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Wymuszone zarządzanie raportami** Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.

Rola	Opis
Główny operator	Przyznaje prawa **odczytu** i **wykonywania** (w stosownych przypadkach) we wszystkich następujących obszarach funkcjonalnych: • **Funkcje ogólne**: • **Podstawowa funkcjonalność** • **Usunięte obiekty** • **Operacje na Serwerze administracyjnym** • **Wdrażanie aplikacji Kaspersky** • **Wirtualne Serwery administracyjne** • **Zarządzanie urządzeniami mobilnymi: ogólne** • **Zarządzanie systemem**, w tym wszystkie funkcje • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje
Administrator zarządzania urządzeniami mobilnymi	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • **Zarządzanie urządzeniami mobilnymi: ogólne**
Operator zarządzania urządzeniami mobilnymi	Przyznaje uprawnienia **Odczyt** i **Wykonywanie** w obszarze funkcjonalnym **Funkcje ogólne**: **Podstawowa funkcjonalność**. Przyznaje uprawnienia **odczytu** i **wysyłania** informacji poleceń na urządzenia mobilne w obszarach funkcjonalnych **Zarządzania urządzeniami mobilnymi**: **Ogólne**.
Specjalista ds. zabezpieczeń	Zezwala na następujące operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Wymuszone zarządzanie raportami** Przyznaje uprawnienia **Odczytu**, **Wpisania**, **Wykonywania**, **Zapisywania** plików z urządzeń na stacji roboczej administratora i **wykonywania działań dla wyborów urządzeń w obszarze funkcjonalnym Zarządzanie systemami: Łączność**. Możesz przypisać tę rolę do specjalisty zarządzającego bezpieczeństwem IT w Twojej firmie.
Użytkownik portalu Self Service Portal	Zezwala na wszystkie operacje w obszarze funkcjonalnym **Zarządzanie urządzeniami mobilnymi: Self Service Portal**. Ta funkcja nie jest obsługiwana w Kaspersky Security Center 11 i nowszej wersji.
Opiekun	Przyznaje prawo do **Odczytu** w obszarach funkcjonalnych **Funkcje ogólne**: **Dostęp do obiektów, niezależnie od ich list ACL** i **Funkcje ogólne**: **Wymuszone zarządzanie raportami**. Możesz przypisać tę rolę do specjalisty ds. zabezpieczeń i innych menadżerów zarządzających bezpieczeństwem IT w Twojej firmie.
Administrator zarządzania lukami i poprawkami	Zezwala na wszystkie operacje w obszarach funkcjonalnych **Funkcje ogólne**: **Podstawowa funkcjonalność** i **Zarządzanie systemem** (w tym wszystkie funkcje).
Operator zarządzania lukami i poprawkami	Przyznaje uprawnienia **Odczyt** i **Wykonywanie** (w stosownych przypadkach) w obszarach funkcjonalnych **Funkcje ogólne**: **Podstawowa funkcjonalność** i **Zarządzanie systemem** (w tym wszystkie funkcje).

Dodawanie roli użytkownika

W celu dodania roli użytkownika:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, na panelu **Sekcje** wybierz **Role użytkownika** i kliknij przycisk **Dodaj**.

Sekcja **Role użytkownika** jest dostępna, jeśli włączona jest opcja Wyświetl sekcje ustawień zabezpieczeń.

4. W oknie właściwości **Nowa rola** skonfiguruj rolę:

   - Na panelu **Sekcje** wybierz **Ogólne** i określ nazwę roli.

     Nazwa roli nie może zawierać więcej niż 100 znaków.

   - Wybierz sekcję **Uprawnienia** i skonfiguruj zestaw uprawnień, zaznaczając pola **Zezwól** i **Odmów** obok funkcji aplikacji.

   Jeśli pracujesz na głównym Serwerze administracyjnym, możesz włączyć opcję **Przekaż listę ról do podrzędnych Serwerów administracyjnych**.

5. Kliknij **OK**.

Rola została dodana.

Role użytkownika utworzone dla Serwera administracyjnego są wyświetlane w oknie właściwości Serwera administracyjnego, w sekcji **Role użytkownika**. Możesz zmodyfikować i usunąć role użytkownika, a także przypisać role do grup bezpieczeństwa lub wybranych użytkowników.

Przypisywanie roli do użytkownika lub grupy bezpieczeństwa

W celu przypisania roli do użytkownika lub grupy użytkowników:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Zabezpieczenia**.

   Sekcja **Zabezpieczenia** jest dostępna, jeśli w oknie ustawień interfejsu dostępne jest pole **Wyświetl sekcje ustawień zabezpieczeń**.

4. W polu **Nazwy grup lub użytkowników** wybierz użytkownika lub grupę użytkowników, do których mają zostać przypisane role.

   Jeśli pole nie zawiera użytkownika lub grupy, możesz je dodać, klikając przycisk **Dodaj**.

   Jeśli dodajesz użytkownika poprzez kliknięcie przycisku **Dodaj**, możesz wybrać typ autoryzacji użytkownika (Microsoft Windows lub Kaspersky Security Center). Autoryzacja Kaspersky Security Center jest używana do wybierania kont wewnętrznych użytkowników, które są używane do pracy z wirtualnymi Serwerami administracyjnymi.

5. Wybierz zakładkę **Role** i kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Role użytkownika**. To okno wyświetla utworzone role użytkownika.

6. W oknie **Role użytkownika** wybierz rolę dla grupy bezpieczeństwa.
7. Kliknij **OK**.

Rola z zestawem uprawnień do pracy z Serwerem administracyjnym zostanie przypisana do użytkownika lub grupy bezpieczeństwa. Przypisane role są wyświetlane na zakładce **Role**, w sekcji **Zabezpieczenia** okna właściwości Serwera administracyjnego.

Przydzielanie uprawnień użytkownikom i grupom

Użytkownikom i grupom możesz nadać uprawnienia do używania różnych funkcji Serwera administracyjnego i programów Kaspersky, dla których posiadasz wtyczki zarządzające, na przykład, Kaspersky Endpoint Security for Windows.

W celu przypisania uprawnień do użytkownika lub grupy użytkowników:

1. W drzewie konsoli wykonaj jedną z następujących czynności:
   - Rozwiń węzeł **Serwer administracyjny** i wybierz podfolder z nazwą żądanego Serwera administracyjnego.
   - Wybierz grupę administracyjną.
2. Z menu kontekstowego Serwera administracyjnego lub grupy administracyjnej wybierz **Właściwości**.
3. W otwartym oknie właściwości Serwera administracyjnego (lub oknie właściwości grupy administracyjnej), w lewym panelu **Sekcje** wybierz **Zabezpieczenia**.

   Sekcja **Zabezpieczenia** jest dostępna, jeśli w oknie ustawień interfejsu dostępne jest pole **Wyświetl sekcje ustawień zabezpieczeń**.
4. W sekcji **Zabezpieczenia**, na liście **Nazwy grup lub użytkowników** wybierz użytkownika lub grupę.
5. Na liście uprawnień w dolnej części obszaru roboczego, na zakładce **Uprawnienia** skonfiguruj zestaw uprawnień dla użytkownika lub grupy:
   a. Kliknij znaki plusa (+), aby rozwinąć węzły na liście i uzyskać dostęp do uprawnień.
   b. Zaznacz pola **Zezwól** i **Odmów** obok żądanych uprawnień.
      Przykład 1: Rozwiń węzeł **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** lub węzeł **Usunięte obiekty** i wybierz **Odczyt**.
      Przykład 2: Rozwiń węzeł **Podstawowa funkcjonalność** i wybierz **Zapis**.
6. Jeśli skonfigurowałeś zestaw uprawnień, kliknij **Zastosuj**.

Zestaw uprawnień dla użytkownika lub grupy użytkowników zostanie skonfigurowany.

Uprawnienia Serwera administracyjnego (lub grupy administracyjnej) są podzielone na następujące obszary:

- Funkcje ogólne:
  - Zarządzanie grupami administracyjnymi
  - Uzyskuj dostęp do obiektów bez względu na ich listy ACL
  - Podstawowa funkcjonalność
  - Usunięte obiekty
  - Przetwarzanie zdarzeń

    - Operacje na Serwerze administracyjnym (tylko w oknie właściwości Serwera administracyjnego)
    - Zdalna instalacja aplikacji Kaspersky
    - Zarządzanie kluczami licencyjnymi
    - Wymuszone zarządzanie raportami
    - Hierarchia Serwerów
    - Uprawnienia użytkownika
    - Wirtualne Serwery administracyjne
- Zarządzanie urządzeniami mobilnymi:
    - Ogólne
- Zarządzanie poprawkami i lukami:
    - Łączność
    - Inwentaryzacja sprzętu
    - Kontrola dostępu do sieci
    - Zdalna instalacja systemów operacyjnych
    - Zarządzaj lukami i poprawkami
    - Instalacja zdalna
    - Inwentaryzacja oprogramowania

Jeśli dla uprawnienia nie wybrano **Zezwól** ani **Odmów**, wówczas uprawnienie jest uznawane za *niezdefiniowane*: zostaje odrzucone, dopóki wyraźnie nie zostanie dozwolone lub odrzucone dla użytkownika.

Uprawnienia użytkownika są sumą:

- Własnych uprawnień użytkownika
- Uprawnień wszystkich ról przypisanych do tego użytkownika
- Uprawnień wszystkich grup bezpieczeństwa, do których należy użytkownik
- Uprawnień wszystkich ról przypisanych do grupy bezpieczeństwa, do których należy użytkownik

Jeśli przynajmniej jeden z tych zestawów uprawnień posiada opcję **Odmów** dla uprawnienia, wówczas dla użytkownika zostaje zabronione to uprawnienie nawet wtedy, gdy inne zestawy zezwalają na nie lub pozostawiają je niezdefiniowane.

Przydzielanie ról użytkownika do podrzędnych Serwerów administracyjnych

Domyślnie, listy ról użytkownika głównego i podrzędnego Serwera administracyjnego są niezależne. Możesz skonfigurować aplikację w taki sposób, aby automatycznie rozsyłała role użytkownika utworzone na głównym Serwerze administracyjnym do wszystkich podrzędnych Serwerów administracyjnych. Role użytkownika mogą także zostać rozesłane z podrzędnego Serwera administracyjnego na swoje własne podrzędne Serwery administracyjne.

W celu przesłania ról użytkownika z głównego Serwera administracyjnego na podrzędne Serwery administracyjne:

1. Otwórz okno główne aplikacji.
2. Wykonaj jedną z poniższych czynności:
   - W drzewie konsoli kliknij prawym klawiszem myszy nazwę Serwera administracyjnego i z otwartego menu kontekstowego wybierz **Właściwości**.
   - Jeśli posiadasz aktywną zasadę Serwera administracyjnego, w obszarze roboczym folderu **Zasady** kliknij prawym klawiszem tą zasadę i z menu kontekstowego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego lub w oknie ustawień zasady, w panelu **Sekcje** wybierz **Role użytkownika**.

   Sekcja **Role użytkownika** jest dostępna, jeśli włączona jest opcja **Wyświetl sekcje ustawień zabezpieczeń**.
4. Włącz opcję **Przekaż listę ról do podrzędnych Serwerów administracyjnych**.
5. Kliknij **OK**.

Aplikacja kopiuje role użytkownika głównego Serwera administracyjnego na podrzędne Serwery administracyjne.

Jeśli opcja **Przekaż listę ról do podrzędnych Serwerów administracyjnych** jest włączona, a role użytkownika są przesyłane, nie mogą być edytowane ani usuwane na podrzędnych Serwerach administracyjnych. Jeśli tworzysz nową rolę lub edytujesz już tę istniejącą na głównym Serwerze administracyjnym, zmiany są automatycznie kopiowane do podrzędnych Serwerów administracyjnych. Jeśli usuwasz rolę użytkownika na głównym Serwerze administracyjnym, ta rola pozostanie na podrzędnych Serwerach administracyjnych, ale może być edytowana lub zostać usunięta.

Role, które zostają przesłane na podrzędny Serwer administracyjny z Serwera głównego, są wyświetlane z ikoną kłódki (🔒). Nie możesz edytować tych ról na podrzędnym Serwerze administracyjnym.

Jeśli tworzysz rolę na głównym Serwerze administracyjnym i istnieje rola z tą samą nazwą na swoim podrzędnym Serwerze administracyjnym, nowa rola zostaje skopiowana do podrzędnego Serwera administracyjnego z indeksem dodanym do jego nazwy, na przykład: ~~1, ~~2 (indeks może być losowy).

Jeśli wyłączysz opcję **Przekaż listę ról do podrzędnych Serwerów administracyjnych**, wszystkie role użytkownika pozostaną na podrzędnych Serwerach administracyjnych, ale staną się niezależne od tych na głównym Serwerze administracyjnym. Po tym, jak role użytkownika staną się niezależne, role użytkownika na podrzędnych Serwerach administracyjnych mogą być edytowane lub usuwane.

Wskazywanie użytkownika jako właściciela urządzenia

Możesz wskazać użytkownika jako właściciela urządzenia, aby przypisać urządzenie do tego użytkownika. Jeśli musisz wykonać jakiekolwiek działania na urządzeniu (na przykład zaktualizować oprogramowanie), administrator może poinformować właściciela urządzenia, aby autoryzował te działania.

W celu wskazania użytkownika jako właściciela urządzenia:

1. W drzewie konsoli wybierz folder **Zarządzane urządzenia**.
2. W obszarze roboczym folderu, na zakładce **Urządzenia** wybierz urządzenie, dla którego chcesz wskazać właściciela.
3. Z otwartego menu kontekstowego urządzenia wybierz **Właściwości**.
4. W oknie właściwości urządzenia wybierz **Informacje o systemie** → **Sesje**.
5. Kliknij przycisk **Przypisz** znajdujący się obok pola **Właściciel urządzenia**.
6. W oknie **Wybór użytkownika** wybierz użytkownika, którego chcesz wskazać jako właściciela urządzenia, i kliknij **OK**.
7. Kliknij **OK**.

Właściciel urządzenia zostanie przypisany. Domyślnie pole **Właściciel urządzenia** jest uzupełnione wartością z Active Directory i jest aktualizowane podczas każdego przeszukiwania Active Directory. Listę właścicieli urządzeń możesz sprawdzić w **Raporcie dotyczącym właścicieli urządzeń**. Raport można utworzyć przy użyciu kreatora tworzenia nowego raportu.

Dostarczanie wiadomości użytkownikom

W celu wysyłania wiadomości do użytkownika za pośrednictwem poczty elektronicznej:

1. Z drzewa konsoli, w folderze **Konta użytkowników** wybierz użytkownika.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.
2. Z menu kontekstowego użytkownika wybierz **Powiadom przez e-mail**.
3. W oknie **Wyślij wiadomość do użytkownika** uzupełnij odpowiednie pola, a następnie kliknij przycisk **OK**.

Wiadomość zostanie wysłana na adres e-mail określony we właściwościach użytkownika.

W celu wysyłania wiadomości SMS do użytkownika:

1. Z drzewa konsoli, w folderze **Konta użytkowników** wybierz użytkownika.
2. W menu kontekstowym użytkownika wybierz **Wyślij SMS**.
3. Uzupełnij odpowiednie pola w oknie **Treść SMS-a** i kliknij przycisk **OK**.

Wiadomość zostanie wysłana na urządzenie mobilne o numerze określonym we właściwościach użytkownika.

Przeglądanie listy urządzeń mobilnych użytkownika

W celu przejrzenia listy urządzeń mobilnych użytkownika:

1. Z drzewa konsoli, w folderze **Konta użytkowników** wybierz użytkownika.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. Z menu kontekstowego konta użytkownika wybierz **Właściwości**.

3. W oknie właściwości konta użytkownika wybierz sekcję **Urządzenia mobilne**.

W sekcji **Urządzenia mobilne** możesz wyświetlić listę urządzeń mobilnych użytkownika oraz informacje o każdym z tych urządzeń. Kliknij przycisk **Eksportuj do pliku**, aby zapisać listę urządzeń mobilnych do pliku.

Instalowanie certyfikatu dla użytkownika

Możesz zainstalować trzy certyfikaty dla użytkownika:

- Certyfikat współdzielony, który jest wymagany do identyfikacji urządzenia mobilnego użytkownika.
- Certyfikat poczty, który jest niezbędny do skonfigurowania poczty firmowej na urządzeniu mobilnym użytkownika.
- Certyfikat VPN, który jest niezbędny do skonfigurowania wirtualnej sieci prywatnej na urządzeniu mobilnym użytkownika.

W celu wydania certyfikatu dla użytkownika i jego zainstalowania:

1. W drzewie konsoli otwórz folder **Konta użytkowników** i wybierz konto użytkownika.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. Z menu kontekstowego konta użytkownika wybierz **Zainstaluj certyfikat**.

   Zostanie uruchomiony kreator instalacji certyfikatu. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora instalacji certyfikatu, certyfikat zostanie utworzony i zainstalowany. Listę zainstalowanych certyfikatów użytkownika można przejrzeć oraz wyeksportować do pliku.

Wyświetlanie listy certyfikatów wydanych dla użytkownika

W celu wyświetlenia listy certyfikatów wydanych dla użytkownika:

1. Z drzewa konsoli, w folderze **Konta użytkowników** wybierz użytkownika.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. Z menu kontekstowego konta użytkownika wybierz **Właściwości**.

3. W oknie właściwości konta użytkownika wybierz sekcję **Certyfikaty**.

W sekcji **Certyfikaty** możesz wyświetlić listę certyfikatów użytkownika oraz informacje o każdym z tych certyfikatów. Kliknij przycisk **Eksportuj do pliku**, aby zapisać listę certyfikatów do pliku.

Informacje o administratorze wirtualnego Serwera administracyjnego

Administrator sieci firmowej zarządzanej poprzez wirtualny Serwer administracyjny uruchamia Kaspersky Security Center Web Console z poziomu konta użytkownika określonego w tym oknie, aby wyświetlić szczegóły ochrony antywirusowej.

Jeśli jest to konieczne, na Serwerze wirtualnym można utworzyć kilka kont administratora.

Użytkownikom utworzonym na Serwerze wirtualnym nie można przypisać roli na Serwerze administracyjnym.

Administrator wirtualnego Serwera Administracyjnego jest wewnętrznym użytkownikiem Kaspersky Security Center. Do systemu operacyjnego nie są przesyłane żadne dane dotyczące wewnętrznych użytkowników. Kaspersky Security Center autoryzuje wewnętrznych użytkowników.

Zdalna instalacja systemów operacyjnych i aplikacji

Kaspersky Security Center umożliwia tworzenie obrazów systemów operacyjnych i instalowanie ich na urządzeniach klienckich w sieci, a także wykonywanie zdalnej instalacji aplikacji firmy Kaspersky lub innych producentów.

Aby tworzyć obrazy systemów operacyjnych, musisz zainstalować narzędzia wdrażania Windows ADK i dodatek Windows PE dla Windows ADK na Serwerze administracyjnym. Możesz utworzyć obraz dowolnej wersji systemu operacyjnego Windows, która spełnia wymagania Kaspersky Security Center.

Kaspersky Security Center nie obsługuje 64-bitowych wersji Windows ADK i Windows PE.

Przechwytywanie obrazów systemów operacyjnych

Kaspersky Security Center może przechwytywać obrazy systemów operacyjnych z urządzeń i przesyłać je do Serwera administracyjnego. Takie obrazy systemów operacyjnych są przechowywane na Serwerze administracyjnym w dedykowanym folderze. Obraz systemu operacyjnego odpowiedniego urządzenia może zostać przechwycony i utworzony przy użyciu zadania tworzenia pakietu instalacyjnego.

Funkcja przechwytywania obrazu systemu operacyjnego posiada następujące cechy:

- Obraz systemu operacyjnego nie może zostać przechwycony na urządzeniu z zainstalowanym Serwerem administracyjnym.
- Podczas przechwytywania obrazu systemu operacyjnego narzędzie sysprep.exe resetuje ustawienia odpowiedniego urządzenia. Jeśli chcesz przywrócić ustawienia urządzenia referencyjnego, zaznacz pole wyboru **Utwórz kopię zapasową stanu urządzenia** w kreatorze tworzenia zadania OS Imaging.
- Proces przechwytywania obrazu umożliwia ponowne uruchomienie odpowiedniego urządzenia.

Instalowanie obrazów systemów operacyjnych na nowych urządzeniach

Możesz użyć przechwyconych obrazów do zainstalowania ich na nowych urządzeniach w sieci, na których nie zainstalowano jeszcze systemu operacyjnego. W tym przypadku wykorzystywana jest technologia Preboot eXecution Environment (PXE). Wybierz w sieci urządzenie, które będzie używane jako serwer PXE. Urządzenie musi spełniać następujące wymagania:

- Na urządzeniu powinien zostać zainstalowany Agent sieciowy.
- Na urządzeniu nie może być aktywny żaden serwer DHCP, ponieważ serwer PXE używa tych samych portów co serwer DHCP.
- Segment sieci, który zawiera urządzenie, nie powinien zawierać innych serwerów PXE.

W celu zainstalowania systemu operacyjnego należy spełnić następujące warunki:

- W urządzeniu powinna znajdować się karta sieciowa.
- Urządzenie musi być połączone z siecią.
- Podczas uruchamiania urządzenia, w BIOS-ie należy wybrać opcję Network boot.

Zdalna instalacja systemów operacyjnych odbywa się w następujący sposób:

1. Urządzenie klienckie nawiązuje połączenie z serwerem PXE podczas procesu uruchamiania.
2. Urządzenie klienckie uruchamia się w środowisku preinstalacji systemu Windows (WinPE).

   Włączenie urządzenia do środowiska WinPE może wymagać konfiguracji zestawu sterowników dla WinPE.

3. Urządzenie klienckie jest rejestrowane na Serwerze administracyjnym.
4. Administrator przypisuje do urządzenia klienckiego pakiet instalacyjny z obrazem systemu operacyjnego.

   Administrator może dodać żądane sterowniki do pakietu instalacyjnego z obrazem systemu operacyjnego. Administrator może także określić plik konfiguracji z ustawieniami systemu operacyjnego (plik odpowiedzi), który będzie stosowany podczas instalacji.

5. System operacyjny zostanie zainstalowany na urządzeniu klienckim.

Administrator może ręcznie określić adresy MAC urządzeń klienckich, które nie zostały jeszcze połączone, i przypisać do nich pakiet instalacyjny z obrazem systemu operacyjnego. Po połączeniu wybranych urządzeń klienckich z serwerem PXE, system operacyjny jest automatycznie instalowany na tych urządzeniach.

Instalowanie obrazów systemów operacyjnych na urządzeniach, na których zainstalowany jest już inny system operacyjny

Zdalna instalacja obrazów systemów operacyjnych na urządzeniach klienckich, na których zainstalowany jest już inny system operacyjny, odbywa się poprzez zadanie zdalnej instalacji dla określonych urządzeń.

Należy pamiętać, że wykonywana jest czysta instalacja systemu operacyjnego. Wszystkie dane zostaną usunięte.

Instalowanie aplikacji firmy Kaspersky i innych producentów

Administrator może utworzyć pakiety instalacyjne dowolnych aplikacji, łącznie z tymi określonymi przez użytkownika, oraz zainstalować aplikacje na urządzeniach klienckich przy użyciu zadania zdalnej instalacji.

Tworzenie obrazów systemów operacyjnych

Obrazy systemów operacyjnych są tworzone przy użyciu zadania usuwania obrazu systemu operacyjnego odpowiedniego urządzenia.

W celu utworzenia zadania tworzenia obrazu systemu operacyjnego:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
2. Kliknij przycisk **Utwórz pakiet instalacyjny**, aby uruchomić Kreator tworzenia nowego pakietu.
3. W oknie **Wybierz typ pakietu instalacyjnego** kliknij przycisk **Utwórz pakiet instalacyjny zawierający obraz systemu operacyjnego**.
4. Postępuj zgodnie z instrukcjami kreatora.

   Po zakończeniu pracy kreatora, zostaje utworzone zadanie Serwera administracyjnego o nazwie **Tworzenie pakietu instalacyjnego bazującego na obrazie systemu operacyjnego zainstalowanego na urządzeniu**. Zadanie można zobaczyć w folderze **Zadania**.

Po zakończeniu wykonywania zadania **Tworzenie pakietu instalacyjnego bazującego na obrazie systemu operacyjnego zainstalowanego na urządzeniu** tworzony jest pakiet instalacyjny, który może zostać użyty do zainstalowania systemu operacyjnego na urządzeniach klienckich poprzez serwer PXE lub zadanie zdalnej instalacji. Pakiet instalacyjny można zobaczyć w folderze **Pakiety instalacyjne**.

Instalowanie obrazów systemów operacyjnych

Kaspersky Security Center umożliwia instalację obrazów WIM pulpitu i serwerowych systemów operacyjnych Windows® na urządzeniach w sieci organizacji.

W celu uzyskania obrazu systemu operacyjnego, który będzie mógł zostać zainstalowany przy użyciu narzędzi Kaspersky Security Center:

- Zaimportuj obraz z pliku install.wim znajdującego się w pakiecie dystrybucyjnym systemu Windows
- Przechwyć obraz z urządzenia odniesienia

Dla instalacji obrazów systemu operacyjnego są obsługiwane dwa scenariusze:

- Zdalna instalacja na "czystym" urządzeniu, na którym nie ma zainstalowanego systemu operacyjnego
- Zdalna instalacja na urządzeniu działającym pod kontrolą systemu Windows

Użyj środowiska preinstalacyjnego Windows (Windows PE) do przechwytywania i wdrażania obrazów systemu operacyjnego. Wszystkie sterowniki niezbędne do właściwego funkcjonowania wszystkich urządzeń docelowych muszą zostać dodane do obrazu WinPE. Zasadniczo należy dodać sterowniki karty sieciowej i kontrolera pamięci masowej.

W celu zaimplementowania scenariuszy przechwytywania i instalacji obrazu muszą być spełnione następujące warunki:

- Windows Automated Installation Kit (WAIK) wersja 2.0, lub nowsza, lub Windows ADK z dodatkiem Windows PE dla Windows ADK musi być zainstalowany na Serwerze administracyjnym. Jeśli scenariusz przewiduje instalowanie i przechwytywanie obrazów na systemie Windows XP, należy zainstalować Windows WAIK.
- W sieci, w której znajduje się urządzenie docelowe, musi być dostępny serwer DHCP.
- Folder współdzielony Serwera administracyjnego musi zostać otwarty do odczytu w sieci, w której znajduje się urządzenie docelowe. Jeśli folder współdzielony znajduje się na Serwerze administracyjnym, wymagany jest dostęp dla konta KlPxeUser (to konto jest tworzone automatycznie podczas działania instalatora Serwera administracyjnego). Jeśli folder współdzielony znajduje się poza Serwerem administracyjnym, uprawnienie dostępu musi zostać nadane każdemu.

Podczas wybierania instalowanego obrazu systemu operacyjnego administrator musi wyraźnie określić architekturę procesora urządzenia docelowego: x86 lub x86-64.

Konfigurowanie adresu serwera proxy KSN

Domyślnie, nazwa połączenia lub adres IP Serwera administracyjnego pokrywa się z adresem serwera proxy KSN. Jeśli zmienisz nazwę połączenia lub adres IP dla Serwera administracyjnego, musisz określić poprawny adres serwera proxy KSN, aby zapobiec utracie połączenia między hostem a KSN.

W celu skonfigurowania adresu serwera proxy KSN:

1. W drzewie konsoli przejdź do **Zaawansowane** → **Zdalna instalacja** → **Pakiety instalacyjne**.
2. Z menu kontekstowego **Pakiety instalacyjne** wybierz **Właściwości**.
3. W otwartym oknie, na zakładce **Ogólne** określ nowy adres serwera proxy KSN.
4. Kliknij przycisk **Zastosuj**.

Od teraz określany adres jest używany jako adres serwera proxy KSN. Zalecamy włączenie opcji **Użyj KSN Proxy** w celu optymalizacji ruchu w sieci.

Dodawanie sterowników dla Windows Preinstallation Environment (WinPE)

W celu dodania sterowników dla Windows Preinstallation Environment (WinPE):

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Wdrażanie obrazów urządzenia**.
2. W obszarze roboczym folderu **Wdrażanie obrazów urządzenia** kliknij przycisk **Akcje dodatkowe** i z listy rozwijalnej wybierz **Konfiguruj zestaw sterowników Środowiska preinstalacji systemu Windows (WinPE)**.

   Zostanie otwarte okno **Sterowniki środowiska preinstalacji systemu Windows**.
3. W oknie **Sterowniki środowiska preinstalacji systemu Windows** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Wybierz sterownik**.
4. W oknie **Wybierz sterownik** wybierz sterownik z listy.

   Jeśli na liście nie ma żądanego sterownika, kliknij przycisk **Dodaj** i określ nazwę sterownika oraz folder pakietu dystrybucyjnego sterownika w oknie **Dodaj sterownik**, które zostanie otwarte.

   Możesz wybrać folder, klikając przycisk **Przeglądaj**.

   W oknie **Dodaj sterownik** kliknij **OK**.
5. W oknie **Wybierz sterownik** kliknij **OK**.

   Sterownik zostanie dodany do repozytorium Serwera administracyjnego. Po dodaniu do repozytorium, sterownik jest wyświetlany w oknie **Wybierz sterownik**.
6. W oknie **Sterowniki środowiska preinstalacji systemu Windows** kliknij **OK**.

Sterownik zostanie dodany do Windows Preinstallation Environment (WinPE).

Dodawanie sterowników do pakietu instalacyjnego z obrazem systemu operacyjnego

W celu dodania sterowników do pakietu instalacyjnego z obrazem systemu operacyjnego:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
2. Z menu kontekstowego pakietu instalacyjnego z obrazem systemu operacyjnego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości pakietu instalacyjnego.
3. W oknie właściwości pakietu instalacyjnego wybierz sekcję **Dodatkowe sterowniki**.
4. Kliknij przycisk **Dodaj** w sekcji **Dodatkowe sterowniki**.

   Zostanie otwarte okno **Wybierz sterownik**.

5. W oknie **Wybierz sterownik** wybierz sterowniki, które chcesz dodać do pakietu instalacyjnego z obrazem systemu operacyjnego.

   Nowe sterowniki można dodać do repozytorium Serwera administracyjnego, klikając przycisk **Dodaj** dostępny w oknie **Wybierz sterownik**.

6. Kliknij **OK**.

Dodane sterowniki są wyświetlane w sekcji **Dodatkowe sterowniki** okna właściwości pakietu instalacyjnego z obrazem systemu operacyjnego.

Konfigurowanie narzędzia sysprep.exe

Narzędzie sysrep.exe jest przeznaczone do przygotowania urządzenia do utworzenia obrazu systemu operacyjnego.

W celu skonfigurowania narzędzia sysprep.exe:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
2. Z menu kontekstowego pakietu instalacyjnego z obrazem systemu operacyjnego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości pakietu instalacyjnego.
3. W oknie właściwości pakietu instalacyjnego wybierz sekcję **Ustawienia sysprep.exe**.
4. W sekcji **Ustawienia sysprep.exe** określ plik konfiguracyjny, który zostanie użyty podczas instalacji systemu operacyjnego na urządzeniu klienckim:

   - **Użyj domyślnego pliku konfiguracyjnego**. Wybierz tę opcję, aby użyć pliku odpowiedzi, domyślnie wygenerowanego podczas przechwytywania obrazu systemu operacyjnego.
   - **Określ niestandardowe wartości głównych ustawień**. Wybierz tę opcję, aby określić wartości dla ustawień poprzez interfejs.
   - **Określ plik konfiguracyjny**. Wybierz tę opcję, aby użyć niestandardowego pliku odpowiedzi.
5. W celu zastosowania wprowadzonych zmian należy kliknąć przycisk **Zastosuj**.

Instalowanie systemów operacyjnych na urządzeniach w sieci

W celu zainstalowania systemu operacyjnego na nowych urządzeniach, na których jeszcze nie zainstalowano żadnego systemu operacyjnego:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Wdrażanie obrazów urządzenia**.

   Upewnij się, że opcja **Wyświetl zarządzanie lukami i poprawkami** jest włączona w **oknie** Konfiguruj interfejs. W przeciwnym razie folder **Zdalna instalacja** nie zostanie wyświetlony.
2. Kliknij przycisk **Akcje dodatkowe** i z listwy rozwijalnej wybierz **Zarządzaj listą serwerów PXE znajdujących się w sieci**.

   Zostanie otwarte okno **Właściwości: Rozsyłanie obrazów urządzenia** na sekcji **Serwery PXE**.

3. W sekcji **Serwery PXE** kliknij przycisk **Dodaj** i w oknie **Serwery PXE**, które zostanie otwarte, wybierz urządzenie, które będzie używane jako serwer PXE.

   Urządzenie, które dodałeś, jest wyświetlone w sekcji Serwery PXE. Utworzone pliki WinPE są przesyłane do urządzenia z Serwera administracyjnego. Proces przesyłania plików trwa zwykle ok. 10 minut. Po zakończeniu transferu wyświetlana wartość **Stan** zmienia się z **Rozpoczynanie pracy** na **Gotowy**.

4. W sekcji **Serwery PXE** wybierz serwer PXE i kliknij przycisk **Właściwości**.

5. W oknie właściwości wybranego serwera PXE, na zakładce **Ustawienia połączenia z serwerem PXE** skonfiguruj połączenie między Serwerem administracyjnym a serwerem PXE.

6. Uruchom urządzenie klienckie, na którym chcesz zainstalować system operacyjny.

7. W BIOS-ie urządzenia klienckiego wybierz opcję Network boot.

   Urządzenie klienckie nawiąże połączenie z serwerem PXE, a następnie jest wyświetlane w obszarze roboczym folderu **Wdrażanie obrazów urządzenia**.

8. W sekcji **Akcje** kliknij odnośnik **Przypisz pakiet instalacyjny**, aby wybrać pakiet instalacyjny, który zostanie użyty do zainstalowania systemu operacyjnego na wybranym urządzeniu.

   Użyj narzędzia DiskPart na wybranym urządzeniu, aby sprawdzić dostępne dyski. W wierszu polecenia Windows PE wpisz `diskpart`, aby otworzyć narzędzie DiskPart. Wpisz `list disk`, aby wyświetlić listę dysków.

   Po dodaniu urządzenia i przypisaniu do niego pakietu instalacyjnego, zdalna instalacja systemu operacyjnego zostanie automatycznie uruchomiona na tym urządzeniu.

9. Aby anulować zdalną instalację systemu operacyjnego na urządzeniu klienckim, w sekcji **Akcje** kliknij odnośnik **Anuluj instalację obrazu systemu operacyjnego**.

W celu dodania urządzeń według adresu MAC:

- W folderze **Wdrażanie obrazów urządzenia** kliknij **Dodaj adres MAC urządzenia**, aby otworzyć okno **Nowe urządzenie**, w którym określ adres MAC urządzenia, które chcesz dodać.

- W folderze **Wdrażanie obrazów urządzenia** kliknij **Importuj adresy MAC urządzeń z pliku**, aby wybrać plik zawierający listę adresów MAC wszystkich urządzeń, na których chcesz zainstalować system operacyjny.

Instalowanie systemów operacyjnych na urządzeniach klienckich

W celu zainstalowania systemu operacyjnego na urządzeniach klienckich, na których jest już zainstalowany inny system operacyjny:

1. W drzewie konsoli otwórz folder **Zdalna instalacja** i kliknij odnośnik **Roześlij pakiet instalacyjny na zarządzane urządzenia (stacje robocze)**, aby uruchomić Kreator wdrażania ochrony.

2. W oknie **Wybierz pakiet instalacyjny** wskaż pakiet instalacyjny z obrazem systemu operacyjnego.

3. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora, zostanie utworzone zadanie zdalnej instalacji dla instalacji systemu operacyjnego na urządzeniach klienckich. Zadanie może zostać uruchomione lub zatrzymane w folderze **Zadania**.

Tworzenie pakietów instalacyjnych aplikacji

W celu utworzenia pakietu instalacyjnego aplikacji:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
2. Kliknij przycisk **Utwórz pakiet instalacyjny**, aby uruchomić Kreator tworzenia nowego pakietu.
3. W oknie **Wybierz typ pakietu instalacyjnego** kliknij jeden z następujących przycisków:

   - **Utwórz pakiet instalacyjny dla aplikacji Kaspersky**. Wybierz tę opcję, jeśli chcesz utworzyć pakiet instalacyjny dla aplikacji Kaspersky.
   - **Utwórz pakiet instalacyjny dla określonego pliku wykonywalnego**. Wybierz tę opcję, jeśli chcesz utworzyć pakiet instalacyjny dla aplikacji innej firmy przy użyciu pliku wykonywalnego. Zazwyczaj plik wykonywalny to plik instalacyjny aplikacji.

     - **Kopiuj całą zawartość folderu do pakietu instalacyjnego**

       Wybierz tę opcję, jeśli plikowi wykonywalnemu towarzyszą dodatkowe pliki wymagane do zainstalowania aplikacji. Przed włączeniem tej opcji upewnij się, że wszystkie wymagane pliki są przechowywane w tym samym folderze. Jeśli ta opcja jest włączona, aplikacja doda całą zawartość folderu, w tym określony plik wykonywalny, do pakietu instalacyjnego.

     - **Określ parametry instalacji**

       Aby zdalna instalacja zakończyła się pomyślnie, dla większości aplikacji wymagane jest wykonanie instalacji w trybie cichym. W takim przypadku należy określić parametr dla cichej instalacji.

       Skonfiguruj ustawienia instalacji:

       - **Wiersz polecenia pliku wykonywalnego**

         Jeśli dla cichej instalacji aplikacja wymaga dodatkowych parametrów, określ je w tym polu. Więcej informacji można znaleźć w dokumentacji producenta.

         Możesz też wprowadzić inne parametry.

       - **Konwertuj ustawienia na zalecane wartości dla aplikacji rozpoznawanych przez Kaspersky Security Center**

         Aplikacja zostanie zainstalowana z zalecanymi ustawieniami, jeśli informacje o określonej aplikacji znajdują się w bazie danych Kaspersky.

         Jeśli wprowadziłeś parametry w polu **Wiersz polecenia pliku wykonywalnego**, zostaną zapisane z zalecanymi ustawieniami.

         Domyślnie opcja ta jest włączona.

         Baza danych Kaspersky jest tworzona i zarządzana przez analityków z Kaspersky. Dla każdej aplikacji dodanej do bazy danych analitycy z Kaspersky definiują optymalne ustawienia instalacji. Ustawienia są definiowane, aby zapewnić pomyślną zdalną instalację aplikacji na urządzeniu klienckim. Baza danych jest automatycznie aktualizowana na Serwerze administracyjnym, gdy uruchamiasz zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego.

- **Wybierz aplikację z bazy danych Kaspersky do utworzenia pakietu instalacyjnego**. Wybierz tę opcję, jeśli chcesz wybrać wymaganą aplikację innej firmy z bazy danych Kaspersky do utworzenia pakietu instalacyjnego. Baza danych jest tworzona automatycznie, gdy uruchamiasz zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego; aplikacje są wyświetlane na liście.

- **Utwórz pakiet instalacyjny zawierający obraz systemu operacyjnego**. Wybierz tę opcję, jeśli chcesz utworzyć pakiet instalacyjny z obrazem systemu operacyjnego odpowiedniego urządzenia.

  Po zakończeniu pracy kreatora, zostaje utworzone zadanie Serwera administracyjnego o nazwie **Utwórz pakiet instalacyjny na podstawie obrazu referencyjnego systemu operacyjnego urządzenia**. Po zakończeniu wykonywania zadania tworzony jest pakiet instalacyjny, który może zostać użyty do zainstalowania obrazu systemu operacyjnego poprzez serwer PXE lub zadanie zdalnej instalacji.

4. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora, zostanie utworzony pakiet instalacyjny, który może zostać użyty do zainstalowania aplikacji na urządzeniach klienckich. Możesz przejrzeć pakiet instalacyjny, wybierając **Pakiety instalacyjne** w drzewie konsoli.

Tworzenie certyfikatu dla pakietów instalacyjnych aplikacji

W celu utworzenia certyfikatu dla pakietu instalacyjnego aplikacji:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.

   Domyślnie folder **Zdalna instalacja** to podfolder folderu **Zaawansowane**.

2. Z menu kontekstowego folderu **Pakiety instalacyjne** wybierz **Zaawansowane**.

   To spowoduje otwarcie okna właściwości folderu **Pakiety instalacyjne**.

3. W oknie właściwości folderu **Pakiety instalacyjne** wybierz sekcję **Podpisz pakiety autonomiczne**.

4. W sekcji **Podpisz pakiety autonomiczne** kliknij przycisk **Określ**.

   Okno **Certyfikat**.

5. W polu **Typ certyfikatu** określ typ certyfikatu - publiczny lub prywatny:

   - Jeśli wybrana jest wartość **Kontener PKCS #12**, określ plik certyfikatu i hasło.

   - Jeśli wybrana jest wartość **Certyfikat X.509**:

     a. Określ plik klucza prywatnego (z rozszerzeniem *.prk lub *.pem).

     b. Określ hasło dla klucza prywatnego.

     c. Określ plik klucza publicznego (z rozszerzeniem *.cer).

6. Kliknij **OK**.

Zostanie utworzony certyfikat dla pakietu instalacyjnego aplikacji.

Instalowanie aplikacji na urządzeniach klienckich

W celu zainstalowania aplikacji na urządzeniach klienckich:

1. W drzewie konsoli otwórz folder **Zdalna instalacja** i kliknij **Roześlij pakiet instalacyjny na zarządzane urządzenia (stacje robocze)**, aby uruchomić Kreator wdrażania ochrony.
2. W oknie **Wybierz pakiet instalacyjny** wskaż pakiet instalacyjny aplikacji, którą chcesz zainstalować.
3. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora, zostanie utworzone zadanie zdalnej instalacji dla instalacji aplikacji na urządzeniach klienckich. Zadanie może zostać uruchomione lub zatrzymane w folderze **Zadania**.

Użyj kreatora wdrażania ochrony, aby zainstalować Agenta sieciowego na urządzeniach klienckich działających pod kontrolą systemów Windows, Linux i macOS.

Aby zarządzać 64-bitowymi aplikacjami zabezpieczającymi przy użyciu Kaspersky Security Center na urządzeniach działających pod kontrolą systemu operacyjnego Linux, należy użyć 64-bitowej wersji Agenta sieciowego dla systemu Linux. Żądaną wersję Agenta sieciowego można pobrać ze strony internetowej pomocy technicznej.

Przed zdalną instalacją Agenta sieciowego na urządzeniu z systemem Linux należy przygotować urządzenie.

Zarządzanie rewizjami obiektów

Ta sekcja zawiera informacje dotyczące zarządzania rewizjami obiektów. Kaspersky Security Center umożliwia śledzenie modyfikacji obiektów. Za każdym razem, gdy zapisujesz zmiany wprowadzone w obiekcie, tworzona jest *rewizja*. Każda rewizja posiada numer.

Obiekty aplikacji, które obsługują zarządzanie rewizjami, obejmują:

- Właściwości Serwera administracyjnego
- Zasady
- Zadania
- Grupy administracyjne
- Konta użytkowników
- Pakiety instalacyjne

Na rewizjach obiektów możesz wykonać następujące działania:

- Porównać wybraną rewizję z bieżącą rewizją
- Porównać wybrane rewizje
- Porównać obiekt wybranej rewizji z innym obiektem tego samego typu
- Przejrzeć wybraną rewizję
- Wycofać zmiany wprowadzone w obiekcie do wybranej rewizji
- Zapisać rewizje jako plik .txt

W oknie właściwości dowolnego obiektu obsługującego zarządzanie rewizjami sekcja **Historia rewizji** wyświetla listę rewizji obiektów z następującymi szczegółami:

- Liczbę rewizji obiektu
- Datę i godzinę modyfikacji obiektu
- Nazwę użytkownika, który zmodyfikował obiekt
- Działanie wykonane na obiekcie
- Opis rewizji związanej ze zmianą wprowadzoną w ustawieniach obiektu

Informacje o rewizjach obiektów

Na rewizjach obiektów możesz wykonać następujące działania:

- Porównać wybraną rewizję z bieżącą rewizją
- Porównać wybrane rewizje
- Porównać obiekt wybranej rewizji z innym obiektem tego samego typu
- Przejrzeć wybraną rewizję
- Wycofać zmiany wprowadzone w obiekcie do wybranej rewizji
- Zapisać rewizje jako plik .txt

W oknie właściwości dowolnego obiektu obsługującego zarządzanie rewizjami sekcja **Historia rewizji** wyświetla listę rewizji obiektów z następującymi szczegółami:

- Liczbę rewizji obiektu
- Datę i godzinę modyfikacji obiektu
- Nazwę użytkownika, który zmodyfikował obiekt

- Działanie wykonane na obiekcie
- Opis rewizji związanej ze zmianą wprowadzoną w ustawieniach obiektu

Przeglądanie sekcji Historia rewizji

Możesz porównać rewizje obiektu z bieżącą rewizją, porównać różne rewizje wybrane na liście lub porównać rewizję obiektu z rewizją innego obiektu tego samego typu.

*W celu przejrzenia sekcji **Historia rewizji** obiektu:*

1. W drzewie konsoli wybierz jeden z następujących obiektów:
   - Węzeł **Serwer administracyjny**
   - Folder **Zasady**
   - Folder **Zadania**
   - Folder grupy administracyjnej
   - Folder **Konta użytkowników**
   - Folder **Usunięte obiekty**
   - Podfolder **Pakiety instalacyjne**, który jest zagnieżdżony w folderze **Zdalna instalacja**
2. W zależności od lokalizacji żądanego obiektu, wykonaj jedną z następujących czynności:
   - Jeśli obiekt znajduje się w węźle **Serwera administracyjnego** lub w węźle grupy administracyjnej, kliknij węzeł prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Właściwości**.
   - Jeśli obiekt znajduje się w folderze **Zasady**, **Zadania**, **Konta użytkowników**, **Usunięte obiekty**, lub **Pakiety instalacyjne**, wybierz folder, a w odpowiednim obszarze roboczym wybierz obiekt.

   Zostanie otwarte okno właściwości obiektu.
3. W lewym panelu **Sekcje** wybierz **Historia rewizji**.

Historia rewizji jest wyświetlana w obszarze roboczym.

Porównywanie rewizji obiektu

Możesz porównać poprzednie rewizje obiektu z bieżącą rewizją, porównać różne rewizje wybrane na liście lub porównać rewizję obiektu z rewizją innego obiektu tego samego typu.

W celu porównania rewizji obiektu:

1. Wybierz obiekt i przejdź do okna właściwości obiektu.
2. W oknie właściwości przejdź do sekcji **Historia rewizji**.

3. W obszarze roboczym, na liście rewizji obiektu wybierz rewizję do porównania.

   Aby wybrać więcej niż jedną rewizję obiektu, użyj klawiszy **Shift** i **Ctrl**.

4. Wykonaj jedną z poniższych czynności:

   - Kliknij przycisk podziału **Porównaj** i z listy rozwijalnej wybierz jedną z wartości:

     - **Porównaj z bieżącą rewizją**

       Wybierz tę opcję, aby porównać wybraną rewizję z bieżącą rewizją.

     - **Porównaj wybrane rewizje**

       Wybierz tę opcję, aby porównać dwie wybrane rewizje.

     - **Porównaj z innym zadaniem**

       Jeśli pracujesz z rewizjami zadania, wybierz **Porównaj z innym zadaniem**, aby porównać wybraną rewizję z rewizją innego zadania.

       Jeśli pracujesz z rewizjami zasady, wybierz **Porównaj z inną zasadą**, aby porównać wybraną rewizję z rewizją innej zasady.

   - Kliknij dwukrotnie nazwę rewizji i w otwartym oknie właściwości rewizji kliknij jeden z następujących przycisków:

     - **Porównaj z bieżącą**

       Kliknij ten przycisk, aby porównać wybraną rewizję z bieżącą rewizją.

     - **Porównaj z poprzednią**

       Kliknij ten przycisk, aby porównać wybraną rewizję z poprzednią rewizją.

   W domyślnej przeglądarce zostanie wyświetlony raport w formacie HTML z porównaniem rewizji.

   W tym raporcie możesz zminimalizować niektóre sekcje zawierające ustawienia rewizji. Aby zminimalizować sekcję z ustawieniami rewizji obiektu, kliknij ikonę strzałki (▲) obok nazwy sekcji.

Rewizje Serwera administracyjnego zawierają wszystkie szczegóły dotyczące wprowadzonych zmian, za wyjątkiem szczegółów z następujących obszarów:

- Sekcja **Ruch sieciowy**
- Sekcja **Reguły znakowania**
- Sekcja **Powiadamianie**
- Sekcja **Punkty dystrybucji**
- Sekcja **Epidemia wirusa**

  Z sekcji **Epidemia wirusa** nie są zapisywane żadne informacje o konfiguracji aktywacji zasady, która nastąpiła, gdy zdarzenie Epidemia wirusa zostało wyzwolone.

Możesz porównać rewizje usuniętego obiektu z rewizją istniejącego obiektu, ale nie odwrotnie: nie możesz porównać rewizji istniejącego obiektu z rewizją usuniętego obiektu.

Określanie czasu przechowywania rewizji obiektu oraz informacji o usuniętym obiekcie

Okres przechowywania rewizji obiektu i informacji o usuniętych obiektach jest taki sam. Domyślnie okres przechowywania wynosi 90 dni. Jest to wystarczający czas na przeprowadzenie regularnego audytu programu.

Tylko użytkownicy z uprawnieniem **Modyfikacja** w obszarze uprawnień **Usunięte obiekty** mogą zmienić okres przechowywania.

W celu zmiany okresu przechowywania rewizji obiektu i informacji o usuniętych obiektach:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz zmienić okres przechowywania.
2. W menu kontekstowym kliknij prawym klawiszem myszy i wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, które zostanie otwarte, w sekcji **Repozytorium historii rewizji** wprowadź żądany okres przechowywania (liczba dni).
4. Kliknij **OK**.

Rewizje obiektu i informacje o usuniętych obiektach będą przechowywane przez liczbę dni, którą wprowadziłeś.

Przeglądanie rewizji obiektu

Jeśli chcesz wiedzieć, jakie modyfikacje zostały wprowadzone w obiekcie w określonym przedziale czasu, możesz przejrzeć rewizje tego obiektu.

W celu przejrzenia rewizji obiektu:

1. Przejdź do sekcji **Historia rewizji** obiektu.
2. Na liście rewizji obiektu wybierz rewizję, której ustawienia chcesz przejrzeć.
3. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Wyświetl rewizję**.
   - Otwórz okno właściwości rewizji, klikając dwukrotnie nazwę rewizji, a następnie klikając przycisk **Wyświetl rewizję**.

Zostanie wyświetlony raport w formacie HTML zawierający ustawienia wybranej rewizji obiektu. W tym raporcie możesz zminimalizować niektóre sekcje z ustawieniami rewizji obiektu. Aby zminimalizować sekcję z ustawieniami rewizji obiektu, kliknij ikonę strzałki (▲) obok nazwy sekcji.

Zapisywanie rewizji obiektu do pliku

Rewizję obiektu możesz zapisać jako plik tekstowy, na przykład, aby wysłać go za pośrednictwem poczty elektronicznej.

W celu zapisania rewizji obiektu do pliku:

1. Przejdź do sekcji **Historia rewizji** obiektu.
2. Na liście rewizji obiektu wybierz tę, której ustawienia chcesz zapisać.
3. Kliknij przycisk **Zaawansowane** i z listy rozwijalnej wybierz wartość **Zapisz do pliku**.

   Rewizja zostanie zapisana do pliku .txt.

Wycofywanie zmian

Jeśli to konieczne, możesz wycofać zmiany wprowadzone w obiekcie. Na przykład, konieczne może być przywrócenie ustawień zasady z określonego dnia.

W celu wycofania zmian wprowadzonych w obiekcie:

1. Przejdź do sekcji **Historia rewizji** obiektu.
2. Na liście rewizji obiektu wybierz numer rewizji, do której chcesz wycofać zmiany.
3. Kliknij przycisk **Zaawansowane** i z listy rozwijalnej wybierz wartość **Wycofaj**.

   Obiekt zostanie wycofany do wybranej rewizji. Lista rewizji obiektu wyświetla wpis dotyczący podjętego działania. Opis rewizji wyświetla informacje o numerze rewizji, do której wycofałeś obiekt.

Dodawanie opisu rewizji

Możesz dodać opis dla rewizji, aby uprościć wyszukiwanie rewizji na liście.

W celu dodania opisu rewizji:

1. Przejdź do sekcji **Historia rewizji** obiektu.
2. Na liście rewizji obiektu wybierz rewizję, dla której chcesz dodać opis.
3. Kliknij przycisk **Opis**.
4. W oknie **Opis rewizji obiektu** wprowadź opis rewizji.

   Domyślnie, pole opisu rewizji obiektu jest puste.
5. Kliknij **OK**.

Usuwanie obiektów

W tej sekcji znajdują się informacje dotyczące usuwania obiektów.

Możesz usuwać obiekty, w tym:

- Zasady
- Zadania
- Pakiety instalacyjne
- Wirtualne Serwery administracyjne
- Użytkownicy
- Grupy bezpieczeństwa
- Grupy administracyjne

W celu usunięcia obiektu:

1. Otwórz wymaganą sekcję Kaspersky Security Center Web Console, a następnie wybierz obiekt.
2. Na pasku narzędzi kliknij przycisk **Usuń**.
3. W otwartym oknie kliknij **OK**, aby potwierdzić swój wybór.

   Wybrany obiekt zostanie usunięty.

Jeśli usuniesz obiekt, informacje o nim pozostaną w bazie danych. Okres przechowywania informacji o usuniętych obiektach jest taki sam, jak okres przechowywania rewizji obiektu (zalecany okres wynosi 90 dni). Możesz zmienić okres przechowywania tylko wtedy, gdy posiadasz uprawnienie **Modyfikacja** w obszarze uprawnień **Usunięte obiekty**.

Informacje o usuwaniu urządzeń klienckich

Gdy usuniesz urządzenie zarządzane z grupy administracyjnej, aplikacja przeniesie je do grupy Urządzenia nieprzypisane. Po usunięciu urządzenia zainstalowane aplikacje Kaspersky — Agent sieciowy i dowolna aplikacja zabezpieczająca, na przykład Kaspersky Endpoint Security — pozostają na urządzeniu.

Kaspersky Security Center obsługuje urządzenia w grupie Urządzenia nieprzypisane zgodnie z następującymi zasadami:

- Jeśli skonfigurowałeś reguły przenoszenia urządzeń i urządzenie spełnia kryteria reguły przenoszenia, urządzenie jest automatycznie przenoszone do grupy administracyjnej zgodnie z regułą.
- Urządzenie jest przechowywane w grupie Urządzenia nieprzypisane i automatycznie usuwane z grupy zgodnie z regułami przechowywania urządzeń.

  Reguły przechowywania urządzeń nie mają wpływu na urządzenia, które mają jeden lub więcej napędów zaszyfrowanych za pomocą pełnego szyfrowania dysku. Takie urządzenia nie są usuwane automatycznie — można je usunąć tylko ręcznie. Jeśli chcesz usunąć urządzenie z zaszyfrowanym dyskiem, najpierw odszyfruj dysk, a następnie usuń urządzenie.

Przy usuwaniu urządzenia z zaszyfrowanym dyskiem dane wymagane do odszyfrowania dysku są również usuwane. Jeżeli zaznaczysz pole **Rozumiem ryzyko i chcę usunąć wybrane urządzenia** w oknie potwierdzenia otwierającym się po usunięciu takich urządzeń (z grupy **Urządzenia nieprzypisane** lub z grupy **Zarządzane urządzenia**), oznacza to, że masz świadomość związanego z tym usunięcia danych.

Aby odszyfrować dysk, muszą zostać spełnione następujące warunki:

- Urządzenie zostaje ponownie podłączone do Serwera administracyjnego w celu przywrócenia danych wymaganych do odszyfrowania dysku.
- Użytkownik urządzenia zapamięta hasło do odszyfrowania.
- Aplikacja zabezpieczająca, która została użyta do zaszyfrowania dysku, na przykład Kaspersky Endpoint Security for Windows, jest nadal zainstalowana na urządzeniu.

Jeśli dysk został zaszyfrowany przy użyciu technologii Kaspersky Disk Encryption, możesz również spróbować odzyskiwania danych przy użyciu narzędzia FDERT Restore Utility.

W przypadku VDI, jeśli masz urządzenie z zaszyfrowanymi dyskami, informacje na zaszyfrowanym dysku zostaną usunięte po usunięciu urządzenia.

Gdy ręcznie usuniesz urządzenie z grupy Urządzenia nieprzypisane, aplikacja usunie je z listy. Po usunięciu urządzenia zainstalowane aplikacje Kaspersky (jeśli istnieją) pozostają na urządzeniu. Następnie, jeśli urządzenie jest nadal widoczne dla Serwera administracyjnego i przeprowadzona została regularna konfiguracja przeszukiwania sieci Kaspersky Security Center wykrywa urządzenie podczas przeszukiwania sieci i dodaje je z powrotem do grupy Urządzenia nieprzypisane. Dlatego rozsądne jest ręczne usunięcie urządzenia tylko wtedy, gdy jest ono niewidoczne dla Serwera administracyjnego.

Usuwanie obiektu

Możesz usuwać obiekty, takie jak zasady, zadania, pakiety instalacyjne, użytkownicy wewnętrzni i wewnętrzne grupy bezpieczeństwa, jeśli masz uprawnienie Modyfikacja, które jest w kategorii Podstawowe funkcje uprawnień (więcej informacji znajdziesz w artykule Przydzielanie uprawnień użytkownikom i grupom).

Nie można usuwać pakietów instalacyjnych używanych w zadaniach instalacji zdalnej. Najpierw należy wyłączyć odpowiednie zadania. Więcej informacji na temat zadań automatycznej instalacji w grupie administracyjnej można znaleźć w artykule Automatyczna instalacja aplikacji na urządzeniach w grupie administracyjnej.

W celu usunięcia obiektu:

1. W drzewie konsoli, w obszarze roboczym żądanego folderu wybierz obiekt.
2. Wykonaj jedną z poniższych czynności:
   - Kliknij obiekt prawym klawiszem myszy i wybierz **Usuń**.
   - Wciśnij klawisz **DELETE**.

Obiekt zostanie usunięty, a informacje o nim będą przechowywane w bazie danych.

Przeglądanie informacji o usuniętych obiektach

Informacje o usuniętych obiektach są przechowywane w folderze Usunięte obiekty przez ten sam czas, co rewizje obiektu (zalecany okres to 90 dni).

Tylko użytkownicy z uprawnieniem **Odczyt** w obszarze uprawnień **Usunięte obiekty** mogą przeglądać listę usuniętych obiektów (więcej informacji znajdziesz w sekcji Przydzielanie uprawnień użytkownikom i grupom).

W celu wyświetlenia listy usuniętych obiektów:

W drzewie konsoli wybierz **Usunięte obiekty** (domyślnie **Usunięte obiekty** to podfolder folderu **Zaawansowane**).

Jeśli nie masz uprawnienia Odczyt w obszarze uprawnień **Usunięte obiekty**, pusta lista jest wyświetlana w folderze **Usunięte obiekty**.

Obszar roboczy folderu **Usunięte obiekty** zawiera następujące informacje o usuniętych obiektach:

- **Nazwa**. Nazwa obiektu.
- **Typ**. Typ obiektu, taki jak zasada, zadanie lub pakiet instalacyjny.
- **Czas**. Godzina usunięcia obiektu.
- **Użytkownik**. Nazwa konta użytkownika, który usunął obiekt.

W celu wyświetlenia więcej informacji o obiekcie:

1. W drzewie konsoli wybierz **Usunięte obiekty** (domyślnie **Usunięte obiekty** to podfolder folderu **Zaawansowane**).
2. W obszarze roboczym **Usunięte obiekty** wybierz obiekt, którego potrzebujesz.

   W prawej części obszaru roboczego pojawi się okno do pracy z wybranym obiektem.
3. Wykonaj jedną z poniższych czynności:
   - Kliknij odnośnik **Właściwości**, dostępny w oknie.
   - Kliknij prawym klawiszem myszy obiekt, który wybrałeś w obszarze roboczym, a w menu kontekstowym wybierz **Właściwości**.

   Zostanie otwarte okno właściwości obiektu, wyświetlające następujące zakładki:
   - **Ogólne**
   - **Historia rewizji**

Trwałe usuwanie obiektów z listy usuniętych obiektów

Tylko użytkownicy z uprawnieniem **Modyfikacja** w obszarze uprawnień **Usunięte obiekty** mogą trwale usuwać obiekty z listy usuniętych obiektów (więcej informacji znajdziesz w sekcji Przydzielanie uprawnień użytkownikom i grupom).

W celu usunięcia obiektu z listy usuniętych obiektów:

1. W drzewie konsoli wybierz węzeł żądanego Serwera administracyjnego, a następnie wybierz folder **Usunięte obiekty**.
2. W obszarze roboczym wybierz obiekt(y), który chcesz usunąć.
3. Wykonaj jedną z poniższych czynności:
   - Wciśnij klawisz **DELETE**.
   - W menu kontekstowym wybranego obiektu(ów) wybierz **Usuń**.
4. W oknie potwierdzenia kliknij **Tak**.

Obiekt zostaje trwale usunięty z listy usuniętych obiektów. Wszystkie informacje o tym obiekcie (w tym wszystkich jego rewizjach) zostają trwale usunięte z bazy danych. Nie możesz odzyskać tych informacji.

Zarządzanie urządzeniami mobilnymi

Zarządzanie ochroną urządzeń mobilnych poprzez Kaspersky Security Center jest realizowane przy użyciu funkcji Zarządzanie urządzeniami mobilnymi, która wymaga dedykowanej licencji. Jeśli zamierzasz zarządzać urządzeniami mobilnymi należącymi do pracowników Twojej organizacji, musisz włączyć Zarządzanie urządzeniami mobilnymi.

Ta sekcja zawiera instrukcja włączania, konfigurowania i wyłączania Zarządzania urządzeniami mobilnymi. W tej sekcji można znaleźć także opis sposobu zarządzania urządzeniami mobilnymi podłączonymi do Serwera administracyjnego.

Więcej informacji o Kaspersky Security for Mobile można znaleźć w *pomocy do Kaspersky Security for Mobile*.

Scenariusz: Wdrażanie Zarządzania urządzeniami mobilnymi

Ta sekcja zawiera scenariusz konfigurowania funkcji Zarządzanie urządzeniami mobilnymi w Kaspersky Security Center.

Wymagania wstępne

Upewnij się, że masz licencję, która daje dostęp do funkcji Zarządzanie urządzeniami mobilnymi.

Etapy

Wdrożenie funkcji Zarządzanie urządzeniami mobilnymi odbywa się w etapach:

1. **Przygotowywanie portów**

   Upewnij się, że port 13292 jest dostępny na Serwerze administracyjnym. Ten port jest wymagany do podłączania urządzeń mobilnych. Możesz także chcieć udostępnić port 17100. Ten port jest wymagany tylko do aktywacji poprzez serwer proxy dla zarządzanych urządzeń mobilnych; jeśli zarządzane urządzenia mobilne mają dostęp do internetu, nie musisz udostępniać tego portu.

2. **Włączanie Zarządzania urządzeniami mobilnymi**

   Możesz włączyć Zarządzanie urządzeniami mobilnymi, gdy uruchamiasz Kreator wstępnej konfiguracji Serwera administracyjnego lub w późniejszym czasie.

3. **Określanie zewnętrznego adresu Serwera administracyjnego**

   Możesz określić zewnętrzny adres, gdy uruchamiasz Kreator wstępnej konfiguracji Serwera administracyjnego lub w późniejszym czasie. Jeśli nie wybrałeś Zarządzania urządzeniami mobilnymi do zainstalowania i nie określiłeś adresu kreatora instalacji, określ zewnętrzny adres we właściwościach pakietu instalacyjnego.

4. **Dodawanie urządzeń mobilnych do grupy Zarządzane urządzenia**

   Dodaj urządzenia mobilne do grupy Zarządzane urządzenia, abyś mógł zarządzać tymi urządzeniami poprzez zasady. Możesz utworzyć regułę przenoszenia w jednym z kroków kreatora wstępnej konfiguracji Serwera administracyjnego. Możesz także utworzyć regułę przenoszenia w późniejszym czasie. Jeśli nie utworzysz takiej reguły, możesz ręcznie dodać urządzenia mobilne do grupy Zarządzane urządzenia.

   Możesz dodać urządzenia mobilne bezpośrednio do grupy Zarządzane urządzenia lub możesz utworzyć dla nich podgrupę (lub kilka podgrup).

   W dowolnym późniejszym czasie możesz podłączyć dowolne nowe urządzenie mobilne do Serwera administracyjnego przy użyciu kreatora podłączania nowego urządzenia mobilnego.

5. **Tworzenie zasady dla urządzeń mobilnych**

   Aby zarządzać urządzeniami mobilnymi, utwórz dla nich zasadę (lub kilka zasad) w grupie, do której należą te urządzenia. Możesz zmienić ustawienia tej zasady w dowolnym późniejszym czasie.

Wyniki

Po zakończeniu tego scenariusza, możesz zarządzać urządzeniami Android i iOS przy użyciu Kaspersky Security Center. Możesz pracować z certyfikatami urządzeń mobilnych i wysłać polecenia do urządzeń mobilnych.

Informacje o zasadzie grupy do zarządzania urządzeniami iOS MDM

Aby zarządzać urządzeniami iOS MDM, możesz wykorzystać wtyczkę zarządzającą Kaspersky Device Management for iOS, która znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center. Kaspersky Device Management for iOS umożliwia tworzenie zasad grupy do określania ustawień konfiguracji urządzeń iOS MDM bez użycia narzędzia iPhone® Configuration Utility.

Zasada grupy do zarządzania urządzeniami iOS MDM oferuje administratorowi następujące opcje:

- Konfigurowanie ustawień bezpieczeństwa hasła.
- Konfigurowanie ograniczeń użycia funkcji sprzętowych urządzenia oraz ograniczeń instalacji i dezinstalacji aplikacji mobilnych.
- Konfigurowanie ograniczeń użycia fabrycznie zainstalowanych aplikacji mobilnych, takich jak YouTube™, iTunes® Store lub Safari.
- Konfigurowanie ograniczeń przeglądania mediów (filmów i programów TV) według regionu, w którym zlokalizowane jest urządzenie.
- Konfigurowanie ustawień połączenia urządzenia z internetem poprzez serwer proxy (globalny serwer pośredniczący HTTP).
- Konfigurowanie ustawień konta, przy użyciu którego użytkownik może uzyskać dostęp do usług i aplikacji firmowych (technologia pojedynczego logowania - Single Sign On).
- Monitorowanie korzystania z internetu (odwiedzanych stron internetowych) na urządzeniach mobilnych.
- Konfigurowanie ustawień sieci bezprzewodowych (Wi-Fi), punktów dostępu (APN) i wirtualnych sieci prywatnych (VPN), które używają różnych mechanizmów autoryzacji i protokołów sieciowych.
- Konfigurowanie ustawień nawiązywania połączenia z urządzeniami AirPlay® do przesyłania zdjęć, muzyki i filmów.
- Konfigurowanie ustawień nawiązywania połączenia z drukarkami AirPrint™ w celu bezprzewodowego drukowania dokumentów z urządzenia.
- Konfigurowanie ustawień synchronizacji z serwerem Microsoft Exchange i kontami użytkowników w celu korzystania z poczty firmowej na urządzeniach.
- Konfigurowanie danych uwierzytelniających użytkowników do synchronizacji z usługą katalogową LDAP.
- Konfigurowanie danych uwierzytelniających użytkowników do nawiązywania połączenia z usługami CalDAV i CardDAV, które dają użytkownikom dostęp do kalendarzy firmowych i list kontaktów.
- Konfigurowanie ustawień interfejsu iOS na urządzeniu użytkownika, takich jak czcionki lub ikony dla ulubionych stron internetowych.
- Dodawanie nowych certyfikatów zabezpieczeń na urządzeniach.
- Konfigurowanie ustawień serwera Simple Certificate Enrollment Protocol (SCEP) do automatycznego pobierania certyfikatów z Urzędu certyfikacji.
- Dodawanie niestandardowych ustawień dla pracy z aplikacjami mobilnymi.

Zasada do zarządzania urządzeniami iOS MDM wyróżnia się tym, że jest przypisana do grupy administracyjnej, która zawiera serwer iOS MDM (zwane dalej "serwery urządzeń mobilnych"). Wszystkie ustawienia określone w tej zasadzie są w pierwszej kolejności stosowane do serwerów urządzeń mobilnych, a następnie do urządzeń mobilnych zarządzanych przez takie serwery. W przypadku hierarchicznej struktury grup administracyjnych, podrzędne serwery urządzeń mobilnych pobierają ustawienia zasady z głównych serwerów urządzeń mobilnych i rozsyłają je na urządzenia mobilne.

Więcej informacji dotyczących używania zasady grupy do zarządzania urządzeniami iOS MDM w Konsoli administracyjnej Kaspersky Security Center można znaleźć w dokumentacji do *Kaspersky Security for Mobile*.

Włączanie Zarządzania urządzeniami mobilnymi

Aby możliwe było zarządzanie urządzeniami mobilnymi, należy włączyć Zarządzanie urządzeniami mobilnymi. Jeśli nie włączono tej funkcji w kreatorze wstępnej konfiguracji, możesz włączyć ją później. Zarządzanie urządzeniami mobilnymi wymaga licencji.

Włączenie Zarządzania urządzeniami mobilnymi jest dostępne tylko na głównym Serwerze administracyjnym.

W celu włączenia Zarządzania urządzeniami mobilnymi:

1. W drzewie konsoli wybierz folder **Zarządzanie urządzeniami mobilnymi**.
2. W obszarze roboczym folderu kliknij przycisk **Włącz zarządzanie urządzeniami mobilnymi**. Ten przycisk jest dostępny, jeśli wcześniej nie włączyłeś **Zarządzanie urządzeniami mobilnymi**.

   Zostanie wyświetlone okno **Dodatkowe składniki** kreatora wstępnej konfiguracji Serwera administracyjnego.
3. Wybierz **Włącz zarządzanie urządzeniami mobilnymi**, aby zarządzać urządzeniami mobilnymi.
4. W oknie **Wybierz metodę aktywacji aplikacji** aktywuj aplikację przy użyciu pliku klucza lub kodu aktywacyjnego.

   Zarządzanie urządzeniami mobilnymi będzie niemożliwe, dopóki nie aktywujesz funkcji Zarządzanie urządzeniami mobilnymi.
5. Na stronie **Ustawienia serwera proxy umożliwiającego dostęp do internetu** zaznacz pole **Użyj serwera proxy**, jeśli podczas nawiązywania połączenia z internetem chcesz używać serwera proxy. Jeśli to pole jest zaznaczone, dostępne staną się pola do wprowadzenia ustawień. Określ ustawienia połączenia z serwerem proxy.
6. Na stronie **Sprawdzanie aktualizacji dla wtyczek i pakietów instalacyjnych** wybierz jedną z następujących opcji:

   - **Sprawdź, czy wtyczki i pakiety instalacyjne są aktualne**

     Rozpoczynanie sprawdzania, czy wtyczki i pakiety instalacyjne są aktualne. Jeśli podczas sprawdzania zostaną wykryte przestarzałe wersje wtyczek lub pakietów instalacyjnych, kreator wyświetli okno z pytaniem o pobranie aktualnych wersji do zastąpienia tych przestarzałych.

   - **Pomiń sprawdzanie**

     Kontynuowanie pracy bez sprawdzania, czy wtyczki i pakiety instalacyjne są aktualne. Możesz wybrać tę opcję, jeśli, na przykład, nie posiadasz dostępu do Internetu lub jeśli z jakiegoś powodu chcesz korzystać z przestarzałej wersji aplikacji.

     Pominięcie sprawdzania dostępności uaktualnień dla wtyczek może spowodować niepoprawne działanie aplikacji.

7. W oknie **Dostępna jest najnowsza wersja wtyczki** pobierz i zainstaluj najnowsze wersje wtyczek w wersji językowej wymaganej przez wersję posiadanej aplikacji. Do aktualizowania wtyczek nie jest wymagana licencja.

   Po zainstalowaniu wtyczek i pakietów, aplikacja sprawdza, czy zainstalowane są wszystkie wtyczki niezbędne do poprawnego działania urządzeń mobilnych. Jeśli zostaną wykryte przestarzałe wersje wtyczek, kreator wyświetli okno z pytaniem o pobranie aktualnych wersji do zastąpienia tych przestarzałych.

8. Na stronie **Ustawienia połączenia urządzenia mobilnego** skonfiguruj porty Serwera administracyjnego.

Po zakończeniu pracy kreatora zostaną wprowadzone następujące zmiany:

- Zostanie utworzona zasada Kaspersky Endpoint Security for Android.
- Zostanie utworzona zasada Kaspersky Device Management for iOS.
- Porty zostaną otwarte na Serwerze administracyjnym dla urządzeń mobilnych.

Modyfikowanie ustawień Zarządzania urządzeniami mobilnymi

W celu włączenia obsługi urządzeń mobilnych:

1. W drzewie konsoli wybierz folder **Zarządzanie urządzeniami mobilnymi**.
2. W obszarze roboczym folderu kliknij odnośnik **Porty połączenia dla urządzeń mobilnych**.

   Zostanie wyświetlona sekcja **Porty dodatkowe** okna właściwości Serwera administracyjnego.
3. W sekcji **Porty dodatkowe** zmodyfikuj odpowiednie ustawienia:

   - **Port SSL do aktywacji przy użyciu serwera proxy**
   - **Otwórz port dla urządzeń mobilnych**

     Port zostaje otwarty dla urządzeń mobilnych do połączenia z serwerem licencjonowania. Możesz zdefiniować numer portu i inne ustawienia w polach poniżej.

     Domyślnie opcja ta jest włączona.
   - **Port do synchronizacji urządzeń mobilnych**

     Numer portu, za pomocą którego urządzenia mobilne będą łączyć się z Serwerem administracyjnym i będą wymieniać z nim dane. Domyślny numer portu to 13292.

     Jeśli port 13292 jest używany do innych celów, można przypisać inny port.
   - **Port do aktywacji urządzeń mobilnych**

     Port do łączenia Kaspersky Endpoint Security for Android z serwerami aktywacji Kaspersky.

     Domyślny numer portu to 17100.
4. Kliknij **OK**.

Wyłączanie Zarządzania urządzeniami mobilnymi

Wyłączenie Zarządzania urządzeniami mobilnymi jest dostępne tylko na głównym Serwerze administracyjnym.

W celu wyłączenia Zarządzania urządzeniami mobilnymi:

1. W drzewie konsoli wybierz folder **Zarządzanie urządzeniami mobilnymi**.
2. W obszarze roboczym tego folderu kliknij odnośnik **Skonfiguruj dodatkowe składniki**.

   Zostanie wyświetlone okno **Dodatkowe składniki** kreatora wstępnej konfiguracji Serwera administracyjnego.
3. Wybierz **Nie włączaj Zarządzania urządzeniami mobilnymi**, jeśli nie chcesz już zarządzać urządzeniami mobilnymi.
4. Kliknij **OK**.

   Wcześniej podłączone urządzenia mobilne nie będą mogły nawiązać połączenia z Serwerem administracyjnym. Port dla połączenia urządzenia mobilnego oraz port dla aktywacji urządzenia mobilnego zostaną zamknięte automatycznie.

   Zasady, które zostały utworzone dla Kaspersky Endpoint Security for Android i Kaspersky Device Management for iOS, nie zostaną usunięte. Reguły wydawania certyfikatów nie zostaną zmodyfikowane. Zainstalowane wtyczki nie zostaną usunięte. Reguła przenoszenia dla urządzeń mobilnych nie zostanie usunięta.

Po ponownym włączeniu Zarządzania urządzeniami mobilnymi na zarządzanych urządzeniach mobilnych, konieczne może być ponowne zainstalowanie aplikacji mobilnych, wymaganych do zarządzania urządzeniami mobilnymi.

Praca z poleceniami dla urządzeń mobilnych

Ta sekcja zawiera informacje o poleceniach do zarządzania urządzeniami mobilnymi obsługiwanych przez Kaspersky Security Center. Sekcja zawiera instrukcje dotyczące wysyłania poleceń na urządzenia mobilne, a także dotyczące przeglądania stanów wykonywania poleceń w raporcie poleceń.

Polecenia zarządzania urządzeniem mobilnym

Kaspersky Security Center obsługuje polecenia do zarządzania urządzeniami mobilnymi.

Takie polecenia są używane do zdalnego zarządzania urządzeniami mobilnymi. Na przykład, gdy urządzenie mobilne zostanie zgubione, można usunąć z niego wszystkie dane firmowe, korzystając z odpowiedniego polecenia.

Możesz użyć poleceń dla następujących typów zarządzanych urządzeń mobilnych:

- Urządzenia iOS MDM
- Urządzenia Kaspersky Endpoint Security (KES)

Każde urządzenie obsługuje dedykowany zestaw poleceń.

Uwagi dotyczące pewnych poleceń

- W przypadku wszystkich typów urządzeń, gdy polecenie **Przywróć ustawienia fabryczne** zostanie pomyślnie wykonane, wszystkie dane zostaną usunięte z urządzenia i zostaną przywrócone ustawienia fabryczne.
- Po pomyślnym wykonaniu polecenia **Wyczyść dane firmowe** na urządzeniu iOS MDM, wszystkie zainstalowane profile konfiguracyjne, profile informacyjne, profil iOS MDM oraz aplikacje, dla których zaznaczono pole **Usuń wraz z profilem iOS MDM**, zostaną usunięte z urządzenia.
- Jeśli polecenie **Wyczyść dane firmowe** zostanie pomyślnie wykonane na urządzeniu KES, wszystkie dane firmowe, wpisy z Kontaktów, historia wiadomości SMS, rejestr połączeń, kalendarz, ustawienia połączenia internetowego oraz konta użytkownika (za wyjątkiem konta Google™) zostaną usunięte z urządzenia. W przypadku urządzeń KES zostaną usunięte także wszystkie dane z karty pamięci.
- Przed wysłaniem polecenia **Lokalizacja** na urządzenie KES konieczne będzie potwierdzenie, że korzystasz z tego polecenia do autoryzowanego wyszukiwania zagubionego urządzenia, które należy do Twojej organizacji lub do jednego z pracowników. Urządzenie mobilne, które otrzymuje polecenie **Lokalizacja**, nie jest zablokowane.

Lista poleceń dla urządzeń mobilnych

Poniższa tabela wyświetla zestawy poleceń dla urządzeń iOS MDM.

Obsługiwane polecenia do zarządzania urządzeniami mobilnymi: urządzenia iOS MDM

Polecenia	Wynik wykonania polecenia
Zablokuj	Urządzenie mobilne zostanie zablokowane.
Odblokuj	Zablokowanie urządzenia mobilnego przy użyciu kodu PIN jest wyłączone. Wcześniej określony kod PIN został zresetowany.
Przywróć ustawienia fabryczne	Wszystkie dane zostaną usunięte z urządzenia mobilnego oraz zostaną przywrócone ustawienia domyślne.
Wyczyść dane firmowe	Wszystkie zainstalowane profile konfiguracyjne, profile informacyjne, profil iOS MDM oraz aplikacje, dla których zaznaczono pole **Usuń wraz z profilem iOS MDM**, zostaną usunięte z urządzenia.
Synchronizuj urządzenie	Dane urządzenia mobilnego zostaną zsynchronizowane z Serwerem administracyjnym.
Zainstaluj profil	Profil konfiguracyjny zostaje zainstalowany na urządzeniu mobilnym.
Usuń profil	Profil konfiguracyjny zostaje usunięty z urządzenia mobilnego.
Zainstaluj profil informacyjny	Profil informacyjny zostaje zainstalowany na urządzeniu mobilnym.
Usuń profil informacyjny	Profil informacyjny zostaje usunięty z urządzenia mobilnego.
Zainstaluj aplikację	Aplikacja zostanie zainstalowana na urządzeniu mobilnym.
Usuń aplikację	Aplikacja zostanie usunięta z urządzenia mobilnego.
Wprowadź kod wykupu	Wprowadzenie kodu wykupu dla płatnej aplikacji.
Konfiguruj roaming	Włączenie lub wyłączenie roamingu danych i roamingu połączeń.

Poniższa tabela wyświetla zestawy poleceń dla urządzeń KES.

Polecenie	Wynik wykonania polecenia
Zablokuj	Urządzenie mobilne zostanie zablokowane.
Odblokuj	Zablokowanie urządzenia mobilnego przy użyciu kodu PIN jest wyłączone. Wcześniej określony kod PIN został zresetowany.
Przywróć ustawienia fabryczne	Wszystkie dane zostaną usunięte z urządzenia mobilnego oraz zostaną przywrócone ustawienia domyślne.
Wyczyść dane firmowe	Dane firmowe, wpisy w Kontaktach, historia wiadomości SMS, rejestr połączeń, kalendarz, ustawienia połączenia internetowego oraz konta użytkownika (za wyjątkiem konta Google) zostaną usunięte. Dane znajdujące się na karcie pamięci także zostaną usunięte.
Synchronizuj urządzenie	Dane urządzenia mobilnego zostaną zsynchronizowane z Serwerem administracyjnym.
Zlokalizuj urządzenie	Urządzenie mobilne zostanie zlokalizowanie, a jego pozycja zostanie wyświetlona na Google Maps™. Operator telefonii komórkowej pobiera opłatę za wysłanie wiadomości SMS oraz za korzystanie z internetu.
Wykonaj zdjęcie (mugshot)	Urządzenie mobilne zostanie zablokowane. Zostanie wykonane zdjęcie urządzenia przednią kamerą, a następnie zostanie ono wysłane na Serwer administracyjny. Zdjęcia można przejrzeć w raporcie poleceń. Operator telefonii komórkowej pobiera opłatę za wysłanie wiadomości SMS oraz za korzystanie z internetu.
Alarm	Urządzenie mobilne włączy alarm.

Korzystanie z Firebase Cloud Messaging

Aby zapewnić dostarczanie w odpowiednim momencie poleceń na urządzenia KES działające pod systemem operacyjnym Android, Kaspersky Security Center korzysta z mechanizmów powiadomień push. Powiadomienia push są wymieniane pomiędzy urządzeniami KES a Serwerem administracyjnym za pośrednictwem usługi Firebase Cloud Messaging (zwanej dalej FCM). W Konsoli administracyjnej Kaspersky Security Center możesz określić ustawienia Firebase Cloud Messaging do podłączania urządzeń KES do usługi.

Aby pobrać ustawienia Firebase Cloud Messaging, należy posiadać konto Google.

W celu włączenia korzystania z FCM:

1. W Konsoli administracyjnej wybierz węzeł **Zarządzanie urządzeniami mobilnymi** oraz folder **Urządzenia mobilne**.
2. Z otwartego menu kontekstowego folderu **Urządzenia mobilne** wybierz **Właściwości**.
3. We właściwościach folderu wybierz sekcję **Ustawienia Firebase Cloud Messaging**.
4. W polu **Numer projektu Firebase** podaj identyfikator nadawcy FCM.
5. W polu **Plik klucza prywatnego (w formacie JSON)** wybierz plik klucza prywatnego.

   Przy kolejnej synchronizacji z Serwerem administracyjnym, urządzenia KES, działające pod systemami operacyjnymi Android, zostaną połączone z Firebase Cloud Messaging.

Możesz zmodyfikować ustawienia Firebase Cloud Messaging, klikając przycisk **Resetuj ustawienia**.

Wysyłanie poleceń

W celu wysłania polecenia na urządzenie mobilne użytkownika:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. Wybierz urządzenie mobilne użytkownika, na które chcesz wysłać polecenie.

3. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

4. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji z nazwą polecenia, które chcesz wysłać na urządzenie mobilne, a następnie kliknij przycisk **Wyślij polecenie**.

   W zależności od wybranego polecenia, kliknięcie przycisku **Wyślij polecenie** może spowodować otwarcie okna zaawansowanych ustawień aplikacji. Na przykład, jeśli wyślesz polecenie usunięcia profilu informacyjnego z urządzenia mobilnego, aplikacja wyświetli pytanie o wybór profilu informacyjnego, który musi zostać usunięty z urządzenia mobilnego. Zdefiniuj zaawansowane ustawienia polecenia w tym oknie i potwierdź swój wybór. Polecenie zostanie wysłane na urządzenie mobilne.

   Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

   Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

   Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

5. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Przeglądanie stanów poleceń w raporcie poleceń

Aplikacja zapisuje do raportu poleceń informacje o wszystkich poleceniach, które zostały wysłane na urządzenia mobilne. Raport poleceń zawiera informacje o godzinie i dacie wysłania każdego polecenia na urządzenie mobilne, ich odpowiednich stanach i szczegółowych opisach wyników wykonania poleceń. Na przykład, gdy wykonanie polecenia zakończy się niepowodzeniem, raport będzie wyświetlał przyczynę błędu. Wpisy są przechowywane w raporcie poleceń najwyżej przez 30 dni.

Polecenia wysłane na urządzenia mobilne mogą posiadać następujące stany:

- *Uruchomione*—polecenie zostało wysłane na urządzenie mobilne.
- *Zakończone*—wykonanie polecenia zostało pomyślnie zakończone.
- *Zakończone błędem*—wykonanie polecenia nie powiodło się.
- *Usuwanie*— polecenie jest usuwane z kolejki poleceń wysyłanych na urządzenie mobilne.
- *Usunięte*—polecenie zostało usunięte z kolejki poleceń wysyłanych na urządzenie mobilne.
- *Błąd usuwania*—polecenie nie mogło zostać usunięte z kolejki poleceń wysyłanych na urządzenie mobilne.

Aplikacja przechowuje raport poleceń dla każdego urządzenia mobilnego.

W celu przejrzenia raportu poleceń wysłanych na urządzenie mobilne:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. Na liście urządzeń mobilnych wybierz to, dla którego chcesz przejrzeć raport poleceń.

3. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

   Zostanie otwarte okno **Polecenia administracyjne urządzenia mobilnego**. Sekcje okna **Polecenia administracyjne urządzenia mobilnego** odpowiadają poleceniom, które mogą być wysłane na urządzenie mobilne.

4. Wybierz sekcje zawierające żądane polecenia i przejrzyj informacje dotyczące wysłania i wykonania poleceń w sekcji **Raport poleceń**.

W sekcji **Raport poleceń** możesz przejrzeć listę poleceń, które zostały wysłane na urządzenie mobilne, oraz szczegóły dotyczące tych poleceń. Filtr **Pokaż polecenia** umożliwia wyświetlanie na liście tylko poleceń z wybranym stanem.

Praca z certyfikatami urządzeń mobilnych

Ta sekcja zawiera informacje dotyczące pracy z certyfikatami urządzeń mobilnych.

Certyfikat główny dla urządzeń mobilnych ma stały okres ważności wynoszący 700 dni od daty wygenerowania. Certyfikat rezerwowy jest generowany 60 dni przed datą wygaśnięcia. Możesz zmodyfikować okres czasu potrzebny na wygenerowanie certyfikatu rezerwowego za pomocą następującego polecenia:

`klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v <limit czasu w sekundach>`

Okres czasu potrzebny na wygenerowanie certyfikatu zapasowego musi być wystarczająco długi, aby wszystkie zarządzane urządzenia mobilne zdążyły zsynchronizować się z serwerem administracyjnym i pobrać certyfikat.

Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Ręczne odnawianie certyfikatu głównego dla urządzeń mobilnych nie jest obsługiwane.

Uruchamianie kreatora instalacji certyfikatu

Na urządzeniu mobilnym użytkownika możesz zainstalować następujące typy certyfikatów:

- Certyfikaty współdzielone do identyfikacji urządzenia mobilnego
- Certyfikat pocztowy do konfiguracji poczty firmowej na urządzeniu mobilnym
- Certyfikat VPN do konfigurowania dostępu do wirtualnej sieci prywatnej na urządzeniu mobilnym

W celu zainstalowania certyfikatu na urządzeniu mobilnym użytkownika:

1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.

2. W obszarze roboczym folderu **Certyfikaty** kliknij odnośnik **Dodaj certyfikat**, aby uruchomić kreator instalacji certyfikatu.

   Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora, certyfikat zostanie utworzony i dodany do listy certyfikatów użytkownika. Dodatkowo, do użytkownika zostanie wysłane powiadomienie zawierające odsyłacz do pobrania i zainstalowania certyfikatu na urządzeniu mobilnym. Listę wszystkich certyfikatów można przejrzeć oraz wyeksportować do pliku. Możesz usunąć i ponownie wydać certyfikaty, a także wyświetlić ich właściwości.

Krok 1. Wybieranie typu certyfikatu

Określ typ certyfikatu, który musi być zainstalowany na urządzeniu mobilnym użytkownika:

- **Certyfikat dla urządzeń mobilnych**—do identyfikowania urządzenia mobilnego
- **Certyfikat pocztowy**—do skonfigurowania poczty firmowej na urządzeniu mobilnym
- **Certyfikat VPN**—do skonfigurowania dostępu do wirtualnej sieci prywatnej na urządzeniu mobilnym

Krok 2. Wybieranie typu urządzenia

To okno jest wyświetlane tylko wtedy, gdy jako typ certyfikatu wybrałeś **Certyfikat pocztowy** lub **Certyfikat VPN**.

Określ typ systemu operacyjnego na urządzeniu:

- **Urządzenie iOS MDM**. Wybierz tę opcję, jeśli musisz zainstalować certyfikat na urządzeniu mobilnym, które jest podłączone do serwera iOS MDM przy użyciu protokołu iOS MDM.
- **Urządzenie KES zarządzane przez Kaspersky Security for Mobile**. Wybierz tę opcję, jeśli musisz zainstalować certyfikat na urządzeniu KES. W tym przypadku certyfikat będzie używany do identyfikacji użytkownika po każdym połączeniu z Serwerem administracyjnym.
- **Urządzenie KES połączone z Serwerem administracyjnym bez uwierzytelniania certyfikatu użytkownika**. Wybierz tę opcję, jeśli musisz zainstalować certyfikat na urządzeniu KES bez użycia uwierzytelniania certyfikatu. W tym przypadku, w ostatnim kroku kreatora, w oknie **Metoda powiadamiania użytkownika** administrator musi wybrać typ uwierzytelniania użytkownika używany przy każdym połączeniu z Serwerem administracyjnym.

Krok 3. Wybieranie użytkownika

Na liście wybierz użytkowników, grupy bezpieczeństwa lub grupy bezpieczeństwa Active Directory, dla których musisz zainstalować certyfikat.

W oknie **Wybór użytkownika** możesz wyszukać użytkowników wewnętrznych Kaspersky Security Center. Możesz kliknąć **Dodaj**, aby dodać użytkownika wewnętrznego.

Krok 4. Wybieranie źródła certyfikatu

W tym oknie można wybrać źródło certyfikatu, którego Serwer administracyjny będzie używał do identyfikowania urządzeń mobilnych. Certyfikat można określić przy użyciu jednej z następujących metod:

- Automatycznie utwórz certyfikat przy użyciu narzędzi Serwera administracyjnego, a następnie wyślij certyfikat na urządzenie.
- Określ plik certyfikatu, który został utworzony wcześniej. Ta metoda nie jest dostępna, jeśli w poprzednim kroku zaznaczono wielu użytkowników.

Zaznacz pole **Opublikuj certyfikat**, jeśli musisz wysłać użytkownikowi powiadomienie o utworzeniu certyfikatu dla jego/jej urządzenia mobilnego.

Jeśli dla urządzenia mobilnego użytkownika przeprowadzono już uwierzytelnianie z użyciem certyfikatu, dzięki czemu nie ma potrzeby określenia nazwy konta i hasła do pobrania nowego certyfikatu, odznacz pole **Opublikuj certyfikat**. W tym przypadku okno **Metoda powiadamiania użytkownika** nie zostanie wyświetlone.

Krok 5. Przypisywanie znacznika do certyfikatu

Okno **Znacznik certyfikatu** jest wyświetlane, jeśli opcja **Urządzenie iOS MDM** została wybrana w **Typ urządzenia**.

Na liście rozwijalnej możesz przypisać znacznik do certyfikatu urządzenia iOS MDM użytkownika. Certyfikat z przypisanym znacznikiem może posiadać określone parametry ustawione dla tego znacznika we właściwościach zasady Kaspersky Device Management for iOS.

Lista rozwijana oferuje wybranie znacznika *Szablon certyfikatu 1*, *Szablon certyfikatu 2* lub *Szablon certyfikatu 3*. Znaczniki można skonfigurować w następujących sekcjach:

- Jeśli w oknie **Typ certyfikatu** wybrano **Certyfikat pocztowy**, znaczniki dla tego certyfikatu można skonfigurować we właściwościach konta Exchange ActiveSync dla urządzeń mobilnych (**Zarządzane urządzenia** → **Zasady** → Właściwości zasady Kaspersky Device Management for iOS > sekcja **Exchange ActiveSync** → **Dodaj** → **Zaawansowane**).
- Jeśli w oknie **Typ certyfikatu** wybrano **Certyfikat VPN**, znaczniki dla tego certyfikatu można skonfigurować we właściwościach VPN dla urządzeń mobilnych (**Zarządzane urządzenia** → **Zasady** → Właściwości zasady Kaspersky Device Management for iOS → sekcja **VPN** → **Dodaj** → **Zaawansowane**). Nie możesz skonfigurować znaczników używanych dla certyfikatów VPN, jeśli dla swojego VPN wybrano typ połączenia L2TP, PPTP lub IPSec (Cisco™).

Krok 6. Określanie ustawień publikowania certyfikatu

W tym oknie możesz określić następujące ustawienia publikowania certyfikatu:

- **Nie powiadamiaj użytkownika o nowym certyfikacie**

  Włącz tę opcję, jeśli nie chcesz wysłać użytkownikowi powiadomienia o tworzeniu certyfikatu dla urządzenia mobilnego użytkownika. W tym przypadku okno **Metoda powiadamiania użytkownika** nie zostanie wyświetlone.

  > Ta opcja jest stosowana tylko do urządzeń z zainstalowanym programem Kaspersky Endpoint Security for Android.

  Możesz włączyć tę opcję, na przykład, jeśli urządzenie mobilne użytkownika zostało wcześniej uwierzytelnione przy użyciu certyfikatu, więc nie ma konieczności określenia nazwy konta i hasła do odebrania nowego certyfikatu.

- **Zezwól urządzeniu na wielu odbiorców jednego certyfikatu (wyłącznie dla urządzeń z zainstalowaną aplikacją Kaspersky Endpoint Security for Android)**

  Włącz tę opcję, jeśli chcesz, żeby Kaspersky Security Center automatycznie rozsyłała certyfikat za każdym razem, gdy wkrótce wygaśnie lub gdy nie zostanie znaleziony na urządzeniu docelowym.

  Certyfikat jest automatycznie rozsyłany kilka dni przed datą wygaśnięcia certyfikatu. Możesz ustawić liczbę dni w oknie Reguły wydawania certyfikatu.

  W niektórych przypadkach certyfikat nie może zostać znaleziony na urządzeniu. Na przykład, to może mieć miejsce, gdy użytkownik zainstaluje ponownie aplikację zabezpieczającą Kaspersky na urządzeniu lub zresetuje dane i przywróci domyślne ustawienia urządzenia. W tym przypadku Kaspersky Security Center sprawdza identyfikator urządzenia przy kolejnej próbie połączenia urządzenia z Serwerem administracyjnym. Jeśli urządzenie posiada ten sam identyfikator, który miał, gdy certyfikat został wydany, aplikacja wyśle certyfikat na urządzenie.

Krok 7. Wybieranie metody powiadamiania użytkownika

> To okno nie jest wyświetlane, jeśli jako typ urządzenia wybrałeś **Urządzenie iOS MDM** lub jeśli wybrałeś opcję **Nie powiadamiaj użytkownika o nowym certyfikacie**.

W sekcji **Metoda powiadamiania użytkownika** możesz skonfigurować powiadamianie użytkownika o instalacji certyfikatu na urządzeniu mobilnym.

W polu **Metoda uwierzytelniania** określ typ uwierzytelniania użytkownika:

- **Poświadczenia (domena lub alias)**

  W tym przypadku, do pobrania nowego certyfikatu użytkownik stosuje hasło domeny lub hasło wewnętrznego użytkownika Kaspersky Security Center.

- **Hasło jednorazowe**

  W tym przypadku użytkownik otrzymuje hasło jednorazowe, które zostanie wysłane w wiadomości e-mail lub SMS. To hasło musi zostać wprowadzone, aby możliwe było pobranie nowego certyfikatu.

Ta opcja zmieni się na **Hasło**, jeśli w oknie **Ustawienia publikowania certyfikatu** włączyłeś (zaznaczyłeś) opcję **Zezwól na wiele urządzeń odbierających jeden certyfikat (wyłącznie dla urządzeń mobilnych z zainstalowanymi aplikacjami Kaspersky)**.

- **Hasło**

  W tym przypadku hasło jest używane za każdym razem, gdy certyfikat zostanie wysłany do użytkownika.

  Ta opcja zmieni się na **Hasło jednorazowe**, jeśli w oknie **Ustawienia publikowania certyfikatu** wyłączyłeś (odznaczyłeś) opcję **Zezwól na wiele urządzeń odbierających jeden certyfikat (wyłącznie dla urządzeń mobilnych z zainstalowanymi aplikacjami Kaspersky)**.

To pole jest wyświetlane, jeśli wybrałeś **Certyfikat dla urządzeń mobilnych** w oknie **Typ certyfikatu** lub jeśli jako typ urządzenia wybrałeś **Urządzenie KES połączone z Serwerem administracyjnym bez uwierzytelniania certyfikatu użytkownika**.

Wybierz opcję powiadamiania użytkownika:

- **Po zakończeniu działania kreatora wyświetl hasło uwierzytelniające**

  Jeśli wybierzesz tę opcję, nazwa użytkownika, nazwa użytkownika w Menedżerze kont zabezpieczeń (SAM), a także hasło do odzyskania certyfikatu dla każdego z wybranych użytkowników zostanie wyświetlone w ostatnim kroku kreatora instalacji certyfikatu. Konfiguracja powiadamiania użytkownika o zainstalowanym certyfikacie będzie niedostępna.

  Jeśli dodasz certyfikaty dla kilku użytkowników, możesz zapisać dostarczone poświadczenia do pliku, klikając przycisk **Eksportuj** w ostatnim kroku kreatora instalacji certyfikatu.

  > Ta opcja jest niedostępna, jeśli w kroku **Metoda powiadamiania użytkownika** wybrano Poświadczenia (domena lub alias).

- **Powiadom użytkownika o nowym certyfikacie**

  Jeśli wybierzesz tę opcję, możesz skonfigurować powiadamianie użytkownika o nowym certyfikacie.

  - **Przez e-mail**

    W tej grupie ustawień możesz skonfigurować powiadamianie użytkownika o instalacji nowego certyfikatu na jego urządzeniu mobilnym za pośrednictwem wiadomości e-mail. Ta metoda powiadamiania jest dostępna tylko wtedy, gdy opcja Serwer SMTP jest włączona.

    Kliknij odnośnik **Edytuj wiadomość**, aby wyświetlić i edytować powiadomienie (jeśli to konieczne).

  - **Przez SMS**

    W tej grupie ustawień możesz skonfigurować powiadamianie użytkownika o używaniu wiadomości SMS do zainstalowania certyfikatu na urządzeniach mobilnych. Ta metoda powiadamiania jest dostępna tylko wtedy, gdy opcja Powiadomienia SMS jest włączona.

    Kliknij odnośnik **Edytuj wiadomość**, aby wyświetlić i edytować powiadomienie (jeśli to konieczne).

Krok 8. Generowanie certyfikatu

W tym kroku zostanie utworzony certyfikat.

Możesz kliknąć **Zakończ**, aby zakończyć działanie kreatora.

Certyfikat zostanie wygenerowany i wyświetlony na liście certyfikatów, w obszarze roboczym folderu **Certyfikaty**.

Konfigurowanie reguł wydawania certyfikatów

Certyfikaty są używane do autoryzacji urządzenia na Serwerze administracyjnym. Wszystkie zarządzane urządzenia mobilne muszą posiadać certyfikaty. Możesz skonfigurować sposób publikowania certyfikatów.

W celu skonfigurowania reguł wydawania certyfikatu:

1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.

2. W obszarze roboczym folderu **Certyfikaty** kliknij przycisk **Konfiguruj reguły wydawania certyfikatów**, aby otworzyć okno **Reguły wydawania certyfikatu**.

3. Przejdź do sekcji z nazwą typu certyfikatu:

   Wydawanie certyfikatów dla urządzeń mobilnych—aby skonfigurować wydawanie certyfikatów dla urządzeń mobilnych.

   Wydawanie certyfikatów pocztowych—aby skonfigurować wydawanie certyfikatów pocztowych.

   Wydawanie certyfikatów VPN—aby skonfigurować wydawanie certyfikatów VPN.

4. W sekcji **Ustawienia wydawania** skonfiguruj wydawanie certyfikatów:

   - Określ czas życia certyfikatu w dniach.

     Certyfikaty dla urządzeń mobilnych są ograniczone datą wygaśnięcia certyfikatu głównego. Jeżeli określisz okres ważności certyfikatu dłuższy niż data wygaśnięcia certyfikatu głównego, okres ważności certyfikatu zostanie automatycznie dostosowany w momencie wygenerowania.

   - Wybierz źródło certyfikatu (**Serwer administracyjny** lub **Certyfikaty określone ręcznie**).

     Serwer administracyjny jest wybrany jako domyślne źródło certyfikatów.

   - Określ szablon certyfikatu (**Szablon domyślny**, **Inny szablon**).

     Konfiguracja szablonów jest dostępna, jeśli sekcja **Integracja z PKI** zawiera włączoną integrację z infrastrukturą kluczy publicznych.

5. W sekcji **Ustawienia aktualizacji automatycznych** skonfiguruj automatyczne aktualizacje certyfikatu:

   - W polu **Odnów, gdy certyfikat wygaśnie za (dni)** określ, ile dni przed wygaśnięciem certyfikat powinien zostać odnowiony.

   - Aby włączyć automatyczne aktualizacje certyfikatów, zaznacz pole **Odnów certyfikat automatycznie, jeśli jest to możliwe**.

6. W sekcji **Ochrona hasłem** włącz i skonfiguruj użycie hasła podczas deszyfrowania certyfikatów.

Ochrona hasłem jest dostępna tylko dla certyfikatów dla urządzeń mobilnych.

a. Zaznacz pole **Pytaj o hasło podczas instalowania certyfikatów**.

b. Użyj suwaka, aby zdefiniować maksymalną liczbę znaków w haśle do szyfrowania.

7. Kliknij **OK**.

Integracja z infrastrukturą kluczy publicznych

Integracja aplikacji z Infrastrukturą klucza publicznego (PKI) jest wymagana do uproszczenia wydawania użytkownikom certyfikatów dla domen. Po przeprowadzeniu integracji certyfikaty są generowane automatycznie.

Minimalna obsługiwana wersja serwera PKI to Windows Server 2008.

Musisz skonfigurować konto do integracji z PKI. Konto musi spełniać następujące wymagania:

- Musi być użytkownikiem domeny i administratorem urządzenia, na którym jest zainstalowany Serwer administracyjny.
- Na urządzeniu z zainstalowanym Serwerem administracyjnym musi mieć nadane uprawnienie SeServiceLogonRight.

Aby utworzyć profil użytkownika na stałe, zaloguj się przynajmniej raz z poziomu skonfigurowanego konta użytkownika na urządzeniu, na którym znajduje się Serwer administracyjny. W repozytorium certyfikatów tego użytkownika na urządzeniu, na którym znajduje się Serwer administracyjny, zainstaluj certyfikat Agenta wycofywania, dostarczony przez administratorów domeny.

W celu skonfigurowania integracji z infrastrukturą kluczy publicznych:

1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.
2. W obszarze roboczym kliknij przycisk **Zintegruj z infrastrukturą klucza publicznego**, aby otworzyć sekcję **Integracja z PKI** okna **Reguły wydawania certyfikatu**.

   Zostanie otwarta sekcja **Integracja z PKI** okna **Reguły wydawania certyfikatu**.
3. Zaznacz pole **Zintegruj wystawianie certyfikatów z PKI**.
4. W polu **Konto** określ nazwę konta użytkownika używanego do integracji z infrastrukturą kluczy publicznych.
5. W polu **Hasło** wprowadź hasło domeny do konta.
6. Z listy **Nazwa szablonu certyfikatu w systemie PKI** wybierz szablon certyfikatu, który zostanie użyty do wydania certyfikatów użytkownikom domeny.

   Dedykowana usługa jest uruchamiana w Kaspersky Security Center z poziomu określonego konta użytkownika. Ta usługa jest odpowiedzialna za wydawanie certyfikatów dla domen dla użytkowników. Usługa jest uruchamiania, jeśli lista szablonów certyfikatów zostaje załadowana poprzez kliknięcie przycisku **Odśwież listę** lub po wygenerowaniu certyfikatu.
7. W celu zapisania ustawień kliknij **OK**.

Po przeprowadzeniu integracji certyfikaty są generowane automatycznie.

Włączanie obsługi Kerberos Constrained Delegation

Aplikacja obsługuje użycie Kerberos Constrained Delegation.

W celu włączenia obsługi Kerberos Constrained Delegation:

1. W drzewie konsoli otwórz folder **Zarządzanie urządzeniami mobilnymi**.
2. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**.
3. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.
4. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.
5. W oknie właściwości serwera iOS MDM wybierz sekcję **Ustawienia**.
6. W sekcji **Ustawienia** zaznacz pole **Zapewnij kompatybilność z Kerberos constrained delegation**.
7. Kliknij **OK**.

Dodawanie urządzeń mobilnych iOS do listy zarządzanych urządzeń

Aby dodać urządzenie mobilne iOS do listy zarządzanych urządzeń, współdzielony certyfikat musi zostać pobrany i zainstalowany na tym urządzeniu. Certyfikaty współdzielone są używane przez Serwer administracyjny do identyfikowania urządzeń mobilnych. Współdzielony certyfikat dla urządzenia mobilnego iOS jest dostarczany w obrębie profilu iOS MDM. Po dostarczeniu i zainstalowaniu współdzielonego certyfikatu na urządzeniu mobilnym, urządzenie pojawi się na liście zarządzanych urządzeń.

Kaspersky nie wspiera już Kaspersky Safe Browser.

Możesz dodać urządzenia mobilne użytkowników do listy zarządzanych urządzeń przy użyciu kreatora podłączania urządzenia mobilnego.

W celu połączenia urządzenia iOS z Serwerem administracyjnym przy użyciu certyfikatu współdzielonego:

1. Uruchom kreator podłączania urządzenia mobilnego w jeden z następujących sposobów:
   - Użyj menu kontekstowego z folderu **Konta użytkowników**:
     1. W drzewie konsoli rozwiń folder **Zaawansowane** i wybierz podfolder **Konta użytkowników**.
     2. W obszarze roboczym folderu **Konta użytkowników** wybierz użytkowników, grupy bezpieczeństwa lub grupy bezpieczeństwa Active Directory, dla których chcesz dodać urządzenia mobilne do listy zarządzanych urządzeń.

3. Kliknij prawym klawiszem myszy i z menu kontekstowego konta użytkownika wybierz **Dodaj urządzenie mobilne**.

   Zostanie uruchomiony kreator podłączania urządzenia mobilnego.

- W obszarze roboczym folderu **Urządzenia mobilne** kliknij przycisk **Dodaj urządzenie mobilne**.

  1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Urządzenia mobilne**.

  2. W obszarze roboczym podfolderu **Urządzenia mobilne** kliknij przycisk **Dodaj urządzenie mobilne**.

     Zostanie uruchomiony kreator podłączania urządzenia mobilnego.

2. W oknie **System operacyjny** kreatora, jako typ systemu operacyjnego wskaż **iOS**.

3. Na stronie **Wybieranie Serwera iOS MDM** wybierz serwer iOS MDM.

4. W oknie **Wybierz użytkowników, których urządzeniami mobilnymi chcesz zarządzać** wybierz użytkowników, grupy bezpieczeństwa lub grupy bezpieczeństwa Active Directory, których urządzenia mobilne chcesz dodać do listy zarządzanych urządzeń.

   Ten krok jest pomijany, jeśli uruchamiasz kreator, wybierając element **Dodaj urządzenie mobilne** w menu kontekstowym folderu **Konta użytkowników**.

   Jeśli chcesz dodać nowe konto użytkownika do listy, kliknij przycisk **Dodaj** i wprowadź właściwości konta użytkownika w otwartym oknie. Jeśli chcesz zmodyfikować lub przejrzeć właściwości konta użytkownika, wybierz konto użytkownika z listy i kliknij przycisk **Właściwości**.

5. W oknie **Źródło certyfikatu** określ metodę tworzenia współdzielonego certyfikatu, którego Serwer administracyjny użyje do identyfikacji urządzenia mobilnego. Certyfikat współdzielony można określić na jeden z następujących sposobów:

   - **Wystaw certyfikat przy użyciu narzędzi Serwera administracyjnego**

     Wybierz tę opcję, aby utworzyć nowy certyfikat przy użyciu narzędzi Serwera administracyjnego, jeśli wcześniej go nie utworzyłeś.

     Jeśli ta opcja jest zaznaczona, profil iOS MDM zostanie automatycznie podpisany przez certyfikat wygenerowany przez Serwer administracyjny.

     Opcja ta jest wybrana domyślnie.

   - **Określ plik certyfikatu**

     Wybierz tę opcję, aby określić plik certyfikatu, który został utworzony wcześniej.

     Ta metoda nie jest dostępna, jeśli w poprzednim kroku zaznaczono wielu użytkowników.

6. W oknie **Metoda powiadamiania użytkownika** zdefiniuj ustawienia powiadamiania użytkownika urządzenia mobilnego o utworzeniu certyfikatu za pośrednictwem wiadomości SMS lub wiadomości e-mail:

   - **Pokaż kod QR w kreatorze**

     Jeśli wybierzesz tę opcję, łącze do pakietu instalacyjnego zostanie wyświetlone w ostatnim kroku kreatora połączeń urządzenia mobilnego.

     > Ta opcja nie jest dostępna, jeśli dla połączenia urządzenia wybrano wielu użytkowników.

   - **Wyślij kod QR do użytkownika**

     Zaznaczając tę opcję, zezwalasz na skonfigurowanie powiadamiania użytkownika o podłączeniu nowego urządzenia mobilnego.

     Możesz wybrać typ adresu e-mail, określić dodatkowy adres e-mail oraz zmodyfikować treść wiadomości. Możesz również wybrać typ telefonu użytkownika dla wysyłania wiadomości SMS, określić dodatkowy numer telefonu oraz zmodyfikować treść wiadomości SMS.

     Jeśli Serwer SMTP nie został skonfigurowany, wiadomości e-mail nie będą mogły być wysyłane do użytkowników Jeśli powiadomienia SMS nie zostały skonfigurowane, wiadomości SMS nie będą mogły być wysyłane do użytkowników.

7. W oknie **Wynik** kliknij przycisk **Zakończ**, aby zakończyć działanie kreatora.

Profil iOS MDM jest automatycznie publikowany na Kaspersky Security Center Web Server. Użytkownik urządzenia mobilnego odbiera powiadomienie z odnośnikiem do pobrania profilu iOS MDM z Serwera sieciowego. Użytkownik klika odnośnik. System operacyjny urządzenia mobilnego wyświetli pytanie o zaakceptowanie instalacji profilu iOS MDM. Użytkownik musi wyrazić zgodę na zainstalowanie profilu iOS MDM przed pobraniem profilu iOS MDM na urządzenie mobilne. Po pobraniu profilu iOS MDM i zsynchronizowaniu urządzenia mobilnego z Serwerem administracyjnym, urządzenie zostanie wyświetlone w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli.

> Aby użytkownik mógł przejść na Kaspersky Security Center Web Server, korzystając z odnośnika, na urządzeniu mobilnym powinno być możliwe nawiązanie połączenia z Serwerem administracyjnym poprzez port 8061.

Dodawanie urządzeń mobilnych Android do listy zarządzanych urządzeń

Aby dodać urządzenie mobilne Android do listy zarządzanych urządzeń, Kaspersky Endpoint Security for Android i współdzielony certyfikat muszą zostać dostarczone i zainstalowane na urządzeniu mobilnym. Certyfikaty współdzielone są używane przez Serwer administracyjny do identyfikowania urządzeń mobilnych. Po dostarczeniu i zainstalowaniu współdzielonego certyfikatu na urządzeniu mobilnym, urządzenie pojawi się na liście zarządzanych urządzeń.

Możesz dodać urządzenia mobilne użytkowników do listy zarządzanych urządzeń przy użyciu kreatora podłączania urządzenia mobilnego. Kreator udostępnia dwie opcje dostarczenia i instalacji współdzielonego certyfikatu oraz Kaspersky Endpoint Security for Android:

- Przy użyciu odnośnika do Google Play
- Przy użyciu odnośnika z serwera sieci Web Kaspersky Security Center Web Server

  Pakiet instalacyjny Kaspersky Endpoint Security for Android przechowywany do dystrybucji na Serwerze administracyjnym jest używany do instalacji

Uruchamianie kreatora podłączania urządzenia mobilnego

W celu uruchomienia kreatora podłączania urządzenia mobilnego wykonaj jedną z następujących czynności:

- Użyj menu kontekstowego z folderu **Konta użytkowników**:

  1. W drzewie konsoli rozwiń folder **Zaawansowane** i wybierz podfolder **Konta użytkowników**.
  2. W obszarze roboczym folderu **Konta użytkowników** wybierz użytkowników, grupy bezpieczeństwa lub grupy bezpieczeństwa Active Directory, dla których chcesz dodać urządzenia mobilne do listy zarządzanych urządzeń.
  3. Kliknij prawym klawiszem myszy i z menu kontekstowego konta użytkownika wybierz **Dodaj urządzenie mobilne**.

     Zostanie uruchomiony kreator podłączania urządzenia mobilnego.

- W obszarze roboczym folderu **Urządzenia mobilne** kliknij przycisk **Dodaj urządzenie mobilne**.

  1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Urządzenia mobilne**.
  2. W obszarze roboczym podfolderu **Urządzenia mobilne** kliknij przycisk **Dodaj urządzenie mobilne**.

     Zostanie uruchomiony kreator podłączania urządzenia mobilnego.

Dodawanie urządzenia mobilnego Android przy użyciu odnośnika do Google Play

W celu zainstalowania Kaspersky Endpoint Security for Android i certyfikatu współdzielonego na urządzeniu mobilnym przy użyciu odnośnika do Google Play:

1. Uruchamianie kreatora podłączania urządzenia mobilnego.
2. W oknie **System operacyjny** kreatora, jako typ systemu operacyjnego urządzenia mobilnego wybierz **Android**.
3. W kroku **Metoda instalacji Kaspersky Endpoint Security dla systemu Android na urządzeniach** wybierz **Pobierz aplikację z Google Play**.
4. W oknie **Wybierz użytkowników, których urządzeniami mobilnymi chcesz zarządzać** wybierz użytkowników, grupy bezpieczeństwa lub grupy bezpieczeństwa Active Directory, dla których chcesz dodać urządzenia mobilne do listy zarządzanych urządzeń.

Ten krok jest pomijany, jeśli uruchamiasz kreator, wybierając element **Dodaj urządzenie mobilne** w menu kontekstowym folderu **Konta użytkowników**.

Jeśli chcesz dodać nowe konto użytkownika do listy, kliknij przycisk **Dodaj** i wprowadź właściwości konta użytkownika w otwartym oknie. Jeśli chcesz zmodyfikować lub przejrzeć właściwości konta użytkownika, wybierz konto użytkownika z listy i kliknij przycisk **Właściwości**.

5. W oknie **Źródło certyfikatu** określ metodę tworzenia współdzielonego certyfikatu, którego Serwer administracyjny użyje do identyfikacji urządzenia mobilnego. Certyfikat współdzielony można określić na jeden z następujących sposobów:

   - **Wystaw certyfikat przy użyciu narzędzi Serwera administracyjnego**

     Wybierz tę opcję, aby utworzyć nowy certyfikat przy użyciu narzędzi Serwera administracyjnego, jeśli wcześniej go nie utworzyłeś.

     Jeśli wybierzesz tę opcję, certyfikat zostanie automatycznie utworzony przy użyciu narzędzi Serwera administracyjnego.

     Opcja ta jest wybrana domyślnie.

   - **Określ plik certyfikatu**

     Wybierz tę opcję, aby określić plik certyfikatu, który został utworzony wcześniej.

     Ta metoda nie jest dostępna, jeśli w poprzednim kroku zaznaczono wielu użytkowników.

6. W oknie **Metoda powiadamiania użytkownika** zdefiniuj ustawienia powiadamiania użytkownika urządzenia mobilnego o utworzeniu certyfikatu za pośrednictwem wiadomości SMS lub wiadomości e-mail:

   - **Pokaż kod QR w kreatorze**

     Jeśli wybierzesz tę opcję, łącze do pakietu instalacyjnego zostanie wyświetlone w ostatnim kroku kreatora połączeń urządzenia mobilnego.

     Ta opcja nie jest dostępna, jeśli dla połączenia urządzenia wybrano wielu użytkowników.

   - **Wyślij kod QR do użytkownika**

     Zaznaczając tę opcję, zezwalasz na skonfigurowanie powiadamiania użytkownika o podłączeniu nowego urządzenia mobilnego.

     Możesz wybrać typ adresu e-mail, określić dodatkowy adres e-mail oraz zmodyfikować treść wiadomości. Możesz również wybrać typ telefonu użytkownika dla wysyłania wiadomości SMS, określić dodatkowy numer telefonu oraz zmodyfikować treść wiadomości SMS.

     Jeśli Serwer SMTP nie został skonfigurowany, wiadomości e-mail nie będą mogły być wysyłane do użytkowników Jeśli powiadomienia SMS nie zostały skonfigurowane, wiadomości SMS nie będą mogły być wysyłane do użytkowników.

7. W oknie **Wynik** kliknij przycisk **Zakończ**, aby zakończyć działanie kreatora.

Po zakończeniu działania kreatora, odnośnik oraz kod QR zostaną wysłane na urządzenie mobilne użytkownika, umożliwiając mu w ten sposób pobranie Kaspersky Endpoint Security for Android. Użytkownik klika odnośnik lub skanuje kod QR. System operacyjny urządzenia mobilnego wyświetli pytanie o zaakceptowanie instalacji Kaspersky Endpoint Security for Android. Po pobraniu i zainstalowaniu Kaspersky Endpoint Security for Android, urządzenie mobilne nawiązuje połączenie z Serwerem administracyjnym i pobiera współdzielony certyfikat. Po

zainstalowaniu certyfikatu na urządzeniu mobilnym, urządzenie zostanie wyświetlone w folderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli.

Dodawanie urządzenia mobilnego Android przy użyciu odnośnika z serwera sieci Web Kaspersky Security Center Web Server

Pakiet instalacyjny Kaspersky Endpoint Security for Android opublikowany na Serwerze administracyjnym zostanie użyty do instalacji.

W celu zainstalowania Kaspersky Endpoint Security for Android i certyfikatu współdzielonego na urządzeniu mobilnym przy użyciu odnośnika z serwera sieciowego:

1. Uruchamianie kreatora podłączania urządzenia mobilnego.
2. W oknie **System operacyjny** kreatora, jako typ systemu operacyjnego urządzenia mobilnego wybierz **Android**.
3. W kroku **Metoda instalacji Kaspersky Endpoint Security dla systemu Android na urządzeniach** wybierz **Pobierz pakiet instalacyjny aplikacji z Kaspersky Security Center**.

   W polu, które się pojawi, wybierz pakiet instalacyjny lub utwórz nowy, klikając **Nowy**.
4. W oknie **Wybierz użytkowników, których urządzeniami mobilnymi chcesz zarządzać** wybierz użytkowników, grupy bezpieczeństwa lub grupy bezpieczeństwa Active Directory, dla których chcesz dodać urządzenia mobilne do listy zarządzanych urządzeń.

   Ten krok jest pomijany, jeśli uruchamiasz kreator, wybierając element **Dodaj urządzenie mobilne** w menu kontekstowym folderu **Konta użytkowników**.

   Jeśli chcesz dodać nowe konto użytkownika do listy, kliknij przycisk **Dodaj** i wprowadź właściwości konta użytkownika w otwartym oknie. Jeśli chcesz zmodyfikować lub przejrzeć właściwości konta użytkownika, wybierz konto użytkownika z listy i kliknij przycisk **Właściwości**.
5. W oknie **Źródło certyfikatu** określ metodę tworzenia współdzielonego certyfikatu, którego Serwer administracyjny użyje do identyfikacji urządzenia mobilnego. Certyfikat współdzielony można określić na jeden z następujących sposobów:

   - **Wystaw certyfikat przy użyciu narzędzi Serwera administracyjnego**

     Wybierz tę opcję, aby utworzyć nowy certyfikat przy użyciu narzędzi Serwera administracyjnego, jeśli wcześniej go nie utworzyłeś.

     Jeśli wybierzesz tę opcję, certyfikat zostanie automatycznie utworzony przy użyciu narzędzi Serwera administracyjnego.

     Opcja ta jest wybrana domyślnie.

   - **Określ plik certyfikatu**

     Wybierz tę opcję, aby określić plik certyfikatu, który został utworzony wcześniej.

     Ta metoda nie jest dostępna, jeśli w poprzednim kroku zaznaczono wielu użytkowników.

6. W oknie **Metoda powiadamiania użytkownika** zdefiniuj ustawienia powiadamiania użytkownika urządzenia mobilnego o utworzeniu certyfikatu za pośrednictwem wiadomości SMS lub wiadomości e-mail:

   - **Pokaż kod QR w kreatorze**

     Jeśli wybierzesz tę opcję, łącze do pakietu instalacyjnego zostanie wyświetlone w ostatnim kroku kreatora połączeń urządzenia mobilnego.

     > Ta opcja nie jest dostępna, jeśli dla połączenia urządzenia wybrano wielu użytkowników.

   - **Wyślij kod QR do użytkownika**

     Zaznaczając tę opcję, zezwalasz na skonfigurowanie powiadamiania użytkownika o podłączeniu nowego urządzenia mobilnego.

     Możesz wybrać typ adresu e-mail, określić dodatkowy adres e-mail oraz zmodyfikować treść wiadomości. Możesz również wybrać typ telefonu użytkownika dla wysyłania wiadomości SMS, określić dodatkowy numer telefonu oraz zmodyfikować treść wiadomości SMS.

     Jeśli Serwer SMTP nie został skonfigurowany, wiadomości e-mail nie będą mogły być wysyłane do użytkowników Jeśli powiadomienia SMS nie zostały skonfigurowane, wiadomości SMS nie będą mogły być wysyłane do użytkowników.

7. W oknie **Wynik** kliknij przycisk **Zakończ**, aby zakończyć działanie kreatora.

Pakiet aplikacji mobilnej Kaspersky Endpoint Security for Android jest automatycznie publikowany na Kaspersky Security Center Web Server. Pakiet aplikacji mobilnej zawiera aplikację, ustawienia do łączenia urządzenia mobilnego z Serwerem administracyjnym, a także certyfikat. Użytkownik urządzenia mobilnego otrzymuje powiadomienie z odnośnikiem do pobrania pakietu z Serwera sieciowego. Użytkownik klika odnośnik. System operacyjny urządzenia wyświetla pytanie o zaakceptowanie instalacji pakietu aplikacji mobilnych. Jeśli użytkownik wyrazi zgodę, pakiet zostanie pobrany na urządzenie mobilne. Po pobraniu pakietu i zsynchronizowaniu urządzenia mobilnego z Serwerem administracyjnym, urządzenie zostanie wyświetlone w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli.

Zarządzanie urządzeniami iOS MDM

Ta sekcja opisuje zaawansowane funkcje zarządzania urządzeniami iOS MDM poprzez Kaspersky Security Center. Aplikacja obsługuje następujące funkcje zarządzania urządzeniami iOS MDM:

- Definiowanie ustawień zarządzanych urządzeń iOS MDM w trybie scentralizowanym i ograniczenie funkcji urządzeń przy użyciu profili konfiguracyjnych. Możesz dodać lub zmodyfikować profile konfiguracyjne, a także zainstalować je na urządzeniach mobilnych.

- Instalowanie aplikacji na urządzeniach mobilnych przy użyciu profili informacyjnych, omijając App Store. Na przykład możesz użyć profili informacyjnych do zainstalowania aplikacji firmowych na urządzeniach mobilnych użytkowników. Profil informacyjny zawiera informacje o aplikacji i urządzeniu mobilnym.

- Instalowanie aplikacji na urządzeniu iOS MDM poprzez App Store. Przed zainstalowaniem aplikacji na urządzeniu iOS MDM powinieneś dodać tę aplikację do serwera iOS MDM.

Co 24 godziny na wszystkie podłączone urządzenia mobilne iOS MDM wysyłane jest powiadomienie push w celu zsynchronizowania danych z serwerem iOS MDM.

Informacje o profilu konfiguracyjnym i profilu informacyjnym oraz aplikacjach zainstalowanych na urządzeniu z iOS MDM znajdziesz w oknie właściwości urządzenia.

Podpisywanie profilu iOS MDM za pomocą certyfikatu

Profil iOS MDM można podpisać za pomocą certyfikatu. Możesz użyć certyfikatu, który sam wystawiłeś, lub możesz otrzymać certyfikat od zaufanych urzędów certyfikacji.

Urządzenia z systemem iOS wyświetlają zastrzeżenie dotyczące niepodpisanych profili i monitują użytkownika o zaufanie osobie podpisującej podczas instalowania profilu.

W celu podpisania certyfikatu dla profilu iOS MDM:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.
2. Z otwartego menu kontekstowego folderu **Urządzenia mobilne** wybierz **Właściwości**.
3. W oknie właściwości folderu wybierz sekcję **Ustawienia połączenia dla urządzeń iOS**.
4. Kliknij przycisk **Przeglądaj** znajdujący się pod polem **Wybierz plik certyfikatu**.
   Okno **Certyfikat**.
5. W polu **Typ certyfikatu** określ typ certyfikatu - publiczny lub prywatny:
   - Jeśli wybrana jest wartość **Kontener PKCS #12**, określ plik certyfikatu i hasło.
   - Jeśli wybrana jest wartość **Certyfikat X.509**:
     a. Określ plik klucza prywatnego (z rozszerzeniem *.prk lub *.pem).
     b. Określ hasło dla klucza prywatnego.
     c. Określ plik klucza publicznego (z rozszerzeniem *.cer).
6. Kliknij **OK**.

Profil iOS MDM jest podpisany za pomocą certyfikatu.

Dodawanie profilu konfiguracyjnego

Aby utworzyć profil konfiguracyjny, możesz użyć programu Apple Configurator 2, który jest dostępny na stronie Apple Inc. Apple Configurator 2 działa tylko na urządzeniach z systemem macOS; jeśli nie masz do dyspozycji takich urządzeń, możesz zamiast tego użyć narzędzia iPhone Configuration Utility na urządzeniu z zainstalowaną Konsolą administracyjną. Jednak firma Apple Inc. nie obsługuje już programu iPhone Configuration Utility.

W celu utworzenia profilu konfiguracyjnego przy użyciu iPhone Configuration Utility i dodania go do serwera iOS MDM:

1. W drzewie konsoli wybierz folder **Zarządzanie urządzeniami mobilnymi**.
2. W obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** wybierz podfolder **Serwery urządzeń mobilnych**.

3. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.

4. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera urządzeń mobilnych.

5. W oknie właściwości serwera iOS MDM wybierz sekcję **Profile konfiguracyjne**.

6. W sekcji **Profile konfiguracyjne** kliknij przycisk **Utwórz**.

   Zostanie otwarte okno **Nowy profil konfiguracyjny**.

7. W oknie **Nowy profil konfiguracyjny** określ nazwę i numer ID profilu.

   Numer ID profilu konfiguracyjnego powinien być unikatowy; wartość powinna być określona w formacie Reverse-DNS (odwrotna translacja adresów DNS), na przykład: *com.companyname.identifier*.

8. Kliknij **OK**.

   Następnie zostanie uruchomione narzędzie iPhone Configuration Utility (jeśli jest zainstalowane).

9. Skonfiguruj ponownie profil konfiguracyjny w iPhone Configuration Utility.

   Opis ustawień profilu oraz instrukcje dotyczące sposobu konfiguracji profilu można znaleźć w dokumentacji załączonej do narzędzia iPhone Configuration Utility.

Po skonfigurowaniu profilu przy pomocy narzędzia iPhone Configuration Utility, nowy profil konfiguracyjny zostanie wyświetlony w sekcji **Profile konfiguracyjne**, w oknie właściwości serwera iOS MDM.

Kliknij przycisk **Modyfikuj**, aby zmodyfikować profil konfiguracyjny.

Kliknij przycisk **Importuj**, aby wczytać profil konfiguracyjny do programu.

Kliknij przycisk **Eksportuj**, aby zapisać profil konfiguracyjny do pliku.

Utworzony profil musi zostać zainstalowany na urządzeniach iOS MDM.

Instalowanie profilu konfiguracyjnego na urządzeniu

W celu zainstalowania profilu konfiguracyjnego na urządzeniu mobilnym:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM według typu protokołu (*iOS MDM*).

3. Wybierz urządzenie mobilne użytkownika, na którym chcesz zainstalować profil konfiguracyjny.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego zainstalowania profilu.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Zainstaluj profil** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z jego menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Zainstaluj profil**.

Zostanie otwarte okno **Wybierz profile** wyświetlające listę profili. Wybierz z listy profil, który chcesz zainstalować na urządzeniu mobilnym. Możesz wybrać kilka profili do jednoczesnego zainstalowania na urządzeniu mobilnym. Aby wybrać kilka profili, użyj klawisza **Shift**. Aby wybrać grupę profili, użyj klawisza **CTRL**.

6. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

   Po wykonaniu polecenia, wybrany profil konfiguracyjny zostanie zainstalowany na urządzeniu mobilnym użytkownika. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia w raporcie poleceń zostanie wyświetlony jako *Gotowe*.

   Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

   Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

   Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

7. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Zainstalowany profil możesz sprawdzić i usunąć, jeśli jest to konieczne.

Usuwanie profilu konfiguracyjnego z urządzenia

W celu usunięcia profilu konfiguracyjnego z urządzenia mobilnego:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM, klikając odnośnik **iOS MDM**.

3. Wybierz urządzenie mobilne użytkownika, z którego chcesz usunąć profil konfiguracyjny.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego usunięcia profilu.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Usuń profil** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Usuń profil**.

   Zostanie otwarte okno **Usuń profile** wyświetlające listę profili.

6. Wybierz z listy profil, który chcesz usunąć z urządzenia mobilnego. Możesz wybrać kilka profili do jednoczesnego usunięcia z urządzenia mobilnego. Aby wybrać kilka profili, użyj klawisza **Shift**. Aby wybrać grupę profili, użyj klawisza **CTRL**.

7. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

   Po wykonaniu polecenia, wybrany profil konfiguracyjny zostanie usunięty z urządzenia mobilnego użytkownika. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia zostanie wyświetlony jako *Zakończone*.

   Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

   Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

8. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Dodanie nowego urządzenia poprzez opublikowanie odnośnika do profilu

W Konsoli administracyjnej administrator tworzy nowy profil iOS MDM za pomocą Kreatora instalacji certyfikatów. Kreator wykonuje następujące działania:

- Profil iOS MDM jest automatycznie publikowany na serwerze sieciowym.
- Do użytkownika zostaje wysłany odnośnik do profilu iOS MDM w wiadomości SMS lub e-mail. Po odebraniu wiadomości z odsyłaczem, użytkownik instaluje profil iOS MDM na urządzeniu mobilnym.
- Urządzenie mobilne łączy się z serwerem iOS MDM.

Ze względu na zaostrzoną politykę bezpieczeństwa, wprowadzoną przez firmę Apple, należy skonfigurować wersje protokołów TLS 1.1 i TLS 1.2 podczas łączenia urządzenia mobilnego działającego pod kontrolą systemu iOS 11 z Serwerem administracyjnym, na którym włączono integrację z Infrastrukturą klucza publicznego (PKI).

Dodanie nowego urządzenia mobilnego poprzez zainstalowanie profilu przez administratora

W celu połączenia urządzenia mobilnego z serwerem iOS MDM poprzez zainstalowanie profilu iOS MDM na tym urządzeniu mobilnym, administrator musi wykonać następujące czynności:

1. W Konsoli administracyjnej otwórz Kreator instalacji certyfikatu.
2. Utwórz nowy profil iOS MDM, zaznaczając pole wyboru **Pokaż certyfikat po zakończeniu działania kreatora**.
3. Zapisać profil iOS MDM.
4. Zainstalować profil iOS MDM na urządzeniu mobilnym użytkownika przy pomocy narzędzia Apple Configurator.

   Urządzenie mobilne łączy się z serwerem iOS MDM.

Ze względu na zaostrzoną politykę bezpieczeństwa, wprowadzoną przez firmę Apple, należy skonfigurować wersje protokołów TLS 1.1 i TLS 1.2 podczas łączenia urządzenia mobilnego działającego pod kontrolą systemu iOS 11 z Serwerem administracyjnym, na którym włączono integrację z Infrastrukturą klucza publicznego (PKI).

Dodawanie profilu informacyjnego

W celu dodania profilu informacyjnego do serwera iOS MDM:

1. W drzewie konsoli otwórz folder **Zarządzanie urządzeniami mobilnymi**.
2. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**.
3. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.
4. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera urządzeń mobilnych.
5. W oknie właściwości **serwera iOS MDM** przejdź do sekcji **Profile informacyjne**.
6. W sekcji **Profile informacyjne** kliknij przycisk **Importuj** i określ ścieżkę dostępu do pliku profilu informacyjnego.

Profil zostanie dodany do ustawień serwera iOS MDM.

Kliknij przycisk **Eksportuj**, aby zapisać listę profili informacyjnych do pliku.

Możesz zainstalować profil informacyjny, który zaimportowałeś na urządzenia iOS MDM.

Instalowanie profilu informacyjnego na urządzeniu

W celu zainstalowania profilu informacyjnego na urządzeniu mobilnym:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.
2. W obszarze roboczym przefiltruj urządzenia iOS MDM według typu protokołu (*iOS MDM*).
3. Wybierz urządzenie mobilne użytkownika, na którym chcesz zainstalować profil informacyjny.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego zainstalowania profilu informacyjnego.
4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.
5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Instalowanie profilu informacyjnego** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z jego menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Zainstaluj profil informacyjny**.

   Zostanie otwarte okno **Wybierz profile informacyjne** wyświetlające listę profili informacyjnych. Wybierz z listy profil informacyjny, który chcesz zainstalować na urządzeniu mobilnym. Możesz wybrać kilka profili informacyjnych do jednoczesnego zainstalowania ich na urządzeniu mobilnym. Aby wybrać kilka profili informacyjnych, użyj klawisza **Shift**. Aby wybrać grupę profili informacyjnych, użyj klawisza **Ctrl**.
6. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

Po wykonaniu polecenia, wybrany profil informacyjnych zostanie zainstalowany na urządzeniu mobilnym użytkownika. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia w raporcie poleceń jest wyświetlony jako *Zakończone*.

Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

7. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Zainstalowany profil możesz sprawdzić i usunąć, jeśli jest to konieczne.

Usuwanie profilu informacyjnego z urządzenia

W celu usunięcia profilu informacyjnego z urządzenia mobilnego:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM według typu protokołu (*iOS MDM*).

3. Wybierz urządzenie mobilne użytkownika, z którego chcesz usunąć profil informacyjny.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego usunięcia profilu informacyjnego.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Usuń profil informacyjny** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Usuń profil informacyjny**.

   Zostanie otwarte okno **Usuń profile informacyjne** wyświetlające listę profili.

6. Wybierz z listy profil informacyjny, który chcesz usunąć z urządzenia mobilnego. Możesz wybrać kilka profili informacyjnych do jednoczesnego usunięcia z urządzenia mobilnego. Aby wybrać kilka profili informacyjnych, użyj klawisza **Shift**. Aby wybrać grupę profili informacyjnych, użyj klawisza **Ctrl**.

7. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

   Po wykonaniu polecenia, wybrany profil informacyjny zostanie usunięty z urządzenia mobilnego użytkownika. Aplikacje skojarzone z usuniętym profilem informacyjnym nie będą działać. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia zostanie wyświetlony jako *Zakończone*.

   Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

   Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

   Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

8. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Dodawanie zarządzanej aplikacji

Przed zainstalowaniem aplikacji na urządzeniu iOS MDM powinieneś dodać tę aplikację do serwera iOS MDM. Aplikacja jest postrzegana jako zarządzana, jeśli została zainstalowana na urządzeniu poprzez Kaspersky Security Center. Zarządzana aplikacja może być zarządzana ręcznie poprzez Kaspersky Security Center.

W celu dodania zarządzanej aplikacji do serwera iOS MDM:

1. W drzewie konsoli otwórz folder **Zarządzanie urządzeniami mobilnymi**.
2. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**.
3. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.
4. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera iOS MDM.
5. W oknie właściwości serwera iOS MDM wybierz sekcję **Zarządzane aplikacje**.
6. W sekcji **Zarządzane aplikacje** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Dodaj aplikację**.
7. W oknie **Dodaj aplikację**, w polu **Nazwa aplikacji** określ nazwę dodawanej aplikacji.
8. W polu **Apple ID lub odnośnik do pliku manifestu** określ Apple ID dodawanej aplikacji lub określ odnośnik do pliku manifestu, który może być używany do pobrania aplikacji.
9. Jeśli chcesz, aby zarządzana aplikacja została usunięta z urządzenia mobilnego użytkownika wraz z profilem iOS MDM, zaznacz pole **Usuń wraz z profilem iOS MDM**.
10. Jeśli chcesz zablokować tworzenie kopii zapasowej danych aplikacji poprzez iTunes, zaznacz pole **Zablokuj kopię zapasową danych**.
11. Kliknij **OK**.

Dodana aplikacja będzie wyświetlana w sekcji **Zarządzane aplikacje** okna właściwości serwera iOS MDM.

Instalowanie aplikacji na urządzeniu mobilnym

W celu zainstalowania aplikacji na urządzeniu mobilnym iOS MDM:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.
2. Wybierz urządzenie iOS MDM, na którym chcesz zainstalować aplikację.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego zainstalowania aplikacji.
3. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

4. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Zainstaluj aplikację** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z jego menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Zainstaluj aplikację**.

   Zostanie otwarte okno **Wybierz aplikacje** wyświetlające listę profili. Wybierz z listy aplikację, którą chcesz zainstalować na urządzeniu mobilnym. Możesz wybrać kilka aplikacji do jednoczesnego zainstalowania na urządzeniu mobilnym. Aby wybrać kilka aplikacji, użyj klawisza **Shift**. Aby wybrać grupę aplikacji, użyj klawisza **Ctrl**.

5. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

   Po wykonaniu polecenia, wybrana aplikacja zostanie zainstalowana na urządzeniu mobilnym użytkownika. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia w raporcie poleceń zostanie wyświetlony jako *Zakończone*.

   Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika. Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

   Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

6. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Informacje o zainstalowaniu aplikacji są wyświetlane we właściwościach urządzenia mobilnego iOS MDM. Możesz usunąć aplikację z urządzenia mobilnego, korzystając z raportu poleceń lub menu kontekstowego urządzenia mobilnego.

Usuwanie aplikacji z urządzenia

W celu usunięcia aplikacji z urządzenia mobilnego:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM według typu protokołu (*iOS MDM*).

3. Wybierz urządzenie mobilne użytkownika, z którego chcesz usunąć aplikację.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego usunięcia aplikacji.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Usuń aplikację** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z jego menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Usuń aplikację**.

   Zostanie otwarte okno **Usuń aplikacje** wyświetlające listę aplikacji.

6. Wybierz z listy aplikację, którą chcesz usunąć z urządzenia mobilnego. Możesz wybrać kilka aplikacji do ich jednoczesnego usunięcia. Aby wybrać kilka aplikacji, użyj klawisza **Shift**. Aby wybrać grupę aplikacji, użyj klawisza **Ctrl**.

7. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

   Po wykonaniu polecenia, wybrana aplikacja zostanie usunięta z urządzenia mobilnego użytkownika. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia zostanie wyświetlony jako *Zakończone*.

Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

8. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Konfigurowanie roamingu na urządzeniu mobilnym iOS MDM

W celu skonfigurowania roamingu:

1. W drzewie konsoli otwórz folder **Zarządzanie urządzeniami mobilnymi**.
2. W folderze **Zarządzanie urządzeniami mobilnymi** wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.
3. Wybierz urządzenie iOS MDM należące do użytkownika, dla którego chcesz skonfigurować roaming.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego skonfigurowania na nich roamingu.
4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.
5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Konfiguruj roaming** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z menu kontekstowego elementu **Wszystkie polecenia → Konfiguruj roaming**.
6. W oknie **Ustawienia roamingu** określ odpowiednie ustawienia:

   - **Włącz roaming danych**

     Jeśli ta opcja jest włączona, na urządzeniach mobilnych iOS MDM zostanie włączony roaming danych. Użytkownik urządzenia mobilnego iOS MDM może przeglądać internet w strefie roamingu.

     Domyślnie opcja ta jest wyłączona.

Roaming zostanie skonfigurowany dla wybranych urządzeń.

Przeglądanie informacji o urządzeniu iOS MDM

W celu przejrzenia informacji o urządzeniu iOS MDM:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.
2. W obszarze roboczym przefiltruj urządzenia iOS MDM, klikając odnośnik **iOS MDM**.
3. Wybierz urządzenie mobilne, dla którego chcesz wyświetlić informacje.

4. Z menu kontekstowego urządzenia przenośnego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości urządzenia iOS MDM.

Okno właściwości urządzenia mobilnego wyświetla informacje o podłączonym urządzeniu iOS MDM.

Odłączanie urządzenia iOS MDM od funkcji zarządzania

W celu odłączenia urządzenia iOS MDM od serwera iOS MDM:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM, klikając odnośnik **iOS MDM**.

3. Wybierz urządzenie mobilne, które chcesz odłączyć.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Usuń**.

   Urządzenie iOS MDM zostanie oznaczone na liście jako obiekt do usunięcia. Urządzenie mobilne zostanie automatycznie usunięte z listy zarządzanych urządzeń po jego wcześniejszym usunięciu z bazy danych serwera iOS MDM. Urządzenie mobilne zostanie usunięte z bazy danych serwera iOS MDM w ciągu jednej minuty.

Po odłączeniu urządzenia iOS MDM od funkcji zarządzania, wszystkie zainstalowane profile konfiguracyjne, profil iOS MDM oraz aplikacje, dla których włączono opcję **Usuń wraz z profilem iOS MDM**, zostaną usunięte z urządzenia mobilnego.

Wysyłanie poleceń na urządzenie

W celu wysłania polecenia na urządzenie iOS MDM:

1. W Konsoli administracyjnej otwórz węzeł **Zarządzanie urządzeniami mobilnymi**.

2. Wybierz folder **Urządzenia mobilne**.

3. W folderze **Urządzenia mobilne** wybierz urządzenie mobilne, na które mają zostać wysłane polecenia.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

5. Z wyświetlonej listy wybrać polecenie, które ma zostać wysłane na urządzenie mobilne.

Sprawdzanie stanu wykonania wysłanych poleceń

W celu sprawdzenia stanu wykonania polecenia, które zostało wysłane na urządzenie mobilne:

1. W Konsoli administracyjnej otwórz węzeł **Zarządzanie urządzeniami mobilnymi**.

2. Wybierz folder **Urządzenia mobilne**.

3. W folderze **Urządzenia mobilne** wybierz urządzenie mobilne, na którym ma być sprawdzony stan wykonania wybranych poleceń.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

Zarządzanie urządzeniami KES

W Kaspersky Security Center możesz zarządzać urządzeniami mobilnymi KES na następujące sposoby:

- Zarządzać urządzeniami KES w sposób scentralizowany przy pomocy poleceń.
- Przeglądać informacje dotyczące ustawień zarządzania urządzeniami KES.
- Instalować aplikacje przy użyciu pakietów aplikacji mobilnych.
- Odłączać urządzenia KES od funkcji zarządzania.

Tworzenie pakietów aplikacji mobilnych dla urządzeń KES

Aby możliwe było utworzenie pakietu aplikacji mobilnej dla urządzeń KES, niezbędna jest licencja Kaspersky Endpoint Security for Android.

W celu utworzenia pakietu aplikacji mobilnych:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.

   Domyślnie folder **Zdalna instalacja** to podfolder folderu **Zaawansowane**.

2. Kliknij przycisk **Akcje dodatkowe** i z listy rozwijalnej wybierz **Zarządzaj pakietami aplikacji mobilnych**.

3. W oknie **Zarządzanie pakietami aplikacji mobilnych** kliknij przycisk **Nowy**.

4. Zostanie uruchomiony Kreator tworzenia nowego pakietu. Postępuj zgodnie z instrukcjami kreatora.

Nowo utworzony pakiet aplikacji mobilnych jest wyświetlany w oknie **Zarządzanie pakietami aplikacji mobilnych**.

Włączanie uwierzytelniania opartego na certyfikatach urządzeń KES

Aby włączyć uwierzytelnianie oparte na certyfikacie urządzenia KES:

1. Otwórz rejestr systemu urządzenia klienckiego, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).

2. Przejdź do gałęzi:

   - W systemach 32-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

- W systemach 64-bitowych:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. Utwórz klucz o nazwie LP_MobileMustUseTwoWayAuthOnPort13292.
4. Jako typ klucza określ REG_DWORD.
5. Dla klucza wskaż wartość 1.
6. Uruchom ponownie usługę Serwera administracyjnego.

Obowiązkowe uwierzytelnianie oparte na certyfikacie urządzenia KES przy użyciu współdzielonego certyfikatu zostanie włączone po uruchomieniu usługi Serwera administracyjnego.

Pierwsze nawiązanie połączenia między urządzeniem KES i Serwerem administracyjnym nie wymaga certyfikatu.

Domyślnie uwierzytelnianie oparte na certyfikatach urządzeń KES jest wyłączone.

Przeglądanie informacji o urządzeniu KES

W celu przejrzenia informacji o urządzeniu KES:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.
   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.
2. W obszarze roboczym przefiltruj urządzenia KES według typu protokołu (*KES*).
3. Wybierz urządzenie mobilne, dla którego chcesz wyświetlić informacje.
4. Z menu kontekstowego urządzenia przenośnego wybierz **Właściwości**.

Zostanie otwarte okno właściwości urządzenia KES.

Okno właściwości urządzenia mobilnego wyświetla informacje o podłączonym urządzeniu KES.

Odłączanie urządzenia KES od funkcji zarządzania

Aby odłączyć urządzenie KES od funkcji zarządzania, użytkownik musi usunąć Agenta sieciowego z urządzenia mobilnego. Po usunięciu Agenta sieciowego, szczegóły urządzenia mobilnego zostaną usunięte z bazy danych Serwera administracyjnego, a administrator będzie mógł usunąć urządzenie mobilne z listy zarządzanych urządzeń.

W celu usunięcia urządzenia KES z listy zarządzanych urządzeń:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.
   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.
2. W obszarze roboczym przefiltruj urządzenia KES według typu protokołu (*KES*).

3. Wybierz urządzenie mobilne, które chcesz odłączyć od funkcji zarządzania.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Usuń**.

Urządzenie mobilne zostanie usunięte z listy zarządzanych urządzeń.

Jeśli program Kaspersky Endpoint Security for Android nie został usunięty z urządzenia mobilnego, po synchronizacji z Serwerem administracyjnym to urządzenie mobilne ponownie pojawi się na liście zarządzanych urządzeń.

Szyfrowanie i ochrona danych

Szyfrowanie danych zmniejsza ryzyko przypadkowego wycieku danych w sytuacji, gdy notebook, nośnik wymienny lub dysk twardy zostanie skradziony lub zgubiony, bądź też, gdy dostęp do danych uzyskują nieautoryzowani użytkownicy lub aplikacje.

Kaspersky Endpoint Security for Windows oferuje funkcję szyfrowania. Kaspersky Endpoint Security for Windows umożliwia szyfrowanie plików przechowywanych na dyskach lokalnych urządzeń i nośnikach wymiennych, a także całych nośników wymiennych i dysków twardych.

Reguły szyfrowania są konfigurowane przy użyciu Kaspersky Security Center, poprzez zasady. Zgodnie z określonymi regułami, szyfrowanie i deszyfrowanie jest wykonywane po zastosowaniu zasady.

Dostępność funkcji zarządzania szyfrowaniem jest określana przez ustawienia interfejsu.

Administrator może wykonywać następujące akcje:

- Konfigurować i przeprowadzać szyfrowanie lub deszyfrowanie plików na dyskach lokalnych urządzenia.
- Konfigurować oraz przeprowadzać szyfrowanie plików na nośnikach wymiennych.
- Tworzyć reguły dostępu aplikacji do zaszyfrowanych plików.
- Tworzyć i przekazywać użytkownikowi plik klucza dostępu do zaszyfrowanych plików, jeśli funkcja szyfrowania pliku posiada ograniczenia na urządzeniu użytkownika.
- Konfigurować i wykonywać szyfrowanie dysku twardego.
- Zarządzać dostępem użytkownika do zaszyfrowanych dysków twardych i nośników wymiennych (zarządzać kontami Agenta autoryzacji, tworzyć i dostarczać użytkownikom informacje dotyczące przywrócenia nazwy konta i hasła, a także klucze dostępu do zaszyfrowanych urządzeń).
- Wyświetlać stany szyfrowania i raporty dotyczące szyfrowania plików.

Działania te są wykonywane przy użyciu narzędzi zintegrowanych z Kaspersky Endpoint Security for Windows. Szczegółowe instrukcje dotyczące wykonywania działań oraz opis funkcji szyfrowania są dostępne w internetowym systemie pomocy dla Kaspersky Endpoint Security for Windows.

Kaspersky Security Center obsługuje funkcjonalność zarządzania szyfrowaniem dla urządzeń z systemem operacyjnym macOS. Szyfrowanie jest konfigurowane przy użyciu narzędzi Kaspersky Endpoint Security for Mac dla tych wersji aplikacji, które obsługują funkcję szyfrowania. Szczegółowe instrukcje dotyczące wykonywania operacji oraz opis funkcji szyfrowania można znaleźć w Podręczniku administratora *Kaspersky Endpoint Security for Mac*.

Przeglądanie listy zaszyfrowanych urządzeń

W celu przejrzenia listy urządzeń, na których przechowywane są zaszyfrowane informacje:

1. Z drzewa konsoli Serwera administracyjnego wybierz folder **Ochrona i szyfrowanie danych**.
2. Otwórz listę zaszyfrowanych urządzeń przy użyciu jednej z następujących metod:
   - Klikając odnośnik **Przejdź do listy zaszyfrowanych dysków** w sekcji **Zarządzanie zaszyfrowanymi dyskami**.
   - Wybierając folder **Zaszyfrowane dyski** w drzewie konsoli.

W obszarze roboczym zostaną wyświetlone informacje o urządzeniach w sieci, na których przechowywane są zaszyfrowane pliki, oraz o urządzeniach zaszyfrowanych na poziomie dysku. Po odszyfrowaniu informacji na urządzeniu, urządzenie jest automatycznie usuwane z listy.

Informacje przedstawione na liście urządzeń mogą być sortowane (rosnąco lub malejąco) według dowolnej kolumny.

Ustawienia interfejsu użytkownika określają, czy folder **Ochrona i szyfrowanie danych** jest wyświetlany w drzewie konsoli.

Wyświetlanie listy zdarzeń szyfrowania

Podczas wykonywania zadań szyfrowania lub deszyfrowania danych na urządzeniach, Kaspersky Endpoint Security for Windows wysyła do Kaspersky Security Center informacje o zdarzeniach następujących typów:

- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na brak wolnego miejsca na dysku.
- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na problemy z licencją.
- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na brak uprawnień dostępu.
- Dla aplikacji zablokowano dostęp do zaszyfrowanego pliku.
- Nieznane błędy.

W celu wyświetlenia listy zdarzeń, które wystąpiły w trakcie szyfrowania danych na urządzeniach:

1. Z drzewa konsoli Serwera administracyjnego wybierz folder **Ochrona i szyfrowanie danych**.
2. Przejdź do listy zdarzeń występujących podczas szyfrowania, korzystając z jednej z następujących metod:
   - Klikając odnośnik **Przejdź do listy błędów** w sekcji **Błędy szyfrowania danych**.
   - Wybierając folder **Zaszyfrowane dyski** w drzewie konsoli.

W obszarze roboczym zostaną wyświetlone informacje o problemach, które wystąpiły podczas szyfrowania danych na urządzeniach.

Na liście zdarzeń szyfrowania można wykonywać następujące działania:

- Sortować dane w dowolnej kolumnie rosnąco lub malejąco.
- Wykonywać szybkie wyszukiwanie wpisów (przez dopasowanie tekstu podciągiem znaków w dowolnym polu listy).
- Eksportować listę zdarzeń do pliku tekstowego.

Ustawienia interfejsu użytkownika określają, czy folder **Ochrona i szyfrowanie danych** jest wyświetlany w drzewie konsoli.

Eksportowanie listy zdarzeń szyfrowania do pliku tekstowego

W celu wyeksportowania listy zdarzeń szyfrowania do pliku tekstowego:

1. Utwórz listę zdarzeń szyfrowania.
2. Z menu kontekstowego listy zdarzeń wybierz **Eksportuj listę**.

   Zostanie otwarte okno **Eksportuj listę**.
3. W oknie **Eksportuj listę** określ nazwę pliku tekstowego z listą zdarzeń, wybierz folder zapisu i kliknij przycisk **Zapisz**.

   Lista zdarzeń szyfrowania zostanie zapisana w określonym pliku.

Tworzenie i przeglądanie raportów z szyfrowania

Możesz wygenerować następujące raporty:

- Raport o stanie szyfrowania zarządzanych urządzeń. Ten raport zawiera szczegółowe informacje na temat szyfrowania danych na różnych zarządzanych urządzeniach. Na przykład raport pokazuje liczbę urządzeń, do których ma zastosowanie zasada ze skonfigurowanymi regułami szyfrowania. Możesz także dowiedzieć się, na przykład, ile urządzeń wymaga ponownego uruchomienia. Raport zawiera również informacje o technologii i algorytmie szyfrowania dla każdego urządzenia.

- Raport o stanie szyfrowania urządzeń pamięci masowej. Ten raport zawiera podobne informacje jak raport o stanie szyfrowania zarządzanych urządzeń, ale zawiera dane tylko dla urządzeń pamięci masowej i dysków wymiennych.

- Raport o prawach dostępu do zaszyfrowanych dysków. Ten raport pokazuje, które konta użytkowników mają dostęp do zaszyfrowanych dysków.

- Raport o błędach podczas szyfrowania plików. Ten raport zawiera informacje o błędach, które wystąpiły podczas uruchamiania zadań szyfrowania lub odszyfrowywania danych na urządzeniach.

- Raport o zablokowanym dostępie do zaszyfrowanych plików. Ten raport zawiera informacje o blokowaniu dostępu aplikacji do zaszyfrowanych plików. Ten raport jest pomocny, jeśli nieautoryzowany użytkownik lub aplikacja próbuje uzyskać dostęp do zaszyfrowanych plików lub dysków.

W celu wygenerowania raportu dotyczącego szyfrowania urządzeń:

1. Z drzewa konsoli wybierz folder **Ochrona i szyfrowanie danych**.

2. Wykonaj jedną z poniższych czynności:

   - Aby wygenerować raport dotyczący stanu szyfrowania zarządzanych urządzeń, kliknij odnośnik **Wyświetl raport o szyfrowaniu urządzeń pamięci masowej**.

     Jeśli jeszcze nie skonfigurowano tego raportu, zostanie uruchomiony Kreator tworzenia nowego szablonu raportu. Postępuj zgodnie z krokami kreatora.

   - Aby wygenerować raport dotyczący stanu szyfrowania urządzeń pamięci masowej, w drzewie konsoli wybierz podfolder **Zaszyfrowane dyski**, a następnie kliknij przycisk **Wyświetl raport o szyfrowaniu urządzeń pamięci masowej**.

Zostanie rozpoczęte tworzenie raportu. Raport pojawi się na zakładce **Raporty** węzła **Serwer administracyjny**.

W celu wygenerowania raportu o uprawnieniach dostępu do zaszyfrowanych urządzeń:

1. Z drzewa konsoli wybierz folder **Ochrona i szyfrowanie danych**.
2. Wykonaj jedną z poniższych czynności:
   - Kliknij odnośnik **Raport o prawach dostępu do zaszyfrowanych dysków** w sekcji **Zarządzanie zaszyfrowanymi dyskami**, aby uruchomić Kreator tworzenia nowego szablonu raportu.
   - Wybierz podfolder **Zaszyfrowane dyski**, a następnie kliknij przycisk **Raport o prawach dostępu do zaszyfrowanych dysków**, aby uruchomić Kreator tworzenia nowego szablonu raportu.
3. Postępuj zgodnie z instrukcjami kreatora tworzenia nowego szablonu raportu.

Zostanie rozpoczęte tworzenie raportu. Raport pojawi się na zakładce **Raporty** węzła **Serwer administracyjny**.

W celu wygenerowania raportu o błędach szyfrowania plików:

1. Z drzewa konsoli wybierz folder **Ochrona i szyfrowanie danych**.
2. Wykonaj jedną z poniższych czynności:
   - Kliknij odnośnik **Wyświetl raport o błędach podczas szyfrowania plików,** dostępny w sekcji **Błędy szyfrowania danych**, aby uruchomić Kreator tworzenia nowego szablonu raportu.
   - Wybierz podfolder **Zdarzenia szyfrowania**, a następnie kliknij odnośnik **Raport o błędach szyfrowania plików**, aby uruchomić Kreator tworzenia nowego szablonu raportu.
3. Postępuj zgodnie z instrukcjami kreatora tworzenia nowego szablonu raportu.

Zostanie rozpoczęte tworzenie raportu. Raport pojawi się na zakładce **Raporty** węzła **Serwer administracyjny**.

W celu wygenerowania raportu o stanie szyfrowania zarządzanych urządzeń:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Kliknij przycisk **Nowy szablon raportu**, aby uruchomić Kreator tworzenia nowego szablonu raportu.
4. Postępuj zgodnie z instrukcjami kreatora tworzenia nowego szablonu raportu. W oknie **Wybieranie typu szablonu raportu**, w sekcji **Inne** wybierz **Raport o stanie szyfrowania zarządzanych urządzeń**.

   Po zakończeniu pracy kreatora tworzenia nowego szablonu raportu, nowy szablon raportu pojawi się w węźle Serwer administracyjny, na zakładce **Raporty**.
5. W węźle odpowiedniego Serwera administracyjnego, na zakładce **Raporty** wybierz szablon raportu, który został utworzony w poprzednich krokach instrukcji.

Zostanie rozpoczęte tworzenie raportu. Raport pojawi się na zakładce **Raporty** węzła **Serwer administracyjny**.

Możesz również zapoznać się z informacjami o spełnianiu warunków zasady szyfrowania przez stan szyfrowania urządzeń i nośników wymiennych, które są dostępne na panelach informacyjnych, na zakładce **Statystyki**, w węźle Serwer administracyjny.

W celu wygenerowania raportu o blokowaniu dostępu do zaszyfrowanych plików:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Kliknij przycisk **Nowy szablon raportu**, aby uruchomić Kreator tworzenia nowego szablonu raportu.
4. Postępuj zgodnie z instrukcjami kreatora tworzenia nowego szablonu raportu. W oknie **Wybieranie typu szablonu raportu**, w sekcji **Inne** wybierz **Raport o zablokowanym dostępie do zaszyfrowanych plików**.

   Po zakończeniu pracy kreatora tworzenia nowego szablonu raportu, nowy szablon raportu pojawi się w węźle **Serwer administracyjny**, na zakładce **Raporty**.
5. W węźle **Serwer administracyjny**, na zakładce **Raporty** wybierz szablon raportu, który został utworzony w poprzednich krokach instrukcji.

Zostanie rozpoczęte tworzenie raportu. Raport pojawi się na zakładce **Raporty** węzła **Serwer administracyjny**.

Przesyłanie kluczy szyfrowania między Serwerami administracyjnymi

Jeśli funkcja szyfrowania danych jest włączona na zarządzanym urządzeniu, klucz szyfrowania jest przechowywany na Serwerze administracyjnym. Klucz szyfrowania służy do uzyskiwania dostępu do zaszyfrowanych danych i zarządzania zasadą szyfrowania.

Klucz szyfrowania musi zostać przesłany do innego Serwera administracyjnego w następujących przypadkach:

- Ponownie skonfiguruj Agenta sieciowego na zarządzanym urządzeniu, aby przypisać urządzenie do innego Serwera administracyjnego. Jeśli to urządzenie zawiera zaszyfrowane dane, klucz szyfrowania musi zostać przesłany do docelowego Serwera administracyjnego. W przeciwnym razie dane nie mogą zostać odszyfrowane.
- Szyfrujesz dysk wymienny podłączony do urządzenia D1 zarządzanego przez Serwer administracyjny S1, a następnie podłączasz ten dysk wymienny do urządzenia D2 zarządzanego przez Serwer administracyjny S2. Aby uzyskać dostęp do danych na dysku wymiennym, klucz szyfrowania musi zostać przesłany z Serwera administracyjnego S1 do Serwera administracyjnego S2.
- Zaszyfrujesz plik na urządzeniu D1 zarządzanym przez Serwer administracyjny S1, a następnie próbujesz uzyskać dostęp do pliku na urządzeniu D2 zarządzanym przez Serwer administracyjny S2. Aby uzyskać dostęp do pliku, klucz szyfrowania musi zostać przesłany z Serwera administracyjnego S1 do Serwera administracyjnego S2.

Możesz przesłać klucze szyfrowania na następujące sposoby:

- Automatycznie, włączając opcję **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania** we właściwościach dwóch Serwerów administracyjnych, między którymi należy przesłać klucz szyfrowania. Jeśli ta opcja jest wyłączona dla jednego z Serwerów administracyjnych, automatyczne przesyłanie kluczy szyfrowania nie jest możliwe.

  Jeśli włączysz opcję **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania** we właściwościach Serwera administracyjnego, Serwer administracyjny wyśle wszystkie klucze szyfrowania przechowywane w swoim repozytorium do głównego Serwera administracyjnego (jeśli istnieje) o jeden poziom wyżej w hierarchii.

Podczas próby uzyskania dostępu do zaszyfrowanych danych Serwer administracyjny najpierw wyszukuje klucz szyfrowania we własnym repozytorium. Jeśli opcja **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania** jest włączona, a żądany klucz szyfrowania nie został znaleziony w repozytorium, Serwer administracyjny dodatkowo wyśle żądanie do głównych Serwerów administracyjnych (jeśli istnieją) w celu dostarczenia żądanego klucza szyfrowania. Żądanie zostanie wysłane na wszystkie główne Serwery administracyjne, aż do serwera na najwyższym poziomie hierarchii.

Opcja **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania** nie jest obecnie dostępna w interfejsie Web Console. Jeśli nie masz dostępu do Konsoli administracyjnej opartej na MMC, użyj głównego Serwera administracyjnego do zarządzania zaszyfrowanymi urządzeniami.

- Ręcznie z jednego Serwera administracyjnego na inny, eksportując i importując plik zawierający klucze szyfrowania.

  Eksportowanie i importowanie kluczy szyfrowania to czynności uwzględnione w funkcji zarządzania kluczami szyfrowania. Aby wykonać te akcje, skonfiguruj prawa dostępu do funkcji dla użytkowników Kaspersky Security Center w następujący sposób:

  - Przyznaj prawo dostępu **Odczyt** do funkcji zarządzania kluczami szyfrowania użytkownikowi, który eksportuje klucze szyfrowania z pomocniczego Serwera administracyjnego.
  - Przyznaj prawo dostępu **Wpisz** do funkcji zarządzania kluczami szyfrowania użytkownikowi, który importuje klucze szyfrowania na docelowy Serwer administracyjny.

W celu włączenia automatycznego przesyłania kluczy szyfrowania między Serwerami administracyjnymi w obrębie hierarchii:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz włączyć automatyczne przesyłanie kluczy szyfrowania.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości wybierz sekcję **Algorytm szyfrowania**.
4. Włącz opcję **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania**.
5. Kliknij **OK**, aby zastosować zmiany.

Klucze szyfrowania zostaną przesłane na główne Serwery administracyjne (jeśli istnieją) przy kolejnej synchronizacji (puls). Ten Serwer administracyjny dostarczy również, na żądanie, klucz szyfrowania ze swojego repozytorium do podrzędnego Serwera administracyjnego.

W celu ręcznego przesyłania kluczy szyfrowania między Serwerami administracyjnymi:

1. W drzewie konsoli Serwera administracyjnego wybierz podrzędny Serwer administracyjny, z którego chcesz przesyłać klucze szyfrowania.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości wybierz sekcję **Algorytm szyfrowania**.
4. Kliknij **Wyeksportuj klucze szyfrowania z Serwera administracyjnego**.

   Upewnij się, że użytkownik, który eksportuje klucze szyfrowania z serwera, ma przyznane prawo dostępu **Odczyt** do funkcji zarządzania kluczami szyfrowania.

5. W oknie **Eksportuj klucze szyfrowania**:

   - Kliknij przycisk **Przeglądaj**, a następnie określ, gdzie należy zapisać plik.
   - Określ hasło do ochrony pliku przed nieautoryzowanym dostępem.

     Zapamiętaj hasło. Utraconego hasła nie można odzyskać. Jeśli hasło zostanie utracone, należy powtórzyć procedurę eksportowania. Dlatego zanotuj hasło i miej je pod ręką.

6. Prześlij plik na inny Serwer administracyjny, na przykład, poprzez folder współdzielony lub nośnik wymienny.
7. Na docelowym Serwerze administracyjnym upewnij się, że Konsola administracyjna Kaspersky Security Center jest uruchomiona.
8. W drzewie konsoli Serwera administracyjnego wybierz docelowy Serwer administracyjny, gdzie chcesz przesłać klucze szyfrowania.
9. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
10. W oknie właściwości wybierz sekcję **Algorytm szyfrowania**.
11. Kliknij **Zaimportuj klucze szyfrowania do Serwera administracyjnego**.

    Upewnij się, że użytkownik, który eksportuje klucze szyfrowania z serwera, ma przyznane prawo dostępu **Wpisz** do funkcji zarządzania kluczami szyfrowania.
12. W oknie **Importuj klucze szyfrowania**:

    - Kliknij przycisk **Przeglądaj**, a następnie wybierz plik zawierający klucze szyfrowania.
    - Określ hasło.

13. Kliknij **OK**.

Klucze szyfrowania są przesyłane na docelowy Serwer administracyjny.

Repozytoria danych

Ta sekcja zawiera informacje o danych przechowywanych na Serwerze administracyjnym i używanych do śledzenia stanu urządzeń klienckich oraz sposobie zarządzania nimi.

Folder **Repozytoria** drzewa konsoli wyświetla dane używane do śledzenia stanów urządzeń klienckich.

Folder **Repozytoria** zawiera następujące obiekty:

- Uaktualnienia pobrane przez Serwer administracyjny, które mogą zostać rozesłane na urządzenia klienckie
- Listę sprzętu wykrytego w sieci
- Klucze licencyjne wykryte na urządzeniach klienckich
- Pliki umieszczone w folderach Kwarantanny na urządzeniach przez aplikacje zabezpieczające

- Pliki umieszczone w Kopii zapasowej na urządzeniach klienckich
- Pliki, dla których odroczono skanowanie przez aplikacje antywirusowe

Eksportowanie listy obiektów w repozytorium do pliku tekstowego

Możesz wyeksportować listę obiektów z repozytorium do pliku tekstowego.

W celu wyeksportowania listy obiektów z repozytorium do pliku tekstowego:

1. W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder odpowiedniego repozytorium.
2. W podfolderze repozytorium, z menu kontekstowego wybierz **Eksportuj listę**.

   Zostanie otwarte okno **Eksportuj listę**, w którym możesz określić nazwę pliku tekstowego i ścieżkę do folderu, w którym się znajduje.

Pakiety instalacyjne

Kaspersky Security Center umieszcza pakiety instalacyjne aplikacji firmy Kaspersky oraz firm trzecich w repozytoriach danych.

Pakiet instalacyjny to zestaw plików niezbędnych do instalacji aplikacji. Pakiet instalacyjny zawiera ustawienia instalacyjne i wstępnej konfiguracji aplikacji.

Jeśli chcesz zainstalować aplikację na urządzeniu klienckim, utwórz dla niej pakiet instalacyjny lub użyj istniejącego pakietu. Lista utworzonych pakietów instalacyjnych znajduje się w drzewie konsoli, w folderze **Zdalna instalacja**, w podfolderze **Pakiety instalacyjne**.

Główne stany plików w repozytorium

Aplikacje zabezpieczające skanują pliki na urządzeniach w poszukiwaniu znanych wirusów i innych programów, które mogą stwarzać zagrożenie, przydzielają stany do plików i umieszczają niektóre z nich w repozytorium.

Aplikacje zabezpieczające mogą, na przykład:

- Zapisać kopię pliku w repozytorium przed jego usunięciem
- Odizolować prawdopodobnie zainfekowane pliki w repozytorium

Stany plików zostały przedstawione w poniższej tabeli. Możesz uzyskać więcej informacji o działaniach podejmowanych na plikach w odpowiednich systemach pomocy aplikacji zabezpieczających.

Stany plików w repozytorium

Nazwa stanu	Opis stanu
Zainfekowany	Plik zawiera sekcję kodu znanego wirusa lub innego szkodliwego programu, którego informacje zostały wykryte w antywirusowych bazach danych Kaspersky.
Niezainfekowany	W pliku nie wykryto znanych wirusów ani innych szkodliwych programów.
Ostrzeżenie	Plik zawiera fragment kodu, który częściowo odpowiada fragmentowi kodu znanego zagrożenia.

Nazwa stanu	Opis stanu
Prawdopodobnie zainfekowany	Plik zawiera zmodyfikowany kod znanego wirusa lub kod przypominający wirusa, który nie jest jeszcze znany Kaspersky.
Umieszczony w folderze przez użytkownika	Użytkownik ręcznie umieścił plik w repozytorium, ponieważ zachowanie pliku wzbudzało podejrzenie, że może on zawierać jakieś zagrożenia. Użytkownik może przeskanować plik w poszukiwaniu zagrożeń z użyciem aktualnych baz danych.
Fałszywy alarm	Aplikacja Kaspersky przydzieliła stan Zainfekowany do niezainfekowanego pliku, ponieważ jego kod jest podobny do kodu wirusa. Po przeskanowaniu pliku z użyciem aktualnych baz danych, plik zostaje zidentyfikowany jako niezainfekowany.
Wyleczony	Plik został pomyślnie wyleczony.
Usunięty	Plik został usunięty podczas przetwarzania.
Zabezpieczony hasłem	Plik nie może zostać przetworzony, ponieważ jest chroniony hasłem.

Wywoływanie reguł w trybie Inteligentne uczenie

Ta sekcja zawiera informacje o wykrywaniu obiektów, wykonywanym przez reguły Adaptacyjnej kontroli anomalii w Kaspersky Endpoint Security for Windows na urządzeniach klienckich.

Reguły wykrywają nietypowe zachowania na urządzeniach klienckich i mogą je zablokować. Jeśli reguły działają w trybie Inteligentne uczenie, wykrywają nietypowe zachowania i wysyłają raporty o każdym takim wystąpieniu do Serwera administracyjnego Kaspersky Security Center. Te informacje są przechowywane pod postacią listy w podfolderze **Wyzwalacze reguł w Trybie inteligentnego uczenia** folderu **Repozytoria**. Możesz potwierdzić wykrycie obiektów jako poprawne lub dodać je jako wykluczenia, żeby ten typ zachowania nie był już uznawany za nietypowy.

Informacje o wykrytych obiektach są przechowywane w dzienniku zdarzeń na Serwerze administracyjnym (wraz z innymi zdarzeniami) i w raporcie Adaptacyjnej kontroli anomalii.

Więcej informacji o Adaptacyjnej kontroli anomalii, regułach, ich trybach i stanach można znaleźć w pomocy Kaspersky Endpoint Security for Windows.

Przeglądanie listy obiektów wykrytych przy użyciu reguł Adaptacyjnej kontroli anomalii

W celu przejrzenia listy obiektów wykrytych przez reguły Adaptacyjnej kontroli anomalii:

1. W drzewie konsoli wybierz węzeł Serwera administracyjnego, którego potrzebujesz.
2. Wybierz podfolder **Wyzwalacze reguł w Trybie inteligentnego uczenia** (domyślnie jest to podfolder **Zaawansowane → Repozytoria**).

   Lista wyświetla następujące informacje o obiektach wykrytych przy użyciu reguł Adaptacyjnej kontroli anomalii:

   - **Grupa administracyjna**

     Nazwa grupy administracyjnej, do której należy urządzenie.

   - **Nazwa urządzenia**

     Nazwa urządzenia klienckiego, do którego reguła została zastosowana.

   - **Nazwa**

     Nazwa zastosowanej reguły.

- **Stan**

  Wykluczanie—jeśli administrator przetworzył ten element i dodał go jako wykluczenie do reguł. Ten stan pozostanie do kolejnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym; po synchronizacji element zniknie z listy.

  Potwierdzanie—jeśli administrator przetworzył ten element i zatwierdził go. Ten stan pozostanie do kolejnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym; po synchronizacji element zniknie z listy.

  Pusty—jeśli administrator nie przetworzył tego elementu.

- **Łączna liczba wyzwoleń reguł**

  Liczba wykryć w obrębie jednej reguły heurystycznej, jeden proces i jedno urządzenie klienckie. Ta liczba jest zliczana przez Kaspersky Endpoint Security.

- **Nazwa użytkownika**

  Nazwa użytkownika urządzenia klienckiego, który uruchomił proces, który wygenerował wykrycie.

- **Ścieżka procesu źródłowego**

  Ścieżka do procesu źródłowego, czyli do procesu, który wykonuje akcję (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna procesu źródłowego**

  Suma kontrolna SHA256 pliku procesu źródłowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Ścieżka obiektu źródłowego**

  Ścieżka do obiektu, który uruchomił proces (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna obiektu źródłowego**

  Suma kontrolna SHA256 pliku źródłowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Ścieżka procesu docelowego**

  Ścieżka do procesu docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna procesu docelowego**

  Suma kontrolna SHA256 pliku docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Ścieżka obiektu docelowego**

  Ścieżka do obiektu docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna obiektu docelowego**

  Suma kontrolna SHA256 pliku docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Przetworzono**

  Data wykrycia anomalii.

W celu wyświetlenia właściwości każdego elementu informacji:

1. W drzewie konsoli wybierz węzeł Serwera administracyjnego, którego potrzebujesz.
2. Wybierz podfolder **Wyzwalacze reguł w Trybie inteligentnego uczenia** (domyślnie jest to podfolder **Zaawansowane → Repozytoria**).
3. W obszarze roboczym **Wyzwalacze reguł w Trybie inteligentnego uczenia** wybierz żądany obiekt.
4. Wykonaj jedną z poniższych czynności:
   - Kliknij odnośnik **Właściwości** w oknie z informacjami, które pojawi się w prawej części okna.
   - W menu kontekstowym kliknij prawym klawiszem myszy i wybierz **Właściwości**.

   Zostanie otwarte okno właściwości obiektu, wyświetlające informacje o wybranym elemencie.

Możesz potwierdzić lub dodać do wykluczeń dowolny element z listy wykrytych obiektów reguł Adaptacyjnej kontroli anomalii.

W celu zatwierdzenia elementu:

Wybierz element (lub kilka elementów) na liście wykrytych obiektów i kliknij przycisk **Potwierdź**.

Stan elementu(ów) zostanie zmieniony na **Potwierdzanie**.

Twoje potwierdzenie zostanie uwzględnione w statystykach używanych przez reguły (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security 11 for Windows).

W celu dodania elementu jako wykluczenia:

Kliknij prawym klawiszem element (lub kilka elementów) na liście wykrytych obiektów i w menu kontekstowym wybierz **Dodaj do wykluczeń**.

Zostanie uruchomiony Kreator dodawania wykluczenia. Postępuj zgodnie z instrukcjami kreatora.

Jeśli odrzucisz lub zatwierdzisz element, zostanie on wykluczony z listy wykrytych obiektów po kolejnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym i już nie pojawi się na liście.

Dodawanie wykluczeń z reguł Adaptacyjnej kontroli anomalii

Kreator dodawania wykluczenia umożliwia dodanie wykluczeń z reguł Adaptacyjnej kontroli anomalii dla Kaspersky Endpoint Security.

Możesz uruchomić kreator poprzez jedną z trzech poniższych procedur.

W celu uruchomienia kreatora dodawania wykluczenia poprzez węzeł Adaptacyjna kontrola anomalii:

1. Z drzewa konsoli wybierz węzeł żądanego Serwera administracyjnego.
2. Wybierz **Wyzwalacze reguł w Trybie inteligentnego uczenia** (domyślnie jest to podfolder **Zaawansowane → Repozytoria**).

3. W obszarze roboczym kliknij prawym klawiszem element (lub kilka elementów) na liście wykrytych obiektów i wybierz **Dodaj do wykluczeń**.

   Za jednym razem możesz dodać do 1000 wykluczeń. Jeśli wybierzesz więcej elementów i spróbujesz dodać je do wykluczeń, zostanie wyświetlona wiadomość o błędzie.

Zostanie uruchomiony Kreator dodawania wykluczenia.

Możesz uruchomić Kreator dodawania wykluczenia z innych węzłów w drzewie konsoli:

- Zakładki **Zdarzenia** okna głównego Serwera administracyjnego (następnie opcja **Żądania użytkownika** lub opcja **Ostatnie zdarzenia**).

- **Raportu o stanie reguł Adaptacyjnej kontroli anomalii**, kolumny **Liczba wykryć**.

Krok 1. Wybieranie aplikacji

Ten krok może zostać pominięty, jeśli posiadasz tylko jedną wersję Kaspersky Endpoint Security for Windows i nie posiadasz innych aplikacji, które obsługują reguł Adaptacyjnej kontroli anomalii.

Kreator dodawania wykluczenia wyświetla listę aplikacji firmy Kaspersky, których wtyczki zarządzające umożliwiają dodawanie wykluczeń do zasady dla tych aplikacji. Wybierz aplikację z listy i kliknij **Dalej**, aby przejść do wyboru zasady, do którego zostanie dodane wykluczenie.

Krok 2. Wybieranie zasady (zasad)

kreator wyświetla listę profili (z profilami zasad) dla Kaspersky Endpoint Security.

Wybierz wszystkie profile i zasady, do których chcesz dodać wykluczenia, a następnie kliknij **Dalej**.

Krok 3. Przetwarzanie zasady (zasad)

Kreator wyświetla pasek postępu podczas przetwarzania zasady. Możesz przerwać przetwarzanie zasad, klikając **Anuluj**.

Zasad dziedziczonych nie można aktualizować. Jeśli nie masz uprawnień do modyfikowania zasady, ta zasada nie zostanie zaktualizowana.

Jeśli wszystkie zasady są przetwarzane (lub jeśli przerwiesz przetwarzanie), zostanie wyświetlony raport. Pokazuje, które zasady zostały zaktualizowane pomyślnie (zielona ikona), a które zasady zostały zaktualizowane (czerwona ikona).

Jest to ostatni krok kreatora. Kliknij **Zakończ**, aby zamknąć kreator.

Kwarantanna i Kopia zapasowa

Aplikacje antywirusowe firmy Kaspersky, zainstalowane na urządzeniach klienckich, podczas skanowania urządzenia mogą umieszczać pliki w Kwarantannie lub Kopii zapasowej.

Kwarantanna jest specjalnym repozytorium, w którym przechowywane są potencjalnie zainfekowane pliki oraz pliki, które nie mogły zostać wyleczone w momencie wykrycia.

Kopia zapasowa została zaprojektowana do przechowywania kopii zapasowych plików, które w wyniku procesu leczenia zostały usunięte lub zmodyfikowane.

Kaspersky Security Center tworzy listę plików umieszczonych w Kwarantannie lub Kopii zapasowej przez aplikacje Kaspersky zainstalowane na urządzeniach. Agenty sieciowe na urządzeniach klienckich przesyłają informacje o plikach w Kwarantannie i Kopii zapasowej do Serwera administracyjnego. Przy użyciu Konsoli administracyjnej możesz przeglądać właściwości plików przechowywanych w repozytoriach na urządzeniach, uruchamiać skanowanie w zakresie złośliwego oprogramowania tych repozytoriów i usuwać przechowywane pliki. Ikony stanów plików są opisane w dodatku.

Operacje powiązanie z kwarantanną i kopią zapasową są obsługiwane w programie Kaspersky Endpoint Security.

Kaspersky Security Center nie kopiuje plików z repozytoriów do Serwera administracyjnego. Wszystkie pliki są przechowywane w repozytoriach na urządzeniach. Plik można przywrócić tylko na urządzeniu z zainstalowaną aplikacją antywirusową, która umieściła plik w repozytorium.

Włączanie zdalnego zarządzania dla plików w repozytoriach

Domyślnie, nie możesz zarządzać plikami umieszczonymi w repozytoriach na urządzeniach klienckich.

W celu włączenia zdalnego zarządzania plikami przechowywanymi w repozytoriach na urządzeniach klienckich:

1. Z drzewa konsoli wybierz grupę administracyjną, dla której chcesz włączyć zdalne zarządzanie dla plików w repozytorium.
2. W obszarze roboczym grupy otwórz zakładkę **Zasady**.
3. Na zakładce **Zasady** wybierz zasadę aplikacji zabezpieczającej, która umieściła pliki w repozytoriach na urządzeniach.
4. W oknie ustawień zasady, w grupie ustawień **Przesyłanie danych do Serwera administracyjnego** zaznacz pola odpowiadające repozytoriom, dla których chcesz włączyć zdalne zarządzanie.

   Lokalizacja grupy ustawień **Przesyłanie danych do Serwera administracyjnego** w oknie właściwości zasady i nazwy pól zależą od aktualnie używanej aplikacji zabezpieczającej.

Przeglądanie właściwości pliku umieszczonego w repozytorium

W celu przejrzenia właściwości pliku w Kwarantannie lub Kopii zapasowej:

1. Z drzewa konsoli wybierz folder **Repozytoria**, a z niego podfolder **Kwarantanna** lub **Kopia zapasowa**.
2. W obszarze roboczym folderu **Kwarantanna** (**Kopia zapasowa**) wybierz plik, którego właściwości chcesz przejrzeć.
3. Z menu kontekstowego pliku wybierz polecenie **Właściwości**.

Usuwanie plików z repozytoriów

W celu usunięcia pliku z Kwarantanny lub Kopii zapasowej:

1. W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder **Kwarantanna** lub **Kopia zapasowa**.
2. W obszarze roboczym folderu **Kwarantanna** (lub **Kopia zapasowa**) zaznacz pliki, które chcesz usunąć, przy użyciu klawisza **Shift** lub **Ctrl**.
3. Usuń pliki w jeden z następujących sposobów:
   - Wybierając **Usuń** z menu kontekstowego plików.
   - Klikając odnośnik **Usuń** (**Usuń**, jeżeli chcesz usunąć jeden plik) w oknie z informacjami dla wybranych plików.

Aplikacje zabezpieczające, które umieściły pliki w repozytoriach na urządzeniach klienckich, usuną te same pliki z tych repozytoriów.

Przywracanie plików z repozytoriów

W celu przywrócenia pliku z Kwarantanny lub Kopii zapasowej:

1. Z drzewa konsoli wybierz folder **Repozytoria**, a z niego podfolder **Kwarantanna** lub **Kopia zapasowa**.
2. W obszarze roboczym folderu **Kwarantanna** (**Kopia zapasowa**) zaznacz pliki, które chcesz przywrócić, przy użyciu klawisza **Shift** lub **Ctrl**.
3. Uruchom przywracanie plików w jeden z następujących sposobów:
   - Wybierając **Przywróć** z menu kontekstowego plików.
   - Klikając odnośnik **Przywróć** w oknie z informacjami dla wybranych plików.

Aplikacje zabezpieczające, które umieściły pliki w repozytoriach na urządzeniach klienckich, przywrócą te same pliki do ich oryginalnych folderów.

Zapisywanie plików z repozytoriów na dysku

Kaspersky Security Center umożliwia zapisanie na dysku kopii plików, które zostały umieszczone przez aplikację zabezpieczającą w Kwarantannie lub Kopii zapasowej na urządzeniu klienckim. Pliki są kopiowane do określonego folderu na urządzeniu, na którym jest zainstalowany program Kaspersky Security Center.

W celu zapisania kopii pliku z Kwarantanny lub Kopii zapasowej na dysku twardym:

1. Z drzewa konsoli wybierz folder **Repozytoria**, a z niego podfolder **Kwarantanna** lub **Kopia zapasowa**.
2. W obszarze roboczym folderu **Kwarantanna** (**Kopia zapasowa**) wybierz plik, który chcesz skopiować na dysk twardy.

3. Uruchom kopiowanie w jeden z następujących sposobów:

   - Wybierając z menu kontekstowego pliku element **Zapisz na dysku**.
   - Klikając odnośnik **Zapisz na dysku** dostępny w oknie z informacjami dla wybranego pliku.

Aplikacja zabezpieczająca, która umieściła plik w Kwarantannie na urządzeniu klienckim, zapisze kopię tego pliku w określonym folderze.

Skanowanie plików w Kwarantannie

W celu przeskanowania plików poddanych kwarantannie:

1. Z drzewa konsoli wybierz folder **Repozytoria**, a z niego podfolder **Kwarantanna**.
2. W obszarze roboczym folderu **Kwarantanna** zaznacz pliki, które chcesz przeskanować, przy użyciu klawisza **`Shift`** lub **`Ctrl`**.
3. Uruchom skanowanie pliku w jeden z następujących sposobów:

   - Wybierając **Skanuj** z menu kontekstowego pliku.
   - Klikając odnośnik **Skanuj** w oknie z informacjami dla wybranych plików.

   Aplikacja uruchomi zadanie skanowania na żądanie dla aplikacji zabezpieczających, które umieściły wybrane pliki w Kwarantannie na urządzeniach, na których te pliki są przechowywane.

Aktywne zagrożenia

Informacje o nieprzetworzonych plikach wykrytych na urządzeniach klienckich są przechowywane w folderze **Repozytoria**, w podfolderze **Aktywne zagrożenia**.

Odroczone przetwarzanie i leczenie plików jest wykonywane przez aplikację antywirusową na żądanie lub po wystąpieniu określonego zdarzenia. Możesz skonfigurować odroczone przetwarzanie.

Leczenie nieprzetworzonego pliku

W celu uruchomienia leczenia nieprzetworzonego pliku:

1. W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder **Aktywne zagrożenia**.
2. W obszarze roboczym folderu **Aktywne zagrożenia** wybierz plik, który chcesz wyleczyć.
3. Uruchom leczenie pliku w jeden z następujących sposobów:

   - Wybierając **Wylecz** z menu kontekstowego pliku.
   - Klikając odnośnik **Wylecz** w oknie z informacjami dla wybranego pliku.

   Podjęta zostanie próba wyleczenia tego pliku.

Jeśli plik zostanie wyleczony, aplikacja antywirusowa, zainstalowana na urządzeniu klienckim, przywróci go do oryginalnego folderu. Wpis dotyczący pliku zostanie usunięty z listy w folderze **Aktywne zagrożenia**. Jeśli pliku nie można wyleczyć, aplikacja antywirusowa, zainstalowana na urządzeniu, usunie go z tego urządzenia. Wpis dotyczący pliku zostanie usunięty z listy w folderze **Aktywne zagrożenia**.

Możliwości leczenia i usuwania plików mogą się różnić w zależności od zainstalowanej aplikacji zabezpieczającej, jej wersji i ustawień.

Zapisywanie nieprzetworzonego pliku na dysku

Kaspersky Security Center umożliwia zapisywanie na dysku kopii nieprzetworzonych plików, wykrytych na urządzeniach klienckich. Odnosi się to do plików przetwarzanych lub usuwanych przez aplikację. Pliki są kopiowane do określonego folderu na urządzeniu, na którym jest zainstalowany program Kaspersky Security Center.

Możesz zapisywać kopie plików jeżeli pliki zostały usunięte lub zmodyfikowane podczas leczenia, a ich kopie są przechowywane w magazynie Kaspersky Endpoint Security for Windows na zarządzanym urządzeniu.

W celu zapisania kopii nieprzetworzonego pliku na dysku:

1. W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder **Aktywne zagrożenia**.
2. W obszarze roboczym folderu **Aktywne zagrożenia** wybierz pliki, które chcesz skopiować na dysk.
3. Uruchom kopiowanie w jeden z następujących sposobów:
   - Wybierając z menu kontekstowego pliku element **Zapisz na dysku**.
   - Klikając odnośnik **Zapisz na dysku** dostępny w oknie z informacjami dla wybranego pliku.

Aplikacja zabezpieczająca, zainstalowana na urządzeniu klienckim, na którym wykryto nieprzetworzony plik, zapisze kopię tego pliku w określonym folderze.

Usuwanie plików z folderu „Aktywne zagrożenia”

*W celu usunięcia pliku z folderu **Aktywne zagrożenia**:*

1. W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder **Aktywne zagrożenia**.
2. W obszarze roboczym folderu **Aktywne zagrożenia** zaznacz pliki, które chcesz usunąć, przy użyciu klawiszy **Shift** i **Ctrl**.
3. Usuń pliki w jeden z następujących sposobów:
   - Wybierając **Usuń** z menu kontekstowego plików.
   - Klikając odnośnik **Usuń** (**Usuń**, jeżeli chcesz usunąć jeden plik) w oknie z informacjami dla wybranych plików.

Aplikacje zabezpieczające, które umieściły pliki w repozytoriach na urządzeniach klienckich, usuną te same pliki z tych repozytoriów. Wpisy dotyczące plików zostaną usunięte z listy w folderze **Aktywne zagrożenia**.

Kaspersky Security Network (KSN)

Ta sekcja opisuje sposób korzystania z infrastruktury usług online o nazwie Kaspersky Security Network (KSN). Sekcja zawiera szczegóły dotyczące KSN, a także instrukcje związane z włączaniem KSN, konfiguracją dostępu do KSN oraz wyświetlaniem statystyk korzystania z serwera proxy KSN.

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), przy czym funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Informacje o KSN

Kaspersky Security Network (KSN) jest to usługa sieciowa oferująca dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji Kaspersky po wykryciu zagrożeń, ulepszenie działania niektórych składników ochrony oraz zmniejszenie ryzyka fałszywych alarmów. KSN umożliwia korzystanie z baz danych reputacji firmy Kaspersky, z których pobierane są informacje o aplikacjach zainstalowanych na zarządzanych urządzeniach.

Kaspersky Security Center obsługuje następujące rozwiązania infrastrukturalne:

- *KSN* to rozwiązanie umożliwiające wymianę informacji z Kaspersky Security Network. Uczestnicząc w KSN, wyrażasz zgodę na wysyłanie do Kaspersky w trybie automatycznym informacji dotyczących działania aplikacji firmy Kaspersky, zainstalowanych na urządzeniach klienckich, które są zarządzane przez Kaspersky Security Center. Informacje są wysyłane zgodnie z bieżącymi ustawieniami dostępu KSN. Analitycy firmy Kaspersky dodatkowo analizują otrzymane informacje i umieszczają je w reputacyjnych i statystycznych bazach danych Kaspersky Security Network. Kaspersky Security Center domyślnie korzysta z tego rozwiązania.

- *Kaspersky Private Security Network (KPSN)* to rozwiązanie, które umożliwia użytkownikom urządzeń z zainstalowanymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do Globalnej sieci KSN z ich własnych urządzeń. Sieć KPSN została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z jednego z następujących powodów:

  - Urządzenia użytkowników nie są podłączone do internetu.

  - Przekazywanie jakichkolwiek danych poza granice kraju lub poza korporacyjną sieć LAN jest zabronione przez prawo lub ograniczone przez korporacyjną politykę bezpieczeństwa.

  Możesz skonfigurować ustawienia dostępu do Kaspersky Private Security Network w sekcji **Ustawienia KSN Proxy** w oknie właściwości Serwera administracyjnego.

Aplikacja wyświetla pytanie o przyłączenie się do KSN podczas działania kreatora wstępnej konfiguracji. Można rozpocząć lub zakończyć korzystanie z KSN w dowolnym momencie, podczas korzystania z aplikacji.

Korzystasz z KSN zgodnie z Oświadczeniem KSN, które czytasz i akceptujesz, gdy włączasz KSN. Jeśli Oświadczenie KSN zostanie zaktualizowane, zostanie wyświetlone podczas aktualizacji Serwera administracyjnego. Możesz zaakceptować zaktualizowane Oświadczenie KSN lub odrzucić je. Jeśli odrzucisz Oświadczenie, będziesz nadal korzystać z KSN zgodnie z poprzednią wersją Oświadczenia KSN, które zaakceptowałeś wcześniej.

Gdy KSN jest włączone, Kaspersky Security Center sprawdza, czy serwery KSN są dostępne. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Jest to konieczne, aby zapewnić utrzymanie poziomu bezpieczeństwa zarządzanych urządzeń.

Urządzenia klienckie zarządzane przez Serwer administracyjny wchodzą w interakcję z KSN poprzez serwer KSN proxy. Serwer proxy KSN posiada następujące cechy:

- Urządzenia klienckie mogą wysyłać żądania do KSN, otrzymywać informacje z KSN oraz przesyłać informacje do KSN nawet wtedy, gdy nie mają bezpośredniego dostępu do internetu.
- Serwer KSN proxy buforuje przetwarzane dane, ograniczając obciążenie połączenia wychodzącego i czas oczekiwania na informacje żądane przez urządzenie klienckie.

Serwer KSN Proxy można skonfigurować w sekcji **Ustawienia KSN Proxy** dostępnej w oknie właściwości Serwera administracyjnego.

Konfigurowanie dostępu do Kaspersky Security Network

Możesz skonfigurować dostęp do Kaspersky Security Network (KSN) na Serwerze administracyjnym i na punkcie dystrybucji.

W celu skonfigurowania dostępu Serwera administracyjnego do Kaspersky Security Network (KSN):

1. W drzewie konsoli należy wybrać Serwer administracyjny, dla którego chcesz skonfigurować dostęp do KSN.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **KSN Proxy** → **Ustawienia KSN Proxy**.
4. W obszarze roboczym włącz opcję **Użyj Serwera administracyjnego** jako serwera proxy, aby włączyć usługę KSN Proxy.

   Dane są wysyłane z urządzeń klienckich do KSN zgodnie z zasadą Kaspersky Endpoint Security, która jest aktywna na tych urządzeniach klienckich. Jeśli to pole jest odznaczone, żadne dane nie będą wysyłane do KSN z Serwera administracyjnego i urządzeń klienckich poprzez Kaspersky Security Center. Jednakże urządzenia klienckie mogą wysyłać dane bezpośrednio do KSN (z pominięciem Kaspersky Security Center) zgodnie z ich ustawieniami. Zasada Kaspersky Endpoint Security for Windows, aktywna na urządzeniach klienckich, określa, które dane będą wysyłane bezpośrednio z tych urządzeń do KSN (z pominięciem Kaspersky Security Center).
5. Włącz opcję **Zgadzam się na korzystanie z Kaspersky Security Network**.

   Jeśli ta opcja jest włączona, urządzenia klienckie będą wysyłać wyniki instalacji łat do Kaspersky. Przed włączeniem tej opcji należy przeczytać i zaakceptować warunki Oświadczenia KSN.

   Jeśli używasz Kaspersky Private Security Network (KPSN), włącz opcję **Konfiguruj KPSN** i kliknij przycisk **Wybierz plik z ustawieniami KSN Proxy**, aby pobrać ustawienia sieci KPSN (pliki z rozszerzeniami pkcs7 i pem). Po pobraniu ustawień, interfejs wyświetla kontakty i nazwę dostawcy, a także datę utworzenia pliku z ustawieniami prywatnej sieci KPSN.

Jeśli włączysz sieć KPSN, zwróć uwagę na punkty dystrybucji skonfigurowane do wysyłania żądań KSN bezpośrednio do Cloud KSN. Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej) będzie nadal wysyłał żądania KSN do Cloud KSN. Aby ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do sieci KPSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji. Możesz włączyć tę opcję we właściwościach punktu dystrybucji lub w zasadzie Agenta sieciowego.

Jeśli zaznaczysz pole **Konfiguruj KPSN**, pojawi się wiadomość ze szczegółami dotyczącymi sieci KPSN.

Jeśli włączysz opcję **Konfiguruj KPSN** w Kaspersky Security Center, te aplikacje otrzymają informację o obsłudze sieci KPSN. W oknie ustawień aplikacji, w podsekcji **Kaspersky Security Network** sekcji **Zaawansowana ochrona przed zagrożeniami** wyświetlana jest informacja dotycząca wybranego dostawcy sieci KSN – KSN lub KPSN.

Jeśli podczas działania sieci KPSN korzystasz z wcześniejszej wersji aplikacji Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 lub Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent, zalecamy korzystanie z podrzędnych Serwerów administracyjnych, dla których włączono korzystanie z sieci KPSN.

Kaspersky Security Center nie wysyła żadnych danych statystycznych do Kaspersky Security Network, jeśli sieć KPSN została skonfigurowana w sekcji **KSN Proxy** → **Ustawienia KSN Proxy** okna właściwości Serwera administracyjnego.

Jeśli skonfigurowałeś ustawienia serwera proxy we właściwościach Serwera administracyjnego, ale Twoja sieć wymaga, abyś korzystał bezpośrednio z prywatnej sieci KSN, włącz opcję **Ignoruj ustawienia serwera proxy w przypadku łączenia z KPSN**. W przeciwnym razie, żądania z zarządzanych aplikacji nie będą mogły dotrzeć do KPSN.

6. Skonfiguruj połączenie Serwera administracyjnego z usługą KSN proxy:

   - W sekcji **Ustawienia połączenia**, w polu **Port TCP** określ numer portu TCP, który będzie używany do nawiązywania połączenia z serwerem proxy KSN. Domyślny port do nawiązywania połączenia z serwerem KSN proxy to 13111.

   - Jeśli chcesz, żeby Serwer administracyjny nawiązywał połączenie z serwerem proxy KSN poprzez port UDP, włącz opcję **Użyj portu UDP** i w polu **Port UDP** określ numer portu. Domyślnie opcja ta jest wyłączona i używany jest port TCP. Jeśli ta opcja jest włączona, domyślny port UDP do nawiązywania połączenia z serwerem KSN proxy to 15111.

   - Jeśli chcesz, żeby Serwer administracyjny nawiązywał połączenie z serwerem proxy KSN poprzez port HTTPS, włącz opcję **Użyj HTTPS przez port** i określ numer portu. Domyślnie opcja ta jest wyłączona i używany jest port TCP. Jeśli ta opcja jest włączona, domyślny port HTTPS do nawiązywania połączenia z serwerem KSN proxy to 17111.

7. Włącz opcję **Połącz podrzędne Serwery administracyjne z KSN przez główny Serwer administracyjny**.

   Jeśli ta opcja jest włączona, podrzędne Serwery administracyjne używają głównego Serwera administracyjnego jako serwera KSN proxy. Jeśli ta opcja jest wyłączona, podrzędne Serwery administracyjne same łączą się z KSN. W tym przypadku zarządzane urządzenia używają podrzędnych Serwerów administracyjnych jako serwerów KSN proxy.

Podrzędne Serwery administracyjne używają głównego Serwera administracyjnego jako serwera proxy, jeśli w prawej części sekcji **Ustawienia KSN Proxy**, dostępnej we właściwościach podrzędnych Serwerów administracyjnych, zaznaczono pole **Użyj Serwera administracyjnego jako serwera proxy**.

8. Kliknij **OK**.

Ustawienia dostępu do KSN zostaną zapisane.

Możesz także skonfigurować dostęp punktu dystrybucji do KSN, na przykład, jeśli chcesz zmniejszyć obciążenie na Serwerze administracyjnym. Punkt dystrybucji działający jako serwer KSN proxy wysyła żądania KSN z zarządzanych urządzeń bezpośrednio do Kaspersky, bez używania Serwera administracyjnego.

W celu skonfigurowania dostępu punktu dystrybucji do Kaspersky Security Network (KSN):

1. Upewnij się, że punkt dystrybucji został przypisany ręcznie.
2. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
3. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
4. W oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.
5. Na liście wskaż punkt dystrybucji i kliknij przycisk **Właściwości**, aby otworzyć jego okno właściwości.
6. W oknie właściwości punktu dystrybucji, w sekcji **KSN Proxy** zaznacz **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**.
7. Kliknij **OK**.

Punkt dystrybucji będzie działał jako serwer KSN proxy.

Włączanie i wyłączanie KSN

W celu włączenia KSN:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz wyłączyć KSN.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w sekcji **KSN Proxy** wybierz podsekcję **Ustawienia KSN Proxy**.
4. Wybierz **Użyj Serwera administracyjnego jako serwera proxy**.

   Serwer KSN proxy zostanie włączony.
5. Zaznacz pole **Zgadzam się na korzystanie z Kaspersky Security Network**.

   Usługa KSN zostanie włączona.

   Jeśli ta opcja jest zaznaczona, urządzenia klienckie będą wysyłać wyniki instalacji łat do Kaspersky. Przed zaznaczeniem tego pola należy przeczytać i zaakceptować warunki Oświadczenia KSN.
6. Kliknij **OK**.

W celu wyłączenia KSN:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz wyłączyć KSN.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w sekcji **KSN Proxy** wybierz podsekcję **Ustawienia KSN Proxy**.
4. Odznacz pole **Użyj Serwera administracyjnego** jako serwera proxy, aby wyłączyć usługę KSN Proxy, lub odznacz pole **Zgadzam się na korzystanie z Kaspersky Security Network**.

   Jeśli ta opcja jest odznaczona, urządzenia klienckie nie będą wysyłać wyników instalacji łat do Kaspersky.

   Jeśli korzystasz z KPSN, odznacz pole **Konfiguruj KPSN**.

   Usługa KSN zostanie wyłączona.
5. Kliknij **OK**.

Przeglądanie zaakceptowanego Oświadczenia KSN

Po włączeniu Kaspersky Security Network (KSN) musisz przeczytać i zaakceptować Oświadczenie KSN. W każdej chwili możesz przejrzeć zaakceptowane Oświadczenie KSN.

W celu przejrzenia zaakceptowanego Oświadczenia KSN:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego włączyłeś KSN.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w sekcji **KSN Proxy** wybierz podsekcję **Ustawienia KSN Proxy**.
4. Kliknij odnośnik **Wyświetl zaakceptowane oświadczenie KSN**.

W otwartym oknie możesz przejrzeć treść zaakceptowanego Oświadczenia KSN.

Przeglądanie statystyk serwera proxy KSN

Serwer KSN proxy jest usługą ułatwiającą interakcję między infrastrukturą Kaspersky Security Network a urządzeniami klienckimi zarządzanymi przez Serwer administracyjny.

Korzystanie z serwera KSN proxy oferuje następujące możliwości:

- Urządzenia klienckie mogą wysyłać żądania do KSN oraz przesyłać informacje do KSN nawet wtedy, gdy nie mają bezpośredniego dostępu do internetu.
- Serwer KSN proxy buforuje przetwarzane dane, ograniczając obciążenie połączenia wychodzącego i czas oczekiwania na informacje żądane przez urządzenie klienckie.

W oknie właściwości Serwera administracyjnego możesz skonfigurować serwer KSN proxy i przejrzeć statystyki korzystania z serwera KSN proxy.

W celu przejrzenia statystyk dotyczących serwera proxy KSN:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz przejrzeć statystyki KSN.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w sekcji **KSN Proxy** wybierz podsekcję **Statystyki KSN Proxy**.

   W tej sekcji wyświetlane są aktualne statystyki działania serwera proxy KSN (liczba rekordów pamięci podręcznej, pakietów przetworzonych w pamięci podręcznej i otrzymanych pakietów). Również jeśli Serwer administracyjny jest połączony z KSN, wyświetlany jest odpowiedni komunikat informacyjny.

   Jeśli to konieczne, wykonaj dodatkowe działania:

   - Kliknij **Odśwież**, aby zaktualizować statystyki korzystania z serwera KSN proxy.
   - Kliknij przycisk **Eksportuj do pliku**, aby wyeksportować statystyki do pliku CSV.
   - Kliknij przycisk **Sprawdź połączenie z KSN**, aby sprawdzić, czy Serwer administracyjny jest aktualnie połączony z KSN.
4. Kliknij przycisk **OK**, aby zamknąć okno właściwości Serwera administracyjnego.

Akceptowanie zaktualizowanego Oświadczenia KSN

Korzystasz z KSN zgodnie z Oświadczeniem KSN, które czytasz i akceptujesz, gdy włączasz KSN. Jeśli Oświadczenie KSN zostanie zaktualizowane, zostanie wyświetlone podczas aktualizacji lub uaktualniania Serwera administracyjnego. Możesz zaakceptować zaktualizowane Oświadczenie KSN lub odrzucić je. Jeśli odrzucisz Oświadczenie, będziesz nadal korzystać z KSN zgodnie z wersją Oświadczenia KSN, którą zaakceptowałeś wcześniej.

Po aktualizacji lub uaktualnieniu Serwera administracyjnego zaktualizowane Oświadczenie KSN jest wyświetlane automatycznie. Jeśli odrzucisz zaktualizowane Oświadczenie KSN, nadal możesz je przejrzeć i zaakceptować później.

W celu wyświetlenia, a następnie zaakceptowania lub odrzucenia zaktualizowanego Oświadczenia KSN:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Na zakładce **Monitorowanie**, w sekcji **Monitorowanie** kliknij plik odnośnik **Zaakceptowane Oświadczenie Kaspersky Security Network jest nieaktualne**.

   Zostanie otwarte okno **Oświadczenie KSN**.
3. Uważnie przeczytaj Oświadczenie KSN, a następnie podejmij decyzję. Jeśli akceptujesz zaktualizowane Oświadczenie KSN, kliknij przycisk **Akceptuję warunki Umowy licencyjnej**. Jeśli odrzucisz zaktualizowane Oświadczenie KSN, kliknij przycisk **Anuluj**.

W zależności od Twojego wyboru KSN działa zgodnie z warunkami aktualnego lub zaktualizowanego Oświadczenia KSN. Możesz wyświetlić tekst zaakceptowanego Oświadczenia KSN we właściwościach Serwera administracyjnego w dowolnym momencie.

Udoskonalona ochrona przy pomocy Kaspersky Security Network

Kaspersky oferuje użytkownikom dodatkową warstwę ochrony przy pomocy Kaspersky Security Network. Ta metoda ochrony została zaprojektowana do walki z zaawansowanymi zagrożeniami i atakami zero-day. Zintegrowane technologie chmury oraz doświadczenie analityków wirusów z Kaspersky sprawiają, że Kaspersky Endpoint Security jest najlepszym wyborem, jeżeli chodzi o ochronę przed najbardziej wyszukanymi zagrożeniami sieci.

Szczegóły dotyczące udoskonalonej ochrony w Kaspersky Endpoint Security są dostępne na stronie Kaspersky.

Sprawdzanie, czy punkt dystrybucji działa jako serwer proxy KSN

Na zarządzanym urządzeniu przypisanym do pracy jako punkt dystrybucji możesz włączyć serwer proxy KSN. Zarządzane urządzenie działa jako serwer proxy KSN, gdy usługa ksnproxy jest uruchomiona na urządzeniu. Możesz lokalnie sprawdzić, włączyć lub wyłączyć tę usługę na urządzeniu.

Jako punkt dystrybucji można przypisać urządzenie z systemem Windows lub Linux. Metoda sprawdzania punktu dystrybucji zależy od systemu operacyjnego tego punktu dystrybucji.

Aby sprawdzić, czy punkt dystrybucji oparty na systemie Windows działa jako serwer proxy KSN:

1. Na urządzeniu punktu dystrybucji, w systemie Windows otwórz **Usługi** (**Wszystkie programy** → **Narzędzia administracyjne** → **Usługi**).

2. Na liście usług sprawdź, czy usługa ksnproxy jest uruchomiona.

   Jeśli usługa ksnproxy jest uruchomiona, Agent sieciowy na urządzeniu uczestniczy w Kaspersky Security Network i działa jako serwer proxy KSN dla zarządzanych urządzeń należących do obszaru punktu dystrybucji.

Jeśli chcesz, możesz wyłączyć usługę ksnproxy. W takim przypadku Agent sieciowy w punkcie dystrybucji przestaje uczestniczyć w Kaspersky Security Network. To działanie wymaga uprawnień administratora lokalnego.

Aby sprawdzić, czy punkt dystrybucji oparty na systemie Linux działa jako serwer proxy KSN:

1. Na urządzeniu punktu dystrybucji wyświetl listę uruchomionych procesów.

2. Na liście uruchomionych procesów sprawdź, czy proces `/opt/kaspersky/ksc64/sbin/ksnproxy` jest uruchomiony.

Jeśli proces `/opt/kaspersky/ksc64/sbin/ksnproxy` jest uruchomiony, Agent sieciowy na urządzeniu uczestniczy w Kaspersky Security Network i działa jako serwer proxy KSN dla zarządzanych urządzeń należących do obszaru punktu dystrybucji.

Przełączanie między pomocą online i pomocą offline

Jeśli nie masz dostępu do internetu, możesz skorzystać z pomocy offline.

W celu przełączenia między pomocą online i pomocą offline:

1. W oknie głównym Kaspersky Security Center, w drzewie konsoli wybierz **Kaspersky Security Center 15.1**.
2. Kliknij odnośnik **Globalne ustawienia interfejsu**.

   Zostanie otwarte okno ustawień.
3. W oknie ustawień kliknij **Użyj pomocy offline**.
4. Kliknij **OK**.

Ustawienia zostaną zastosowane i zapisane. Jeśli chcesz, możesz w dowolnym momencie wrócić do poprzednich ustawień i rozpocząć korzystanie z pomocy online.

Eksportowanie zdarzeń do systemów SIEM

Ta sekcja opisuje sposób eksportowania zdarzeń zarejestrowanych przez Kaspersky Security Center do zewnętrznych systemów SIEM (Security Information and Event Management).

Konfigurowanie eksportowania zdarzeń do systemów SIEM

Kaspersky Security Center umożliwia konfigurowanie przy użyciu jednej z następujących metod: eksportowanie do dowolnego systemu SIEM korzystającego z formatu Syslog, eksportowanie do systemów QRadar, Splunk, ArcSight SIEM korzystających z formatów LEEF i CEF lub eksportowanie zdarzeń do systemów SIEM bezpośrednio z bazy danych Kaspersky Security Center. Po zakończeniu tego scenariusza Serwer administracyjny automatycznie wysyła zdarzenia do systemu SIEM.

Wymagania wstępne

Zanim rozpoczniesz konfigurowanie eksportowania zdarzeń w Kaspersky Security Center:

- Dowiedz się więcej o metodach eksportowania zdarzeń.
- Upewnij się, że posiadasz wartości ustawień systemowych.

Możesz wykonać kroki tego scenariusza w dowolnej kolejności.

Proces eksportowania zdarzeń do systemu SIEM obejmuje następujące kroki:

- **Konfigurowanie systemu SIEM do odbierania zdarzeń z Kaspersky Security Center**

  Instrukcja: Konfigurowanie eksportowania zdarzeń w systemie SIEM
- **Wybieranie zdarzeń, które chcesz wyeksportować do systemu SIEM:**

Dostępne instrukcje:

- Konsola administracyjna: Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog, Oznaczanie ogólnych zdarzeń do eksportowania w formacie Syslog
- Kaspersky Security Center Web Console: Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog, Oznaczanie ogólnych zdarzeń do eksportowania w formacie Syslog

- **Konfigurowanie eksportowania zdarzeń do systemu SIEM za pomocą jednej z poniższych metod:**
  - Korzystanie z protokołów TCP, UDP lub TLS przez protokoły TCP.

    Dostępne instrukcje:

    - Konsola administracyjna: Konfigurowanie eksportowania zdarzeń do systemów SIEM
    - Kaspersky Security Center Web Console: Konfigurowanie eksportowania zdarzeń do systemów SIEM
  - Używanie eksportowania zdarzeń bezpośrednio z bazy danych Kaspersky Security Center (zestaw widoków publicznych jest dostępny w bazie danych Kaspersky Security Center; opis tych widoków publicznych można znaleźć w dokumencie klakdb.chm).

Wyniki

Po skonfigurowaniu eksportowania zdarzeń do systemu SIEM możesz przeglądać eksportowanie wyników, jeśli wybrałeś zdarzenia, które chcesz wyeksportować.

Czynności niezbędne do wykonania przed rozpoczęciem pracy

Podczas konfigurowania automatycznego eksportowania zdarzeń w Kaspersky Security Center musisz określić niektóre ustawienia systemu SIEM. Zalecane jest wcześniejsze sprawdzenie tych ustawień w celu przygotowania do konfiguracji Kaspersky Security Center.

W celu pomyślnego skonfigurowania automatycznego wysyłania zdarzeń do systemu SIEM należy znać następujące ustawienia:

- **Adres serwera systemu SIEM**

  Adres IP serwera, na którym zainstalowany jest aktualnie używany system SIEM. Sprawdź wartość tego ustawienia w ustawieniach systemu SIEM.

- **Port serwera systemu SIEM**

  Numer portu używanego do nawiązania połączenia pomiędzy Kaspersky Security Center a serwerem Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center i w ustawieniach odbiornika Twojego systemu SIEM.

- **Protokół**

  Protokół używany do przesyłania wiadomości z Kaspersky Security Center do Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center i w ustawieniach odbiornika Twojego systemu SIEM.

Informacje o zdarzeniach w Kaspersky Security Center

Kaspersky Security Center umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Informacje o zdarzeniach są zapisywane w bazie danych Serwera administracyjnego. Możesz wyeksportować te informacje do zewnętrznych systemów SIEM. Eksportowanie informacji o zdarzeniach do zewnętrznych systemów SIEM umożliwia administratorom systemów SIEM natychmiastowe reagowanie na zdarzenia dotyczące systemu bezpieczeństwa, które pojawiają się na zarządzanych urządzeniach lub w grupach administracyjnych.

Typy zdarzeń

W Kaspersky Security Center dostępne są następujące typy zdarzeń:

- Zdarzenia ogólne. Te zdarzenia występują we wszystkich zarządzanych aplikacjach firmy Kaspersky. Przykładem zdarzenia ogólnego jest Epidemia wirusa. Zdarzenia ogólne mają dokładnie zdefiniowaną składnię i semantykę. Zdarzenia ogólne są używane, na przykład, w raportach i pulpitach nawigacyjnych.
- Zarządzane zdarzenia charakterystyczne dla aplikacji firmy Kaspersky. Każda zarządzana aplikacja firmy Kaspersky posiada swój zestaw zdarzeń.

Źródła zdarzeń

Zdarzenia mogą być generowane przez następujące aplikacje:

- Składniki Kaspersky Security Center:
  - Serwer administracyjny
  - Agent sieciowy
  - Serwer iOS MDM
- Zarządzane aplikacje Kaspersky

  Szczegółowe informacje na temat zdarzeń generowanych przez aplikacje zarządzane przez Kaspersky można znaleźć w dokumentacji odpowiedniej aplikacji.

Możesz wyświetlić pełną listę zdarzeń, które mogą być generowane przez aplikację na karcie **Konfiguracja zdarzenia** w zasadzie aplikacji. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić listę zdarzeń we właściwościach Serwera administracyjnego.

Poziom ważności zdarzeń

Każde zdarzenie posiada określony poziom istotności. W zależności od warunków wystąpienia zdarzenia, może ono posiadać różne poziomy istotności. Istnieją cztery poziomy istotności zdarzeń:

- *Zdarzenie krytyczne* to zdarzenie, które wskazuje wystąpienie krytycznego problemu mogącego prowadzić do utraty danych, problemów z działaniem lub błędu krytycznego.
- *Błąd funkcjonalny* to zdarzenie, które wskazuje poważny problem, błąd lub problem z działaniem, który wystąpił podczas działania aplikacji lub podczas przeprowadzania procedury.
- *Ostrzeżenie* to zdarzenie, które niekoniecznie jest poważne, ale wskazuje możliwość wystąpienia potencjalnego problemu w przyszłości. Większość zdarzeń otrzymuje priorytet „Ostrzeżenie", jeśli aplikacja może zostać przywrócona bez utraty danych lub możliwości funkcyjnych aplikacji.
- *Informacja* to zdarzenie, którego celem jest informowanie o pomyślnym zakończeniu działania, właściwym funkcjonowaniu aplikacji lub zakończeniu procedury.

Każde zdarzenie posiada zdefiniowany okres przechowywania, w trakcie którego możesz przejrzeć lub zmodyfikować to zdarzenie w Kaspersky Security Center. Niektóre zdarzenia nie są domyślnie zapisywane w bazie danych Serwera administracyjnego, ponieważ ich zdefiniowany okres przechowywania wynosi zero. Tylko te zdarzenia, które będą przechowywane w bazie danych Serwera administracyjnego przynajmniej jeden dzień, mogą zostać wyeksportowane do systemów zewnętrznych.

Informacje o eksportowaniu zdarzeń

Eksportowanie zdarzeń może być używane w obrębie scentralizowanych systemów, które zajmują się problemami z bezpieczeństwem na poziomie organizacyjnym i technicznym, zapewniają usługi monitorowania ochrony oraz skonsolidowane informacje z różnych rozwiązań. To są systemy SIEM, które oferują przeprowadzania w czasie rzeczywistym analizy alertów o zagrożeniach i zdarzeń zabezpieczeń, wygenerowanych przez aplikacje i sprzęt w sieci, lub Security Operation Centers (SOCs).

Te systemy otrzymują dane z wielu źródeł, w tym sieci, ochrony, serwerów, baz danych i aplikacji. Systemy SIEM oferują także funkcjonalność konsolidowania monitorowanych danych, aby pomóc w uniknięciu przeoczenia zdarzeń krytycznych. Dodatkowo, systemy przeprowadzają zautomatyzowaną analizę powiązanych zdarzeń i alertów w celu powiadomienia administratorów o nagłych problemach z bezpieczeństwem. Wysyłanie alertów może zostać zaimplementowane poprzez pulpit nawigacyjny lub wysyłanie ostrzeżeń może się odbywać poprzez kanały firm trzecich, na przykład pocztę elektroniczną.

Proces eksportowania zdarzeń z Kaspersky Security Center do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia—Kaspersky Security Center oraz odbiorca zdarzenia—system SIEM. Aby pomyślnie eksportować zdarzenia, należy skonfigurować tę funkcję w posiadanym systemie SIEM i w Konsoli administracyjnej Kaspersky Security Center. Nie ma znaczenia, która strona zostanie skonfigurowana jako pierwsza. Możesz skonfigurować przesyłanie zdarzeń w Kaspersky Security Center, a następnie skonfigurować odbieranie zdarzeń przez system SIEM lub na odwrót.

Metody wysyłania zdarzeń z Kaspersky Security Center

Dostępne są trzy metody wysyłania zdarzeń z Kaspersky Security Center do systemów zewnętrznych:

- Wysyłanie zdarzeń po protokole Syslog do dowolnego systemu SIEM

  Korzystając z protokołu Syslog, możesz przekazywać dowolne zdarzenia, które wystąpiły na Serwerze administracyjnym Kaspersky Security Center i w aplikacjach firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Możesz go użyć do eksportowania zdarzeń do systemu SIEM.

  W tym celu należy zaznaczyć zdarzenia, które chcemy przekazać do systemu SIEM. Możesz zaznaczyć zdarzenia w Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console. Tylko zaznaczone zdarzenia będą przekazywane do systemu SIEM. Jeśli nic nie zaznaczysz, żadne zdarzenia nie zostaną przekazane.

- Wysyłanie zdarzeń po protokołach CEF i LEEF do systemów QRadar, Splunk i ArcSight

  Możesz używać protokołów CEF i LEEF do eksportowania zdarzeń ogólnych. Podczas eksportowania zdarzeń po protokołach CEF i LEEF nie masz możliwości wyboru określonych zdarzeń do wyeksportowania. Eksportowane są wszystkie zdarzenia ogólne. Aby skonwertować zdarzenia Kaspersky Security Center na zdarzenia w formacie CEF i LEEF, możesz użyć pliku siem_conversion_rules.xml. Ten plik zawiera listę atrybutów zdarzeń Kaspersky Security Center i odpowiadających im atrybutów zdarzeń w formacie CEF i LEEF. Ponadto plik siem_conversion_rules.xml zawiera reguły generowania komunikatów odpowiadających zdarzeniom. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center.

  W przeciwieństwie do protokołu Syslog, protokoły CEF i LEEF nie są uniwersalne. Protokoły CEF i LEEF są przeznaczone dla odpowiednich systemów SIEM (QRadar, Splunk i ArcSight). Dlatego też, jeśli wybierzesz eksportowanie zdarzeń poprzez jeden z tych protokołów, użyjesz parsera w systemie SIEM.

- Bezpośrednio z bazy danych Kaspersky Security Center do dowolnego systemu SIEM

  Ta metoda eksportowania zdarzeń może zostać użyta do odbierania zdarzeń bezpośrednio z widoków publicznych bazy danych przy użyciu zapytań SQL. Wyniki zapytań są zapisywane do pliku XML, który może zostać użyty jako dane wejściowe systemu zewnętrznego. Tylko zdarzenia dostępne w widokach publicznych mogą być eksportowane bezpośrednio z bazy danych.

Odbieranie zdarzeń przez system SIEM

System SIEM musi odbierać i poprawnie analizować zdarzenia otrzymywane z Kaspersky Security Center. W tym celu należy odpowiednio skonfigurować system SIEM. Konfiguracja zależy od specyfiki używanego systemu SIEM. Jednakże istnieje kilka ogólnych kroków w konfiguracji wszystkich systemów SIEM, takie jak konfigurowanie odbiorcy i analizatora.

Informacje o konfigurowaniu eksportowania zdarzeń w systemie SIEM

Proces eksportowania zdarzeń z Kaspersky Security Center do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia—Kaspersky Security Center oraz odbiorca zdarzenia—system SIEM. Należy skonfigurować eksportowanie zdarzeń w posiadanym systemie SIEM i w Kaspersky Security Center.

Ustawienia określane w systemie SIEM zależą od określonego systemu, którego używasz. Zazwyczaj dla wszystkich systemów SIEM należy skonfigurować odbiorcę i, opcjonalnie, analizatora wiadomości do analizowania otrzymanych zdarzeń.

Konfigurowanie odbiorcy

Aby otrzymywać zdarzenia wysyłane przez Kaspersky Security Center, należy skonfigurować odbiorcę w swoim systemie SIEM. W systemie SIEM powinny zostać określone następujące ustawienia:

- **Protokół eksportu lub typ wejścia**

  Jest to protokół przesyłania wiadomości, na przykład UDP. Ten protokół musi być taki sam, jak protokół, który określiłeś w Kaspersky Security Center.

- **Port**

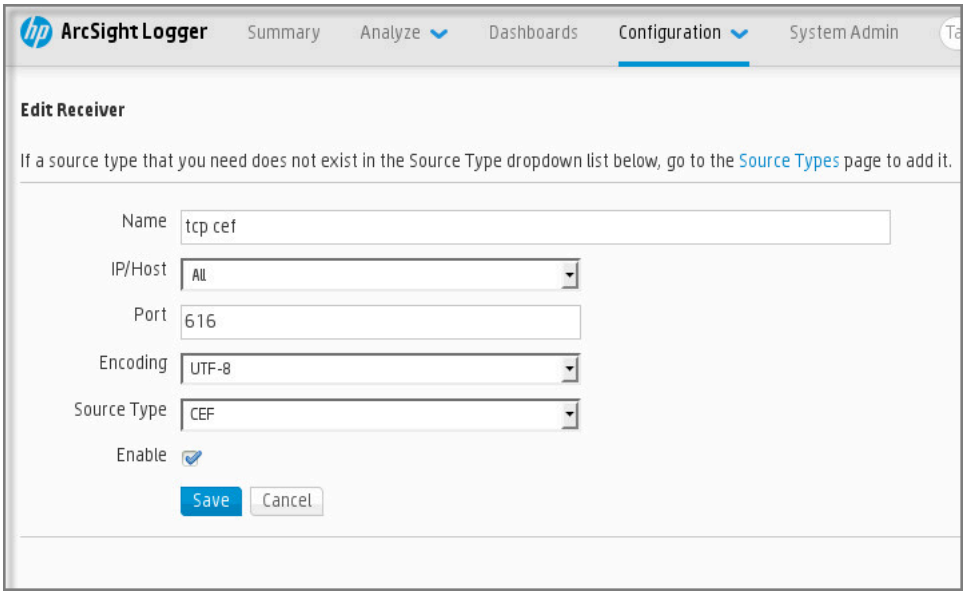
  Numer portu do nawiązana połączenia z Kaspersky Security Center. Ten port musi być taki sam, jak port, który określiłeś w Kaspersky Security Center.

- **Protokół wiadomości lub typ źródła**

  Protokół używany do eksportowania zdarzeń do systemu SIEM. Może to być jeden ze standardowych protokołów: Syslog, CEF lub LEEF. System SIEM wybiera analizatora wiadomości zgodnie z protokołem, który określiłeś.

W zależności od używanego systemu SIEM, konieczne może być określenie niektórych dodatkowych ustawień odbiorcy.

Poniższy rysunek przedstawia okno konfiguracji odbiorcy w ArcSight.



Konfiguracja odbiorcy w ArcSight

Analizator wiadomości

Wyeksportowane zdarzenia są przekazywane do systemu SIEM jako wiadomości. Te wiadomości muszą być odpowiednio przeanalizowane, aby informacje na temat zdarzeń mogły być użyte przez system SIEM. Analizatory wiadomości są częścią systemu SIEM; są używane do podzielenia zawartości wiadomości na odpowiednie pola, takie jak: identyfikator zdarzenia, priorytet, opis, parametry itd. Umożliwia to systemowi SIEM przetworzenie zdarzeń otrzymanych z Kaspersky Security Center tak, aby mogły być przechowywane w bazie danych systemu SIEM.

Oznaczenie zdarzeń do wyeksportowania do systemów SIEM w formacie Syslog

Po włączeniu automatycznego eksportowania zdarzeń, należy wskazać zdarzenia, które zostaną wyeksportowane do zewnętrznego systemu SIEM.

Możesz skonfigurować eksportowanie zdarzeń w formacie Syslog do zewnętrznego systemu w oparciu o jeden z następujących warunków:

- Oznaczanie zdarzeń ogólnych. Jeśli zdarzenia do wyeksportowania oznaczysz w zasadzie, w ustawieniach zdarzenia lub w ustawieniach Serwera administracyjnego system SIEM otrzyma oznaczone zdarzenia, które wystąpiły we wszystkich aplikacjach zarządzanych przez określoną zasadę. Jeśli wyeksportowane zdarzenia były wybrane w zasadzie, nie będziesz mógł ich ponownie zdefiniować dla aplikacji zarządzanej przez tą zasadę.

- Oznaczanie zdarzeń dla zarządzanej aplikacji. Jeśli oznaczysz zdarzenia do wyeksportowania dla zarządzanej aplikacji, zainstalowanej na zarządzanym urządzeniu, system SIEM otrzyma tylko zdarzenia, które wystąpiły w tej aplikacji.

Oznaczanie zdarzeń aplikacji Kaspersky do eksportu w formacie Syslog

Jeśli chcesz wyeksportować zdarzenia, które wystąpiły w pojedynczej zarządzanej aplikacji, zainstalowanej na zarządzanym urządzeniu, dla aplikacji oznacz zdarzenia do wyeksportowania. Jeśli poprzednio wyeksportowane zdarzenia były oznaczone w zasadzie, nie będziesz mógł ponownie zdefiniować oznaczonych zdarzeń dla pojedynczej aplikacji zarządzanej przez tę zasadę.

W celu oznaczenia zdarzeń do wyeksportowania dla pojedynczej zarządzanej aplikacji:

1. W drzewie konsoli Kaspersky Security Center wybierz węzeł **Zarządzane urządzenia** i przejdź na zakładkę **Urządzenia**.

2. Kliknij żądane urządzenie prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Właściwości**.

3. W otwartym oknie właściwości urządzenia wybierz sekcję **Aplikacje**.

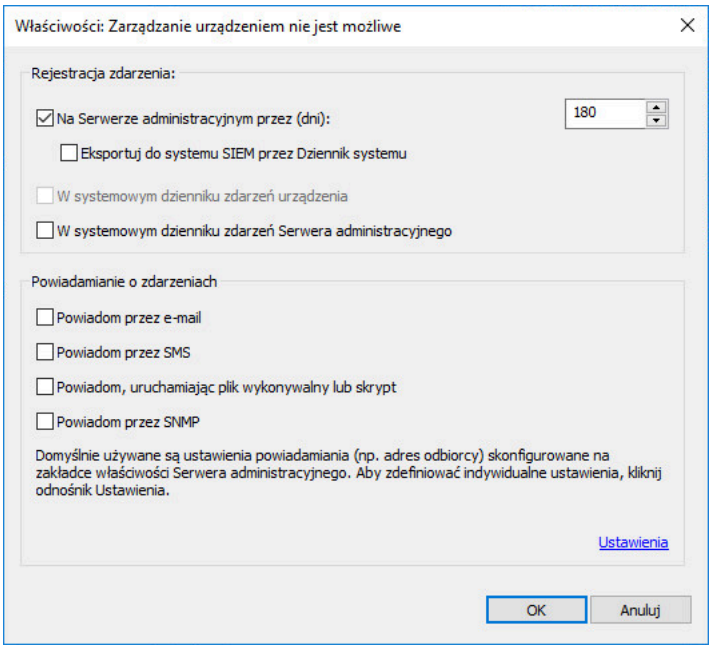
4. Na liście aplikacji, która zostanie wyświetlona, wybierz aplikację, której zdarzenia chcesz wyeksportować, i kliknij przycisk **Właściwości**.

5. W oknie właściwości aplikacji wybierz sekcję **Konfiguracja zdarzenia**.

6. Na liście zdarzeń, która zostanie wyświetlona, wybierz jedno lub kilka zdarzeń do wyeksportowania do systemu SIEM i kliknij przycisk **Właściwości**.

7. W wyświetlonym oknie właściwości zdarzeń zaznacz pole **Eksportuj do systemu SIEM przez Dziennik systemu**, aby zaznaczyć wybrane zdarzenia do eksportu w formacie Syslog. Odznacz pole **Eksportuj do systemu SIEM przez Dziennik systemu** wyboru, aby odznaczyć wybrane zdarzenia do eksportu w formacie Syslog.

Jeśli właściwości zdarzenia są zdefiniowane w zasadzie, pola w tym oknie nie mogą być modyfikowane.



Okno Właściwości zdarzenia

8. Kliknij **OK**, aby zachować zmiany.

9. Kliknij **OK** w oknie właściwości aplikacji i w oknie właściwości urządzenia.

Wybrane zdarzenia zostaną wysłane do systemu SIEM w formacie Syslog. Wydarzenia, dla których odznaczyłeś pole **Eksportuj do systemu SIEM przez Dziennik systemu**, nie zostaną wyeksportowane do systemu SIEM. Proces eksportowania rozpocznie się natychmiast po włączeniu automatycznego eksportowania i wybraniu zdarzeń do wyeksportowania. Skonfiguruj system SIEM, aby mógł otrzymywać zdarzenia z Kaspersky Security Center.

Oznaczanie ogólnych zdarzeń do eksportu w formacie Syslog

Jeśli chcesz wyeksportować zdarzenia, które wystąpiły we wszystkich aplikacjach zarządzanych przez określoną zasadę, w zasadzie wybierz zdarzenia do wyeksportowania. W tym przypadku nie będziesz mógł wybrać zdarzeń dla pojedynczej zarządzanej aplikacji.

W celu oznaczenia zdarzeń ogólnych do wyeksportowania do systemu SIEM:

1. W drzewie konsoli Kaspersky Security Center wybierz węzeł **Zasady**.

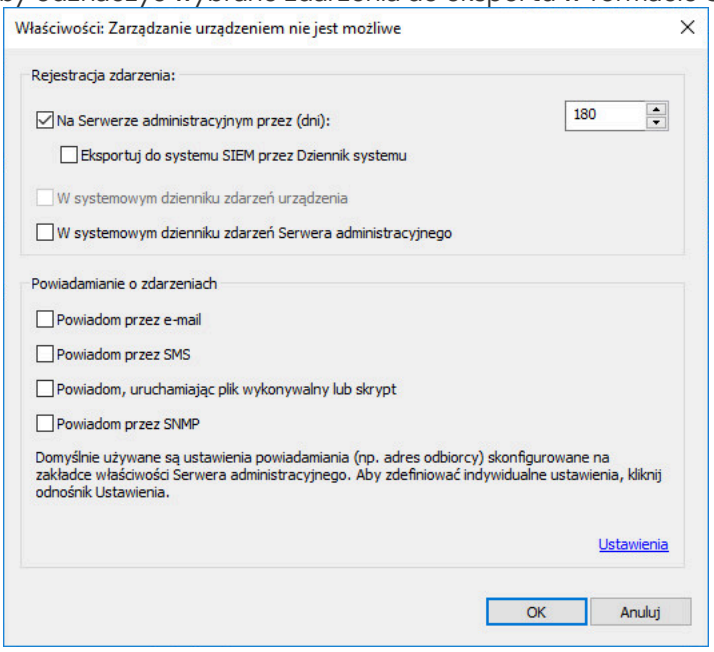
2. Kliknij żądaną zasadę prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Właściwości**.

3. W otwartym oknie właściwości zasady wybierz sekcję **Konfiguracja zdarzenia**.

4. Na liście zdarzeń, która zostanie wyświetlona, wybierz jedno lub kilka zdarzeń do wyeksportowania do systemu SIEM i kliknij przycisk **Właściwości**.

   Jeśli chcesz wybrać wszystkie zdarzenia, kliknij przycisk **Wybierz wszystkie**.

5. W wyświetlonym oknie właściwości zdarzeń zaznacz pole **Eksportuj do systemu SIEM przez Dziennik systemu**, aby zaznaczyć wybrane zdarzenia do eksportu w formacie Syslog. Odznacz pole **Eksportuj do systemu SIEM przez Dziennik systemu**, aby odznaczyć wybrane zdarzenia do eksportu w formacie Syslog.



Okno właściwości zdarzenia Serwera administracyjnego

6. Kliknij **OK**, aby zachować zmiany.

7. W oknie właściwości zasady kliknij **OK**.

Wybrane zdarzenia zostaną wysłane do systemu SIEM w formacie Syslog. Wydarzenia, dla których odznaczyłeś pole **Eksportuj do systemu SIEM przez Dziennik systemu**, nie zostaną wyeksportowane do systemu SIEM. Proces eksportowania rozpocznie się natychmiast po włączeniu automatycznego eksportowania i wybraniu zdarzeń do wyeksportowania. Skonfiguruj system SIEM, aby mógł otrzymywać zdarzenia z Kaspersky Security Center.

Informacje dotyczące eksportowania zdarzeń przy użyciu formatu Syslog

Możesz użyć formatu Syslog do wyeksportowania do systemów SIEM zdarzeń, które występują na Serwerze administracyjnym i w innych aplikacjach firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach.

Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Pozwala on na rozdzielenie oprogramowania, które generuje wiadomości, systemu, które je przechowuje, oraz oprogramowania, które raportuje i analizuje te wiadomości. Do każdej wiadomości przypisywany jest kod funkcji, wskazujący typ oprogramowania, które generuje wiadomość, oraz priorytet.

Format Syslog jest definiowany przez dokumenty RFC (Request for Comments — prośba o komentarze), publikowane przez Internet Engineering Task Force (standardy internetowe). Standard RFC 5424 jest używany do eksportowania zdarzeń z Kaspersky Security Center do systemów zewnętrznych.

W Kaspersky Security Center możesz skonfigurować eksportowanie zdarzeń do systemów zewnętrznych przy użyciu formatu Syslog.

Proces eksportowania składa się z dwóch etapów:

1. Włączanie automatycznego eksportowania zdarzeń. W tym kroku program Kaspersky Security Center jest konfigurowany tak, aby wysyłał zdarzenia do systemu SIEM. Kaspersky Security Center rozpoczyna wysyłanie zdarzeń natychmiast po włączeniu automatycznego eksportowania.

2. Wybieranie zdarzeń eksportowanych do systemu zewnętrznego. W tym kroku wybierasz zdarzenia, które będą eksportowane do systemu SIEM.

Informacje dotyczące eksportowania zdarzeń przy użyciu formatów CEF i LEEF

Możesz użyć formatów CEF i LEEF, aby wyeksportować ogólne zdarzenia do systemów SIEM, a także zdarzenia przesyłane przez aplikacje Kaspersky do Serwera administracyjnego. Zestaw eksportowanych zdarzeń jest predefiniowany i nie możesz wybrać zdarzeń do wyeksportowania. Przed wysłaniem zdarzeń do systemu SIEM (QRadar, ArcSight lub Splunk) konieczna jest interpretacja zdarzeń Kaspersky Security Center jako zdarzeń w formacie CEF i LEEF przy użyciu reguł określonych w pliku siem_conversion_rules.xml.

Wybierz format eksportowania w oparciu o używany system SIEM. Poniższa tabela wyświetla systemy SIEM i odpowiadające im formaty eksportu.

Formaty eksportowania zdarzenia do systemu SIEM

System SIEM	Format eksportu
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) - dostosowany format zdarzeń dla IBM Security QRadar SIEM. QRadar może integrować, identyfikować i przetwarzać zdarzenia LEEF. Zdarzenia LEEF muszą używać kodowania UTF-8. Szczegółowe informacje na temat protokołu LEEF można znaleźć w Centrum wiedzy IBM.

- CEF (Common Event Format)—standard zarządzania dziennikami, który ulepsza współdziałanie zdarzeń dotyczących bezpieczeństwa między różnymi urządzeniami i aplikacjami sieciowymi i zabezpieczającymi. CEF umożliwia korzystanie z podstawowego formatu dziennika zdarzeń, co ułatwia integrowanie i gromadzenie danych do analizy przez system zarządzania korporacji. Zdarzenia CEF muszą używać kodowania UTF-8.

Automatyczne eksportowanie oznacza, że Kaspersky Security Center wysyła ogólne zdarzenia do systemu SIEM. Automatyczne eksportowanie zdarzeń rozpoczyna się od razu po włączeniu tej opcji. Ta sekcja szczegółowo wyjaśnia, jak włączyć automatyczne eksportowanie zdarzeń.

Konfigurowanie Kaspersky Security Center do wyeksportowania zdarzeń do systemu SIEM

Możesz włączyć automatyczne eksportowanie zdarzeń w Kaspersky Security Center.

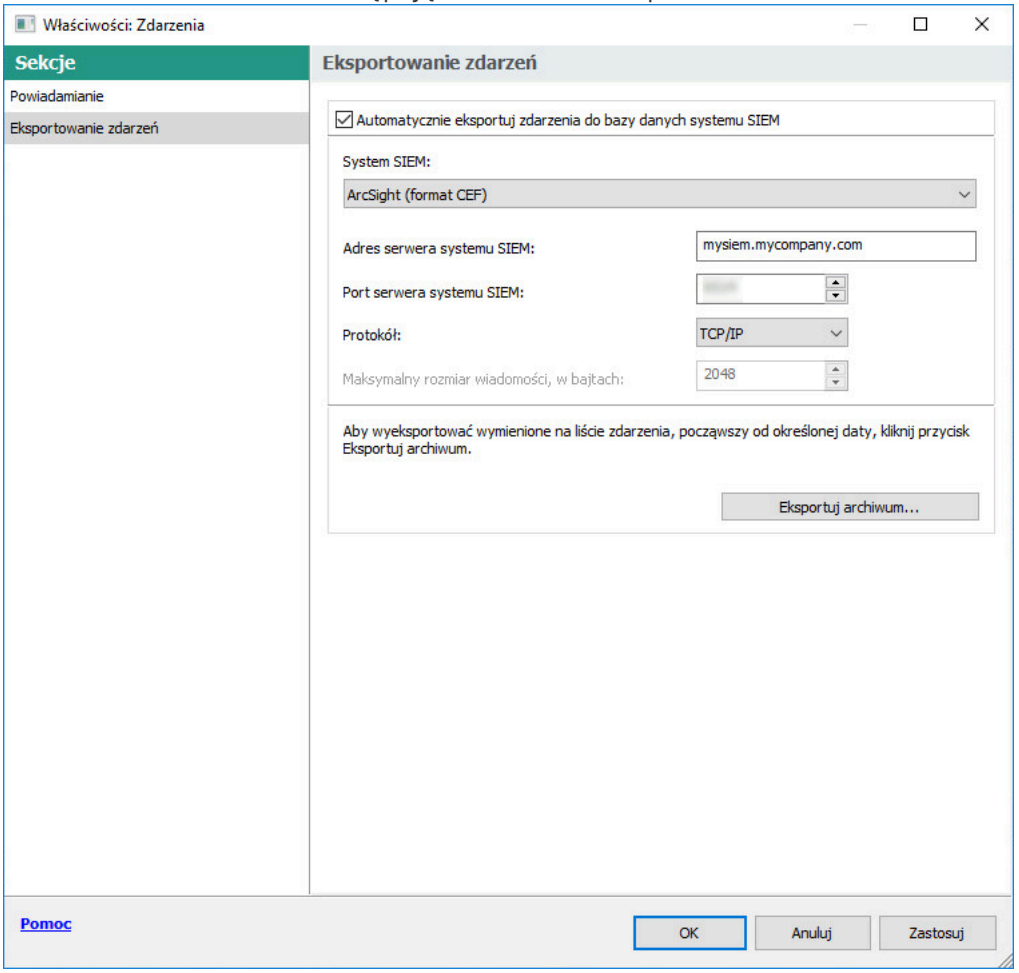
Tylko zdarzenia ogólne mogą być eksportowane z zarządzanych aplikacji w formatach CEF i LEEF. Reguły interpretacji służące do konwersji zdarzeń do formatów CEF i LEEF są określone w pliku siem_conversion_rules.xml znajdującym się w pakiecie dystrybucyjnym Kaspersky Security Center. Zdarzenia specyficzne dla aplikacji nie mogą być eksportowane z zarządzanych aplikacji w formatach CEF i LEEF. Jeśli chcesz wyeksportować zdarzenia zarządzanych aplikacji lub niestandardowy zestaw zdarzeń, który został skonfigurowany przy użyciu zasad zarządzanych aplikacji, wyeksportuj zdarzenia w formacie Syslog.

W celu włączenia automatycznego eksportowania zdarzeń:

1. W drzewie konsoli Kaspersky Security Center wybierz Serwer administracyjny, którego zdarzenia chcesz wyeksportować.
2. W obszarze roboczym wybranego Serwera administracyjnego wybierz zakładkę **Zdarzenia**.
3. Kliknij strzałkę rozwijalną znajdującą się obok odnośnika **Konfiguruj powiadomienia i eksportowanie zdarzeń** i z listy rozwijalnej wybierz **Konfiguruj eksportowanie do SIEM**.

   Okno właściwości zdarzeń zostanie otwarte na sekcji **Eksportowanie zdarzeń**.

4. W sekcji **Eksportowanie zdarzeń** określ następujące ustawienia eksportowania:



Sekcja Eksportowanie zdarzeń w oknie właściwości zdarzeń

- **Automatycznie eksportuj zdarzenia do bazy danych systemu SIEM**

  Zaznacz to pole, aby włączyć automatyczne eksportowanie zdarzeń do systemów SIEM. Zaznaczenie tego pola włącza wszystkie pola w sekcji **Eksportowanie zdarzeń**.

- **System SIEM**

  Wybierz system SIEM, do którego zostaną wyeksportowane zdarzenia: QRadar® (format LEEF), ArcSight (format CEF), Splunk® (format CEF) i format Syslog (RFC 5424).

  Jeśli wybierzesz format Syslog, musisz określić:

  Maksymalny rozmiar wiadomości, w bajtach

  Określ maksymalny rozmiar (w bajtach) jednej wiadomości przekazywanej do systemu SIEM. Każde zdarzenie jest przesyłane w jednej wiadomości. Jeśli rzeczywisty rozmiar wiadomości przekracza określoną wartość, wiadomość jest skracana i dane mogą zostać utracone. Domyślny rozmiar to 2048 bajtów. To pole jest dostępne tylko wtedy, gdy w polu **System SIEM** wybrałeś format dziennika systemu.

- **Adres serwera systemu SIEM**

  Określ adres serwera systemu SIEM. Adres można określić jako nazwę DNS lub NetBIOS lub jako adres IP.

- **Port serwera systemu SIEM**

  Określ numer portu używanego do nawiązywania połączenia z serwerem systemu SIEM. Ten numer portu musi być taki sam, jak ten, którego Twój system SIEM używa do pobierania zdarzeń (więcej informacji można znaleźć w sekcji Konfigurowanie systemu SIEM).

- **Protokół**

  Wybierz protokół, który będzie używany do przesyłania wiadomości do systemu SIEM. Możesz wybrać protokół TCP, UDP lub TLS poprzez protokół TCP.

  Określ następujące ustawienia TLS, jeśli wybierzesz TLS poprzez protokół TCP:

  - **Uwierzytelnianie serwera SIEM**

    Wybierz jeden z poniższych sposobów uwierzytelnienia serwera systemu SIEM:

    - **Używając certyfikatów urzędu certyfikacji** Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji (CA) i przesłać go do Kaspersky Security Center. Kaspersky Security Center sprawdza, czy certyfikat serwera systemu SIEM jest również podpisany przez zaufany urząd certyfikacji, czy nie.

      Aby dodać zaufany certyfikat, kliknij przycisk **Przeglądaj**, a następnie prześlij certyfikat.

      W przypadku wybrania opcji **Używając certyfikatów urzędu certyfikacji** można określić nazwy podmiotów w polu **Podmioty certyfikatów serwera (opcjonalnie)**. *Nazwa podmiotu* to nazwa domeny, dla której otrzymano certyfikat. Kaspersky Security Center nie może połączyć się z serwerem systemu SIEM, jeśli nazwa domeny serwera systemu SIEM nie jest zgodna z nazwą podmiotu certyfikatu serwera systemu SIEM. Jednak serwer systemu SIEM może zmienić swoją nazwę domeny, jeśli zmienisz nazwę w certyfikacie. W tym celu określ nazwy podmiotów w polu **Podmioty certyfikatów serwera (opcjonalnie)** (opcjonalnie). Jeśli dowolna z podanych nazw podmiotów odpowiada nazwie podmiotu certyfikatu systemu SIEM, Kaspersky Security Center zweryfikuje certyfikat serwera systemu SIEM.

    - **Korzystając z odcisków palców SHA1 certyfikatów serwera** Możesz określić odciski palców SHA-1 certyfikatów systemu SIEM w Kaspersky Security Center. Aby dodać odcisk palca SHA-1, wprowadź go w polu pod opcją.

  - **Uwierzytelnianie klienta**

W celu uwierzytelnienia klienta możesz wstawić swój certyfikat lub wygenerować go w Kaspersky Security Center.

- **Wstaw certyfikat**. Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Aby wstawić istniejący certyfikat, kliknij przycisk **Wybierz certyfikat**. W otwartym oknie **Certyfikat** wybierz jeden z poniższych typów certyfikatów, a następnie określ certyfikat i jego klucz prywatny:

  - **Certyfikat X.509**. Prześlij plik z kluczem prywatnym w polu **Klucz prywatny (*.prk, *.pem)** oraz plik z certyfikatem w polu **Certyfikat(*.cer)**. W tym celu kliknij przycisk **Przeglądaj** po prawej stronie odpowiedniego pola, a następnie dodaj wymagany plik. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po przesłaniu obu plików określ hasło do dekodowania klucza prywatnego w polu **Hasło**. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

  - **Kontener PKCS #12**. Prześlij pojedynczy plik zawierający certyfikat i jego klucz prywatny w polu **Plik certyfikatu**. W tym celu kliknij przycisk **Przeglądaj** po prawej stronie odpowiedniego pola, a następnie dodaj wymagany plik. Po przesłaniu pliku określ hasło do dekodowania klucza prywatnego w polu **Hasło**. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

- **Wygeneruj klucz**. Możesz wygenerować certyfikat z podpisem własnym w Kaspersky Security Center. Kliknij przycisk **Wygeneruj certyfikat**, a następnie wprowadź nazwę podmiotu w polu **Temat**. Certyfikat klienta jest generowany dla tej nazwy podmiotu, a odcisk palca SHA-1 tego certyfikatu jest wyświetlany w polu **Odcisk palca SHA1 certyfikatu klienta**. W rezultacie Kaspersky Security Center przechowuje wygenerowany samopodpisany certyfikat i możesz przekazać publiczną część certyfikatu lub odcisk palca SHA-1 do systemu SIEM.

5. Jeśli chcesz wyeksportować do bazy danych systemu SIEM zdarzenia, które wystąpiły po określonej dacie w przeszłości, kliknij przycisk **Eksportuj archiwum** i określ datę początkową dla eksportowania zdarzeń. Domyślnie, eksportowanie zdarzeń rozpoczyna się od razu po włączeniu tej opcji.

6. Aby sprawdzić, czy połączenie z systemem SIEM zostało pomyślnie skonfigurowane, kliknij przycisk **Sprawdź ustawienia**.

   Aplikacja spróbuje nawiązać połączenie z serwerem systemu SIEM i wysłać zdarzenie testowe. Jeżeli połączenie nie zostanie nawiązane, wyświetlony zostanie komunikat o błędzie. Jeśli połączenie zostanie nawiązane, nie zostanie wyświetlony żaden komunikat. W razie potrzeby możesz wyświetlić zdarzenie testowe na karcie **Zdarzenia**.

7. Kliknij **OK**.

Automatyczne eksportowanie zdarzeń jest włączone.

Po włączeniu automatycznego eksportowania zdarzeń, należy wskazać zdarzenia, które zostaną wyeksportowane do systemu SIEM.

Eksportowanie zdarzeń bezpośrednio z bazy danych

Zdarzenia można otrzymywać bezpośrednio z bazy danych Kaspersky Security Center bez konieczności korzystania z interfejsu Kaspersky Security Center. Możesz wykonać zapytanie bezpośrednio do widoków publicznych i pobrać dane zdarzenia lub utworzyć swoje własne widoki w oparciu o istniejące widoki publiczne i adresować je w celu otrzymania żądanych danych.

Widoki publiczne

Dla Twojej wygody, w bazie danych Kaspersky Security Center dostępny jest zestaw widoków publicznych. Opis tych widoków publicznych można znaleźć w dokumentacji klakdb.chm.

Widok publiczny v_akpub_ev_event zawiera zestaw pól, które reprezentują parametry zdarzenia w bazie danych. W dokumencie klakdb.chm możesz także znaleźć informacje dotyczące widoków publicznych odpowiadających innym obiektom Kaspersky Security Center, na przykład: urządzeniom, aplikacjom lub użytkownikom. Możesz użyć tych informacji w swoich zapytaniach.

Ta sekcja zawiera instrukcje dotyczące tworzenia zapytania SQL przy użyciu narzędzia klsql2 oraz przykłady zapytań.

Aby utworzyć zapytania SQL lub widoki bazy danych, możesz także użyć innego dowolnego programu do pracy z bazami danych. Informacje dotyczące przeglądania parametrów połączenia z bazą danych Kaspersky Security Center, takich jak nazwa instancji i nazwa bazy danych, znajdują się w odpowiedniej sekcji.

Tworzenie zapytania SQL przy użyciu narzędzia klsql2

Ten artykuł opisuje sposób pobierania i korzystania z narzędzia klsql2, a także sposób tworzenia zapytań SQL przy użyciu tego narzędzia.

W celu użycia narzędzia klsql2:

1. Zlokalizuj narzędzie klsql2 w folderze instalacyjnym Kaspersky Security Center. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Nie używaj wersji narzędzia klsql2 przeznaczonych dla starszych wersji Kaspersky Security Center.

2. Utwórz plik .sql w dowolnym edytorze tekstu i umieść plik w tym samym folderze co narzędzie.

3. W pliku .sql wpisz typ żądanego zapytania SQL, a następnie zapisz plik.

4. Na urządzeniu z zainstalowanym Serwerem administracyjnym Kaspersky Security Center, w wierszu polecenia wpisz następujące polecenie do uruchomienia zapytania SQL z pliku .sql i zapisz wyniki do pliku result.xml:
   ```
   klsql2 -i src.sql -u <nazwa użytkownika> -p <hasło> -o result.xml
   ```
   gdzie `<nazwa użytkownika>` i `<hasło>` to poświadczenia konta użytkownika, który ma dostęp do bazy danych.

5. W razie potrzeby wprowadź login i hasło konta użytkownika, który ma dostęp do bazy danych.

6. Otwórz nowo utworzony plik result.xml, aby wyświetlić wyniki zapytania SQL.

Możesz zmodyfikować plik .sql i utworzyć dowolne zapytanie SQL do widoków publicznych. Następnie, z poziomu wiersza poleceń, wykonaj zapytanie SQL i zapisz wyniki do pliku.

Przykład zapytania SQL w narzędziu klsql2

W tej sekcji przedstawiono przykład zapytania SQL tworzonego przy użyciu narzędzia klsql2.

Poniższe przykłady ilustrują otrzymanie zdarzeń, które wystąpiły na urządzeniach w ciągu ostatnich siedmiu dni, oraz wyświetlenie zdarzeń według czasu ich wystąpienia. Najnowsze zdarzenia są wyświetlane jako pierwsze.

Przykład dla Microsoft SQL Server:

```
SELECT
  /* identyfikator zdarzenia */
  e.nId,

  /* godzina wystąpienia zdarzenia */
  e.tmRiseTime,

  /* wewnętrzna nazwa typu zdarzenia */
  e.strEventType,

  /* wyświetlona nazwa zdarzenia */
  e.wstrEventTypeDisplayName,

  /* wyświetlony opis zdarzenia */
  e.wstrDescription,

  /* nazwa grupy, w której znajduje się zdarzenie */
  e.wstrGroupName,

  /* wyświetlona nazwa urządzenia, na którym wystąpiło zdarzenie */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* adres IP urządzenia, na którym wystąpiło zdarzenie */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Przykład dla PostgreSQL:

```
SELECT
  /* identyfikator zdarzenia */
  "e"."nId",

  /* godzina wystąpienia zdarzenia */
  "e"."tmRiseTime",

  /* wewnętrzna nazwa typu zdarzenia */
  "e"."strEventType",

  /* wyświetlona nazwa zdarzenia */
  "e"."wstrEventTypeDisplayName",

  /* wyświetlony opis zdarzenia */
  "e"."wstrDescription",

  /* wyświetlony opis zdarzenia */
  "e"."wstrGroupName",

  /* wyświetlona nazwa urządzenia, na którym wystąpiło zdarzenie */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* adres IP urządzenia, na którym wystąpiło zdarzenie */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Przykład dla MySQL lub MariaDB:

```
SELECT

  /* identyfikator zdarzenia */
  `e`.`nId`,

  /* godzina wystąpienia zdarzenia */
  `e`.`tmRiseTime`,

  /* wewnętrzna nazwa typu zdarzenia */
  `e`.`strEventType`,

  /* wyświetlona nazwa zdarzenia */
  `e`.`wstrEventTypeDisplayName`,

  /* wyświetlony opis zdarzenia */
  `e`.`wstrDescription`,

  /* nazwa grupy urządzeń */
  `e`.`wstrGroupName`,

  /* wyświetlona nazwa urządzenia, na którym wystąpiło zdarzenie */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* adres IP urządzenia, na którym wystąpiło zdarzenie */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Sprawdzanie nazwy bazy danych Kaspersky Security Center

Znajomość nazwy bazy danych może być pomocna, jeśli na przykład trzeba wysłać zapytanie SQL i połączyć się z bazą danych z edytora skryptów SQL.

W celu wyświetlenia nazwy bazy danych Kaspersky Security Center:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.

2. W oknie właściwości Serwera administracyjnego, w panelu Sekcje wybierz **Zaawansowane**, a następnie **Szczegóły bieżącej bazy danych**.

3. W sekcji **Szczegóły bieżącej bazy danych** zwróć uwagę na następujące właściwości bazy danych (patrz rysunek poniżej):

   - **Nazwa instancji**

     Nazwa bieżącej instancji bazy danych Kaspersky Security Center. Domyślna wartość to *.\KAV_CS_ADMIN_KIT*.

   - **Nazwa bazy danych**

     Nazwa bazy danych SQL Kaspersky Security Center. Domyślna wartość to *KAV*.

- **Miejsce przeznaczone na bazę danych Kaspersky Security Center**

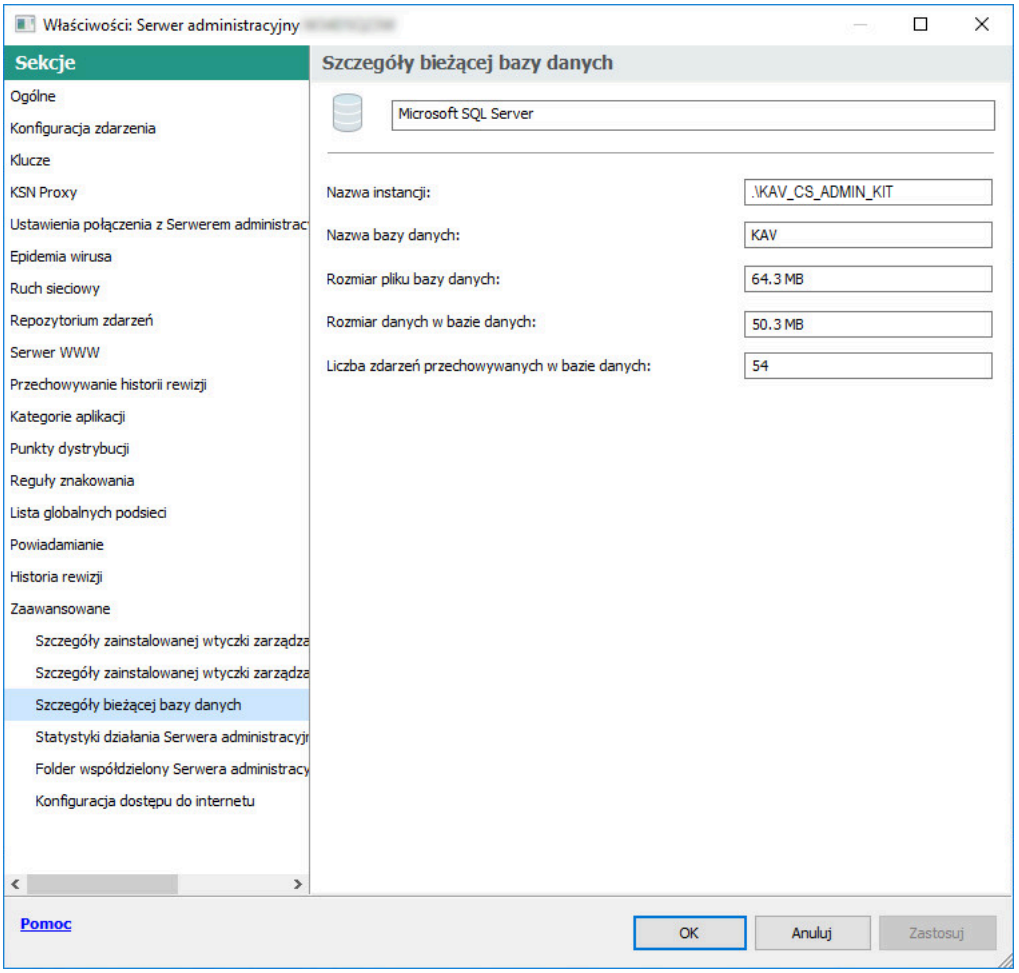
  Rozmiar pliku bazy danych. Jeśli chcesz usunąć niepotrzebne dane, skonfiguruj kompresję bazy danych za pomocą zadania *Konserwacja Serwera administracyjnego*.

- **Rozmiar danych w całej bazie danych**

  Rzeczywisty rozmiar danych obecnie używanych w systemie DBMS. W poniższym artykule opisano sposób diagnozowania systemu DBMS: Rozmiar bazy danych przekracza limit.

- **Liczba zdarzeń przechowywanych w bazie danych**

  Liczba zdarzeń aktualnie przechowywanych w systemie DBMS. Więcej szczegółów można znaleźć w poniższym artykule: Przetwarzanie i przechowywanie zdarzeń.



Sekcja z informacjami o bieżącej bazie danych Serwera administracyjnego

4. Kliknij przycisk **OK**, aby zamknąć okno właściwości Serwera administracyjnego.

Użyj nazwy bazy danych, aby adresować bazę danych w swoich zapytaniach SQL.

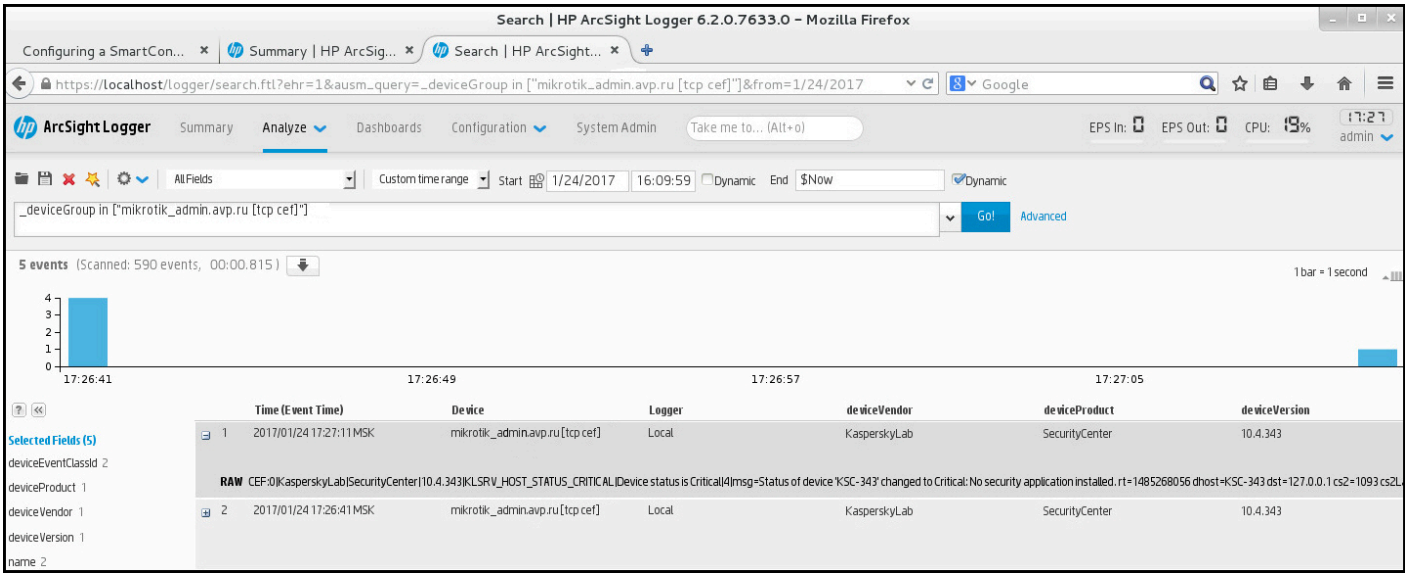
Przeglądanie wyników eksportowania

Możesz kontrolować pomyślne zakończenie procedury eksportowania zdarzeń. W tym celu sprawdź, czy wiadomości z eksportowanymi zdarzeniami są otrzymywane przez Twój system SIEM.

Jeśli zdarzenia wysłane z Kaspersky Security Center są odbierane i poprawnie analizowane przez Twój system SIEM, konfiguracja po obu stronach została przeprowadzona właściwie. Jeśli jest inaczej, sprawdź ustawienia, które określiłeś w Kaspersky Security Center, porównując je z konfiguracją w Twoim systemie SIEM.

Poniższy rysunek przedstawia zdarzenia wyeksportowane do ArcSight. Na przykład, pierwsze zdarzenie jest krytycznym zdarzeniem Serwera administracyjnego: „*Urządzenie posiada stan Krytyczny*”.

Reprezentacja eksportowania zdarzeń w systemie SIEM różni się w zależności od tego, którego systemu SIEM używasz.



Przykład zdarzeń

Używanie protokołu SNMP do wysyłania statystyk do aplikacji firm trzecich

Ta sekcja opisuje sposób pobierania informacji z Serwera administracyjnego przy użyciu protokołu SNMP (Simple Network Management Protocol) w systemie Windows. Kaspersky Security Center zawiera agenta SNMP, który przesyła statystyki działania Serwera administracyjnego do innych aplikacji przy użyciu identyfikatorów OID.

Ta sekcja zawiera również informacje o rozwiązywaniu problemów, które można napotkać podczas używania protokołu SNMP w przypadku Kaspersky Security Center.

Konfigurowanie usługi SNMP do użytku z Kaspersky Security Center

Ta sekcja opisuje jak skonfigurować usługę SNMP w systemie Windows, aby pobierała informacje z serwera administracyjnego przy użyciu protokołu SNMP (Simple Network Management Protocol).

Obsługa protokołu SNMP jest domyślnie wyłączona w systemie Windows.

Aby włączyć obsługę protokołu SNMP w systemie Windows:

1. Przejdź do **Panelu sterowania**.
2. Otwórz menu **Dodaj lub usuń programy**.
3. Kliknij opcję **Włącz lub wyłącz funkcje systemu Windows**.

4. Na liście funkcji systemu Windows przejdź do funkcji SNMP, a następnie kliknij przycisk **OK**.

5. Przejdź do **Panel sterowania** → **Narzędzia administracyjne** → **Usługi**.

6. Wybierz **usługę SNMP** i uruchom ją.

7. Sprawdź, czy nasłuchiwanie działa, testując je za pomocą polecenia `netstat` w przypadku standardowego portu UDP.

Obsługa protokołu SNMP jest włączona w systemie Windows.

Aby skonfigurować usługi SNMP w systemie Windows:

1. Upewnij się, że podczas zwykłej lub cichej instalacji został zainstalowany komponent **Agent SNMP** Kaspersky Security Center.

2. Upewnij się, że usługi Windows **SNMP Service** i **SNMP Trap** są uruchomione.

3. Upewnij się, że w systemie zainstalowana jest przeglądarka ManageEngine MIB Browser.

4. We właściwościach usługi **SNMP Service**, w zakładce **Bezpieczeństwo** dodaj dwie społeczności z następującymi uprawnieniami:

Społeczność	Uprawnienia
`kaspersky`	`POWIADOMIENIA`
`public`	`ODCZYT/ZAPIS`

5. W polu **Akceptuj pakiety SNMP od tych hostów** dodaj adres IP urządzenia, na którym zainstalowana jest przeglądarka ManageEngine MIB Browser, na przykład 10.10.10.105.

6. W zakładce **Traps** wpisz `kaspersky` w polu **Nazwa społeczności**.

7. Aby zapisać wprowadzone zmiany i zamknąć okno właściwości usługi, kliknij **OK**.

8. W przeglądarce ManageEngine MIB załaduj plik adminkit.mib z folderu instalacyjnego Kaspersky Security Center. Domyślnie plik adminkit.mib znajduje się w folderze <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp.

9. W polu **Host** okna przeglądarki ManageEngine MIB dodaj adres IP urządzenia, na którym jest zainstalowany serwer administracyjny Kaspersky Security Center.

Usługa SNMP jest skonfigurowana do pobierania informacji z serwera administracyjnego przy użyciu protokołu SNMP (Simple Network Management Protocol).

Agent SNMP i identyfikatory obiektów

W przypadku Kaspersky Security Center agent SNMP jest zaimplementowany jako dynamiczna biblioteka `klsnmpag.dll`, która jest rejestrowana przez instalator podczas instalacji Serwera administracyjnego. Agent SNMP działa w procesie `snmp.exe` (jest to usługa systemu Windows). Aplikacje firm trzecich używają protokołu SNMP do odbierania statystyk (w postaci liczników) dotyczących działania Serwera administracyjnego.

Każdy licznik ma unikatowy *identyfikator obiektu* (nazywany również OID). Identyfikator obiektu to sekwencja liczb podzielonych kropkami. Identyfikatory obiektów Serwera administracyjnego zaczynają się od przedrostka 1.3.6.1.4.1.23668.1093. Identyfikator OID licznika jest połączeniem tego prefiksu z sufiksem opisującym licznik. Na przykład licznik o wartości OID 1.3.6.1.4.1.23668.1093.1.1.4 ma sufiks o wartości 1.1.4.

Możesz użyć klienta SNMP (takiego jak Zabbix) do monitorowania stanu Twojego systemu. Aby uzyskać informacje, możesz wyszukać wartość OID, która odpowiada informacjom i wprowadzić tę wartość do klienta SNMP. Wówczas Twój klient SNMP zwróci inną wartość, która charakteryzuje stan Twojego systemu.

Lista liczników i typów liczników znajduje się w pliku `adminkit.mib` na Serwerze administracyjnym. *MIB* to skrót od Management Information Base (baza informacji zarządzania). Pliki `.mib` można importować i analizować za pomocą aplikacji MIB Viewer, która służy do wysyłania zapytań o wartości liczników i ich wyświetlania.

Uzyskiwanie nazwy licznika ciągu znaków z identyfikatora obiektu

Aby użyć identyfikatora obiektu (OID) do przesyłania informacji do aplikacji firm trzecich, konieczne może być uzyskanie nazwy licznika ciągu znaków z tego identyfikatora obiektu.

W celu uzyskania nazwy licznika ciągu znaków z identyfikatora obiektu:

1. Otwórz plik `adminkit.mib`, który znajduje się na Serwerze administracyjnym, w edytorze tekstu.
2. Znajdź przestrzeń nazw opisującą pierwszą wartość (od lewej do prawej).

   Na przykład, dla sufiksu identyfikatora OID 1.1.4 będzie to `"counters" (::= { kladminkit 1 })`.
3. Znajdź przestrzeń nazw opisującą drugą wartość.

   Na przykład, dla sufiksu identyfikatora OID 1.1.4 będzie to `counters 1`, co oznacza `deployment`.
4. Znajdź przestrzeń nazw opisującą trzecią wartość.

   Na przykład, dla sufiksu identyfikatora OID 1.1.4 będzie to `deployment 4`, co oznacza `hostsWithAntivirus`.

Nazwa licznika ciągu znaków to połączenie tych wartości, na przykład `<MIB base namespace>.counters.deployment.hostsWithAntivirus` i odpowiada on identyfikatorowi OID o wartości 1.3.6.1.4.1.23668.1093.1.1.4.

Wartości identyfikatorów obiektów dla SNMP

Poniższa tabela przedstawia wartości i opisy identyfikatorów obiektów (OID), które są używane do przesyłania informacji o działaniu Serwera administracyjnego do aplikacji firm trzecich.

Wartość identyfikatora obiektu	Typ danych numerycznych	Identyfikator OID	Opis
deploymentStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.1.1	Stan wdrożenia. Stan może być jednym z następujących: • **Informacja**. Licencja nie jest już ważna dla N urządzeń. • **Ostrzeżenie**. Jeden z następujących: Istnieje M urządzeń z aplikacjami Kaspersky zainstalowanymi na łącznie N urządzeniach w grupach Serwera administracyjnego (N > M). Licencja L utraci ważność na N urządzeniach za M dni. Zadanie T instalacji aplikacji zostało pomyślnie zakończone na N urządzeniach, dla M urządzeń konieczne jest ponowne uruchomienie. • **Krytyczne**. Licencja utraciła ważność dla N urządzeń. • **OK**. Żadne z powyższych.
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.1	deploymentStatus wskazuje, że grupa Serwera administracyjnego zawiera zbyt wiele urządzeń bez zarządzanych aplikacji. Wartość jest równa 1 w przypadku wykrycia kilku urządzeń bez zarządzanych aplikacji, i 0 w innym przypadku.
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.2	deploymentStatus wskazuje, że zadanie zdalnej instalacji nie powiodło się na niektórych urządzeniach. Liczbę tych urządzeń można uzyskać za pośrednictwem wartości hostsRemoteInstallFailed.
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.3	deploymentStatus wskazuje, że istnieją urządzenia, dla których licencja utraci ważność w ciągu następnych 7 dni. Liczbę tych urządzeń można uzyskać za pośrednictwem wartości hostsLicenseExpiring.
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.4	deploymentStatus wskazuje, że istnieją urządzenia z licencją, która utraciła ważność. Liczbę tych urządzeń można uzyskać za pośrednictwem hostsLicenseExpired.
hostsInGroups	Counter32	.1.3.6.1.4.1.23668.1093.1.1.3	Liczba urządzeń w grupach Serwera administracyjnego.
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.23668.1093.1.1.4	Liczba urządzeń w grupach Serwera administracyjnego z zainstalowanymi zarządzanymi aplikacjami.
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.23668.1093.1.1.5	Liczba urządzeń, na których zadanie zdalnej instalacji nie powiodło się.
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.6	Identyfikator klucza licencyjnego, który utraci ważność za mniej niż 7 dni.
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.7	Identyfikator wygasłego klucza licencyjnego.
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.23668.1093.1.1.8	Liczba dni pozostałych do utraty ważności licencji. Dla tego parametru okres licencji uważa się za wygasły, jeśli do daty wygaśnięcia pozostało mniej niż 7 dni. Jeśli do daty wygaśnięcia pozostało więcej niż 7 dni, wartość wynosi 0.
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	Liczba urządzeń z licencją, która wygaśnie za mniej niż 7 dni.
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	Liczba urządzeń z licencją, która utraciła ważność.

Wartość identyfikatora obiektu	Typ danych numerycznych	Identyfikator OID	Opis
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	Aktualny stan aktualizacji antywirusowych baz danych. Stan może być jednym z następujących: • **Informacja**. Bazy antywirusowe na serwerze administracyjnym lub na urządzeniach nie były aktualizowane dłużej niż 1 dzień, a od instalacji aplikacji upłynął mniej niż 1 dzień. • **Ostrzeżenie**. Bazy antywirusowe na serwerze administracyjnym lub na urządzeniach nie były aktualizowane dłużej niż 3 dni. Wartość tę można zmienić w ustawieniach grupy. • **Krytyczne**. Bazy antywirusowe na serwerze administracyjnym lub na urządzeniach nie były aktualizowane dłużej niż 7 dni. Wartość tę można zmienić w ustawieniach grupy. • **OK**. Żadne z powyższych.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	Serwer administracyjny nie był aktualizowany przez długi czas. Okres uważany za długi jest określony w wartości updatesStatus.
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	Niektóre urządzenia nie były aktualizowane przez długi czas (domyślnie 7 dni lub więcej w przypadkach **krytycznych** i 3 dni w przypadku **ostrzeżenia**). Liczbę tych urządzeń można uzyskać za pośrednictwem hostsNotUpdated.
lastServerUpdateTime	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.2.3	Ostatni raz, kiedy antywirusowe bazy danych zostały zaktualizowane na Serwerze administracyjnym.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	Liczba urządzeń zawierających bazy antywirusowe, które nie były aktualizowane przez długi czas (domyślnie 7 dni lub więcej w przypadkach **krytycznych** i 3 dni w przypadkach **ostrzeżeń**). Jeśli istnieją urządzenia ze statusem aktualizacji **krytycznych**, zliczane są tylko te urządzenia. Stan aktualizacji można uzyskać za pomocą updatesStatus.
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	Stan ochrony w czasie rzeczywistym. Jeden z następujących: • **Ostrzeżenie**. Jeden z następujących: Wykryto naruszenie zabezpieczeń na urządzeniu należącym do grupy Serwera administracyjnego. Błędy szyfrowania spowodowały, że niektóre urządzenia zmieniły stan ochrony. Pełne skanowanie nie było wykonywane przez długi czas. • **Krytyczne**. Ochrona antywirusowa nie działa na niektórych urządzeniach w grupach Serwera administracyjnego. • **OK**. Żadne z powyższych.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	Aplikacja zabezpieczająca nie działa na niektórych urządzeniach. Liczbę tych urządzeń można uzyskać za pośrednictwem hostsAntivirusNotRunning.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	Ochrona w czasie rzeczywistym nie działa na niektórych urządzeniach. Liczbę tych urządzeń można uzyskać za pośrednictwem hostsRealtimeNotRunning.
psRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.2.3	Liczba urządzeń, których poziom ochrony w czasie rzeczywistym różni się od poziomu ustawionego przez administratora
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Istnieją urządzenia zawierające niewyleczone obiekty. Liczbę tych urządzeń można uzyskać za pośrednictwem hostsNotCuredObject.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Na niektórych urządzeniach wykryto zagrożenia. Liczbę tych urządzeń można uzyskać za pośrednictwem hostsTooManyThreats.

Wartość identyfikatora obiektu	Typ danych numerycznych	Identyfikator OID	Opis
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	Stan ataku wirusa w systemie. Wartość wynosi 1, jeśli pewna liczba wirusów została znaleziona w określonym czasie, i 0 w przeciwnym wypadku. Liczba wirusów i ilość czasu są określane na Serwerze administracyjnym przy użyciu ustawień Virus attack.
psVulnerabilitiesFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.7	Wykryto luki w zabezpieczeniach.
psEncryptionFaultsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.8	Wykryto błędy szyfrowania, które zmieniły stan ochrony urządzenia.
psVulnerableHostsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.9	Na niektórych urządzeniach wykryto luki w zabezpieczeniach.
psNotScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.10	Wykryto urządzenia bez pełnego skanowania przez dłuższy czas.
psNagentsNotRunningUntilReboot	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.11	Wykryto urządzenia, na których Agent sieciowy uruchamia się dopiero po ponownym uruchomieniu.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	Liczba urządzeń z niedziałającymi aplikacjami zabezpieczającymi.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	Liczba urządzeń z niedziałającą ochroną w czasie rzeczywistym.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	Liczba urządzeń z niedopuszczalnym poziomem ochrony w czasie rzeczywistym.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	Liczba urządzeń zawierających niewyleczone obiekty.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	Liczba urządzeń zawierających zagrożenia.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	Stan pełnego skanowania antywirusowego jest jednym z następujących: • **Informacja**. Od momentu instalacji aplikacji minęło mniej niż 7 dni. • **Ostrzeżenie**. Pełne skanowanie antywirusowe nie było wykonywane od ponad 7 dni od momentu instalacji aplikacji. • **Krytyczne**. Pełne skanowanie antywirusowe nie było wykonywane od ponad 14 dni od momentu instalacji aplikacji. • **OK**. Żadne z powyższych.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Niektóre urządzenia nie były skanowane przez określony czas. Liczbę tych urządzeń można uzyskać za pośrednictwem hostsNotScannedLately. Ilość czas jest określona w wartości fullScanStatus.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	Liczba urządzeń, które nie były skanowane przez określony czas. Ilość czas jest określona w wartości fullScanStatus.
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	Stan sieci logicznej Serwera administracyjnego. Jeden z następujących: • **Ostrzeżenie**. Jeśli istnieją urządzenia ze stanem ostrzeżenia, do których nie można uzyskać dostępu, lub jeśli istnieją urządzenia, które nie należą do żadnej grupy Serwera administracyjnego. • **Krytyczne**. Jeśli istnieją urządzenia, nad którymi kontrola została utracona przez Serwer administracyjny, lub jeśli istnieją urządzenia o stanie krytycznym, do których nie można uzyskać dostępu. • **OK**. Żadne z powyższych.

Wartość identyfikatora obiektu	Typ danych numerycznych	Identyfikator OID	Opis
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	Niektóre urządzenia nie były połączone z Serwerem administracyjnym przez długi czas (7 lub więcej dni w przypadku urządzenia o stanie **Ostrzeżenie** i 4 dni w przypadku urządzenia o stanie **Krytyczne**). Liczbę tych urządzeń można uzyskać za pośrednictwem hostsNotConnectedLongTime.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	Istnieją urządzenia, nad którymi kontrola została utracona przez Serwer administracyjny. Liczbę tych urządzeń można uzyskać za pośrednictwem hostsControlLost.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	Liczba urządzeń znalezionych przez Serwer administracyjny, które nie należą do żadnej grupy Serwera administracyjnego.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	Liczba grup na Serwerze administracyjnym.
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	Liczba urządzeń, które nie były połączone z Serwerem administracyjnym od dłuższego czasu. Okres uważany za długi jest określony w wartości notConnectedLongTime.
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	Liczba urządzeń, które nie są kontrolowane przez Serwer administracyjny.
eventsStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.6.1	Stan podsystemu zdarzeń jest jednym z następujących: • **Ostrzeżenie**. Jeden z następujących: Urządzenia grupy Serwera administracyjnego nie wyszukiwały aktualizacji systemu Windows przez długi czas. Istnieją urządzenia z problemami ze stanem. • **Krytyczne**. Jeden z następujących: Wystąpiło zdarzenie „Krytyczne” na co najmniej jednym urządzeniu. Wystąpiło zdarzenie „Błąd” na co najmniej jednym urządzeniu. Istnieje zdarzenie zadania zakończonego niepomyślnie na co najmniej jednym urządzeniu. Urządzenia grupy Serwera administracyjnego nie wyszukiwały aktualizacji systemu Windows przez długi czas. Istnieją urządzenia z problemami ze stanem. • **Informacja.** Jeden z następujących: Minął mniej niż tydzień od ostatniego pełnego skanowania antywirusowego wszystkich urządzeń. Zadania instalacji zdalnej zostały ukończone i żadne urządzenie nie wymaga ponownego uruchomienia. Minął mniej niż tydzień od ostatniej aktualizacji Serwera administracyjnego. Serwer administracyjny nie był aktualizowany od dłuższego czasu, ale aktualizacja jest obecnie w toku. • **OK**. Żadne z powyższych.
criticalEventOccured	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.6.2.1	eventsStatus wskazuje, że na Serwerze administracyjnym istnieją zdarzenia krytyczne. Liczbę tych zdarzeń można uzyskać, korzystając z funkcji criticalEventsCount. Wartość jest równa 1, jeśli na dowolnym urządzeniu występuje co najmniej jedno zdarzenie krytyczne, i 0 w innym przypadku.
criticalEventsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.6.3	Liczba zdarzeń krytycznych na Serwerze administracyjnym.

Rozwiązywanie problemów

W tej sekcji przedstawiono rozwiązania kilku typowych problemów, które mogą wystąpić podczas korzystania z usługi SNMP.

Aplikacja firmy trzeciej nie może połączyć się z usługą SNMP

Upewnij się, że usługa SNMP jest zainstalowana i skonfigurowana zgodnie z opisem w sekcji Konfigurowanie usługi SNMP do użycia z Kaspersky Security Center.

Usługa SNMP działa, ale aplikacja firmy trzeciej nie może pobrać żadnych wartości

Zezwól na śledzenie agenta SNMP i upewnij się, że został utworzony niepusty plik. Oznacza to, że agent SNMP jest prawidłowo zarejestrowany i działa. Następnie zezwól na połączenia z usługi SNMP w ustawieniach usługi pobocznej. Jeśli usługa poboczna działa na tym samym hoście co agent SNMP, lista adresów IP powinna zawierać albo adres IP tego hosta, albo `loopback 127.0.0.1`.

Usługa SNMP, która komunikuje się z agentami, powinna działać w systemie Windows. Możesz określić ścieżki do agentów SNMP w rejestrze systemu Windows za pomocą programu regedit.

- Windows 10:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- Windows Vista i Windows Server 2008:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

Za pomocą programu regedit możesz również zezwolić na śledzenie agentów SNMP.

- W systemach 32-bitowych:
  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
- W systemach 64-bitowych:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb
  "TraceLevel"=dword:00000004
  "TraceDir"="C:\\"

Wartości nie pasują do stanów Konsoli administracyjnej

Aby zmniejszyć obciążenie na Serwerze administracyjnym, dla agenta SNMP zaimplementowano buforowanie wartości. Opóźnienie między aktualizacją pamięci podręcznej a zmianami wartości na Serwerze administracyjnym może powodować niezgodności między wartościami zwracanymi przez agenta SNMP i rzeczywistymi. Podczas pracy z aplikacjami firm trzecich należy wziąć pod uwagę to możliwe opóźnienie.

Praca w środowisku chmury

Ta sekcja zawiera informacje o zdalnej instalacji i konserwacji Kaspersky Security Center w środowiskach chmury, takich jak Amazon Web Services, Microsoft Azure lub Google Cloud.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), przy czym funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Informacje o pracy w środowisku chmury

Kaspersky Security Center 15.1 pracuje nie tylko z urządzeniami lokalnymi, ale także oferuje specjalne funkcje do pracy w środowisku chmury. Kaspersky Security Center działa z następującymi maszynami wirtualnymi:

- Instancje Amazon EC2 (zwane dalej również *instancjami*). Instancja Amazon EC2 to maszyna wirtualna, która jest tworzona w oparciu o platformę Amazon Web Services (AWS). Kaspersky Security Center używa AWS *API* (Interfejs programowania aplikacji).
- Maszyny wirtualne Microsoft Azure. Kaspersky Security Center używa Azure API.
- Instancje maszyn wirtualnych Google Cloud. Kaspersky Security Center używa Google API.

Możesz zainstalować Kaspersky Security Center na instancji lub maszynie wirtualnej w celu zarządzania ochroną urządzeń w środowisku chmury i używać specjalnych funkcji Kaspersky Security Center do pracy w środowisku chmury. Te funkcje obejmują:

- Wykorzystanie narzędzi API do przeszukiwania urządzeń w środowisku chmury
- Wykorzystanie narzędzi API do zainstalowania Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w środowisku chmury
- Wyszukiwanie urządzeń w oparciu o ich przynależność do określonego segmentu chmury

Możesz również użyć instancji lub maszyny wirtualnej, na której jest zainstalowany Serwer administracyjny Kaspersky Security Center, aby chronić urządzenia lokalne (na przykład, jeśli serwer chmury okazuje się być łatwiejszy w obsłudze i utrzymaniu niż fizyczny). W takim przypadku możesz pracować z Serwerem administracyjnym tak samo, jak gdyby Serwer administracyjny był zainstalowany na urządzeniu lokalnym.

W programie Kaspersky Security Center, który został zainstalowany z płatnego obrazu Amazon Machine Image (AMI) (w AWS) lub z opcji Usage-based monthly billed SKU (w Azure), Zarządzanie poprawkami i lukami (w tym integracja z systemami SIEM) jest automatycznie aktywowane; Zarządzanie urządzeniami mobilnymi nie może zostać aktywowane.

Serwer administracyjny jest instalowany wraz z Konsolą administracyjną. Kaspersky Security for Windows Server jest także instalowany automatycznie na urządzeniu, na którym jest zainstalowany Serwer administracyjny.

Możesz skonfigurować Kaspersky Security Center za pomocą Kreatora konfiguracji środowiska chmury z uwzględnieniem specyfiki pracy w środowisku chmury.

Scenariusz: Wdrażanie ochrony dla środowiska chmury

Ta sekcja opisuje wdrażanie Kaspersky Security Center do pracy w środowiskach chmury, takich jak Amazon Web Services, Microsoft Azure i Google Cloud.

Po zakończeniu scenariusza wdrażania, elementy Serwer administracyjny Kaspersky Security Center i Konsola administracyjna zostaną uruchomione i skonfigurowane z parametrami domyślnymi. Ochrona antywirusowa zarządzana przez Kaspersky Security Center zostanie wdrożona na wybranych instancjach Amazon EC2 lub maszynach wirtualnych Microsoft Azure. Możesz dopasować konfigurację Kaspersky Security Center, utworzyć złożoną strukturę grup administracyjnych oraz utworzyć różne zasady i zadania dla grup.

Wdrożenie Kaspersky Security Center w środowisku chmury obejmuje następujące kroki:

1. Prace przygotowawcze
2. Wdrażanie Serwera administracyjnego
3. Instalowanie aplikacji antywirusowych firmy Kaspersky na urządzeniach wirtualnych, które mają być chronione
4. Konfigurowanie ustawień pobierania uaktualnień
5. Konfigurowanie ustawień zarządzania raportami dotyczącymi stanu ochrony urządzeń

Kreator konfiguracji środowiska chmury jest przeznaczony do przeprowadzania wstępnej konfiguracji. Jest uruchamiany automatycznie pierwszy raz po wdrożeniu Kaspersky Security Center z gotowego do użycia obrazu. Możesz ręcznie uruchomić kreator w dowolnym momencie. Dodatkowo możesz ręcznie wykonać wszystkie działania, które realizuje.

Zalecane jest przeznaczenie przynajmniej jednej godziny na zainstalowanie Serwera administracyjnego Kaspersky Security Center w środowisku chmury oraz przynajmniej jednego dnia roboczego na wdrożenie ochrony w środowisku chmury.

Wdrożenie Kaspersky Security Center w środowisku chmury odbywa się w krokach:

1. **Planowanie konfiguracji segmentów chmury**

   Sprawdzenie, jak Kaspersky Security Center działa w środowisku chmury. Rozplanuj, gdzie zostanie zainstalowany Serwer administracyjny: (wewnątrz lub poza środowiskiem chmury); określ także, ile segmentów chmury chcesz chronić. Jeśli planujesz zainstalować Serwer administracyjny poza środowiskiem chmury lub planujesz chronić więcej niż 5 000 urządzeń, konieczne będzie ręczne zainstalowanie Serwera administracyjnego.

   Aby pracować z Google Cloud, możesz zainstalować Serwer administracyjny tylko ręcznie.

2. **Rozplanowywanie zasobów**

   Upewnij się, że posiadasz wszystko, co jest niezbędne do wdrożenia ochrony.

3. **Subskrypcja na Kaspersky Security Center w postaci gotowego do użycia obrazu**

   Wybierz jeden z gotowych do użycia obrazów AMI w AWS Marketplace lub wybierz Usage-based monthly billed SKU w Azure Marketplace, zapłać za niego zgodnie z regułami rynku, jeśli to konieczne (lub skorzystaj z modelu BYOL) i użyj obrazu do wdrożenia instancji Amazon EC2 / maszyny wirtualnej Microsoft Azure z zainstalowanym Kaspersky Security Center.

Ten krok jest niezbędny tylko wtedy, gdy planujesz zainstalować Serwer administracyjny na instancji / maszynie wirtualnej w obrębie środowiska chmury i planujesz także wdrożenie ochrony dla ponad 5000 urządzeń. W innych sytuacjach wykonanie czynności z tego kroku nie jest konieczne, a zamiast niego konieczne jest ręczne zainstalowanie Serwera administracyjnego, Konsoli administracyjnej i DBMS.

Ten krok jest niedostępny dla Google Cloud.

4. **Określanie lokalizacji DBMS**

   Określ lokalizację Twojego systemu DBMS.

   Jeśli planujesz użyć bazy danych spoza środowiska chmury, upewnij się, że posiadasz działającą bazę danych.

   Jeśli planujesz korzystać z Amazon Relational Database Service (RDS), utwórz bazę danych z RDS w środowisku chmury AWS.

   Jeśli planujesz używać Microsoft Azure SQL DBMS, utwórz bazę danych za pomocą usługi Azure Database w środowisku chmury Microsoft Azure.

   Jeśli planujesz używać Google MySQL, utwórz bazę danych w Google Cloud (szczegóły można znaleźć na stronie https://cloud.google.com/sql/docs/mysql).

5. **Ręczne instalowanie Serwera administracyjnego i Konsoli administracyjnej (opartej na konsoli Microsoft Management Console i/lub konsoli internetowej) na wybranych urządzeniach**

   Zainstaluj Serwer administracyjny, Konsolę administracyjną i system DBMS na wybranych urządzeniach zgodnie z zaleceniami dla głównego scenariusza instalacji Kaspersky Security Center.

   Ten krok jest niezbędny, gdy planujesz umieścić Serwer administracyjny poza środowiskiem chmury lub planujesz wdrożenie ochrony dla ponad 5 000 urządzeń. Następnie upewnij się, że Twój Serwer administracyjny spełnia wymagania sprzętowe. W innych sytuacjach wykonanie czynności z tego kroku nie jest konieczne, a subskrypcja na Kaspersky Security Center w postaci gotowego do użycia obrazu w AWS Marketplace, Azure Marketplace lub Google Cloud jest wystarczająca.

6. **Zapewnianie, że Serwer administracyjny posiada uprawnienia do pracy z interfejsami API chmury**

   W AWS przejdź do konsoli zarządzania AWS i utwórz rolę IAM lub konto użytkownika IAM. Utworzona rola IAM (lub konto użytkownika IAM) umożliwi Kaspersky Security Center pracę z segmentami chmury AWS API: Poll oraz wdrożenie ochrony.

   W Azure utwórz subskrypcję oraz ID aplikacji z hasłem. Kaspersky Security Center używa tych danych uwierzytelniających do pracy z segmentami chmury Azure API: Poll i wdrożenia ochrony.

   W Google Cloud zarejestruj projekt, uzyskaj ID projektu i klucz prywatny. Kaspersky Security Center używa tych danych uwierzytelniających do przeszukiwania segmentów chmury przy użyciu Google API.

7. **Tworzenie roli IAM dla chronionych instancji (tylko dla AWS)**

   W konsoli zarządzania AWS utwórz rolę IAM, która definiuje zestaw uprawnień do wykonywania żądań wysyłanych do AWS. Ta nowo utworzona rola będzie później przypisywana do nowych instancji. Rola IAM jest wymagana do użycia Kaspersky Security Center do zainstalowania aplikacji na instancjach.

8. **Przygotowywanie bazy danych przy użyciu usługi Amazon Relational Database Service lub Microsoft Azure SQL**

   Jeśli planujesz użyć Amazon Relational Database Service (RDS), utwórz instancję bazy danych Amazon RDS i komorę S3, gdzie przechowywana będzie kopia zapasowa bazy danych. Możesz pominąć ten krok, jeśli chcesz mieć bazę danych na tej samej instancji EC2, na której jest zainstalowany Serwer administracyjny, lub jeśli chcesz, aby Twoja baza danych znajdowała się w innym miejscu.

   Jeśli panujesz użyć Microsoft Azure SQL, utwórz konto magazynu i bazę danych w Microsoft Azure.

   Jeśli planujesz używać Google MySQL, skonfiguruj bazę danych w Google Cloud (szczegóły można znaleźć na stronie https://cloud.google.com/sql/docs/mysql).

9. **Licencjonowanie Kaspersky Security Center do pracy w środowisku chmury**

Upewnij się, że posiadasz licencjonowaną wersję Kaspersky Security Center, aby pracować w środowisku chmury, i dostarcz kod aktywacyjny lub plik klucza, aby aplikacja mogła dodać go do magazynu licencji. Ten etap można zakończyć podczas konfiguracji środowiska chmury.

Ten krok jest wymagany, jeśli korzystasz z programu Kaspersky Security Center zainstalowanego z bezpłatnego, gotowego do użycia obrazu AMI na podstawie modelu BYOL lub jeśli ręcznie instalujesz Kaspersky Security Center bez użycia obrazów AMI. W każdym z tych przypadków będziesz potrzebował licencji dla Kaspersky Security for Virtualization lub licencji dla Kaspersky Hybrid Cloud Security, aby aktywować Kaspersky Security Center.

Jeśli używasz Kaspersky Security Center zainstalowanego z gotowego do użycia obrazu, ten etap nie jest konieczny, a odpowiednie okno Kreatora konfiguracji środowiska chmury nie jest wyświetlane.

10. **Autoryzacja w środowisku chmury**

    Dostarcz Kaspersky Security Center swoje dane uwierzytelniające AWS, Azure lub Google Cloud, aby Kaspersky Security Center mógł działać z potrzebnymi uprawnieniami. Ten etap można zakończyć podczas autoryzacji w środowisku chmury.

11. **Przeszukiwanie segmentu chmury, aby Serwer administracyjny mógł uzyskać informacje o urządzeniach w segmencie chmury**

    Uruchom przeszukiwanie segmentu chmury. W środowisku AWS Kaspersky Security Center uzyska adresy i nazwy wszystkich instancji, do których dostęp można uzyskać w oparciu o uprawnienia roli IAM lub użytkownika IAM. W środowisku Microsoft Azure Kaspersky Security Center uzyska adresy i nazwy wszystkich maszyn wirtualnych, do których dostęp można uzyskać w oparciu o uprawnienia roli Czytelnik.

    Następnie możesz użyć Kaspersky Security Center do zainstalowania aplikacji firmy Kaspersky i oprogramowania innych producentów na wykrytych instancjach lub maszynach wirtualnych.

    Kaspersky Security Center regularnie wykonuje przeszukiwanie, co oznacza, że nowe instancje lub maszyny wirtualne są wykrywane automatycznie.

12. **Przyłączanie wszystkich urządzeń sieciowych do grupy administracyjnej Chmura**

    Przenieś wszystkie wykryte instancje /maszyny wirtualne do grupy administracyjnej **Zarządzane urządzenia\Chmura**, aby mogły stać się dostępne do scentralizowanego zarządzania. Jeśli chcesz przydzielić urządzenia do podgrup, na przykład, według zainstalowanego na nich systemu operacyjnego, w grupie **Zarządzane urządzenia\Chmura** możesz utworzyć kilka grup administracyjnych. Możesz włączyć automatyczne przenoszenie wszystkich urządzeń, które zostaną wykryte podczas rutynowego przeszukiwania, do grupy **Zarządzane urządzenia\Chmura**.

13. **Używanie Agenta sieciowego do podłączania urządzeń w sieci do Serwera administracyjnego**

    Zainstaluj Agenta sieciowego na urządzeniach w środowisku chmury. Agent sieciowy jest komponentem Kaspersky Security Center, który zapewnia komunikację pomiędzy urządzeniami a Serwerem administracyjnym. Domyślnie ustawienia Agenta sieciowego są konfigurowane automatycznie.

    Możesz zainstalować Agenta sieciowego na każdym urządzeniu lokalnie. Możesz także zdalnie zainstalować Agenta sieciowego na urządzeniach przy użyciu Kaspersky Security Center. Lub możesz pominąć ten krok i zainstalować Agenta sieciowego wraz z najnowszymi wersjami aplikacji zabezpieczających.

14. **Instalowanie najnowszych wersji aplikacji zabezpieczających na urządzeniach w sieci**

    Wybierz urządzenia, na których chcesz zainstalować aplikacje zabezpieczające, a następnie zainstaluj najnowsze wersje aplikacji zabezpieczających na tych urządzeniach. Instalację można przeprowadzić zdalnie przy użyciu Kaspersky Security Center na Serwerze administracyjnym lub lokalnie.

    Konieczne może być ręczne utworzenie pakietów instalacyjnych dla tych programów.

    Kaspersky Endpoint Security for Linux jest przeznaczony dla instancji i maszyn wirtualnych działających pod kontrolą systemu Linux.

Kaspersky Security for Windows Server jest przeznaczony dla instancji i maszyn wirtualnych działających pod kontrolą systemu Windows.

15. **Konfigurowanie ustawień aktualizacji**

Zadanie **Wyszukiwanie luk i wymaganych aktualizacji** jest tworzone automatycznie po uruchomieniu konfiguracji środowiska chmury. Możesz także ręcznie utworzyć zadanie. To zadanie automatycznie wyszukuje i pobiera wymagane aktualizacje aplikacji dla instalacji na urządzeniach w sieci przy użyciu narzędzi Kaspersky Security Center.

Po zakończeniu konfiguracji środowiska chmury zaleca się wykonanie następującego etapu:

1. **Konfigurowanie zarządzania raportami**

   Możesz przejrzeć raporty na zakładce **Monitorowanie** w obszarze roboczym węzła **Serwer administracyjny** i/lub otrzymać raporty za pośrednictwem poczty elektronicznej. Raporty możesz otrzymać także za pośrednictwem poczty elektronicznej. Raporty na zakładce **Monitorowanie** są dostępne domyślnie. Aby skonfigurować otrzymywanie raportów za pośrednictwem poczty elektronicznej, określ adresy e-mail, na które powinny przychodzić raporty, a następnie skonfiguruj format raportów.

Wyniki

Po zakończeniu scenariusza możesz upewnić się, że wstępna konfiguracja zakończyła się pomyślnie:

- Możesz nawiązać połączenie z Serwerem administracyjnym poprzez Konsolę administracyjną lub Kaspersky Security Center Web Console.
- Najnowsze wersje aplikacji zabezpieczających Kaspersky są zainstalowane i uruchomione na zarządzanych urządzeniach.
- Kaspersky Security Center utworzył domyślne zasady i zadania dla wszystkich zarządzanych urządzeń.

Wymagania wstępne wdrożenia Kaspersky Security Center w środowisku chmury

Przed rozpoczęciem wdrożenia Kaspersky Security Center w środowisku chmury Amazon Web Services lub Microsoft Azure, upewnij się, że posiadasz:

- Dostęp do internetu
- Jedno z następujących kont:
  - Konto Amazon Web Services (do pracy z AWS)
  - Konto Microsoft (do pracy z Azure)
  - Konto Google (do pracy z Google Cloud)
- Jeden z następujących:
  - Licencję dla Kaspersky Security for Virtualization
  - Licencję dla Kaspersky Hybrid Cloud Security

- Fundusze na zakup takiej licencji (Kaspersky Security for Virtualization lub Kaspersky Hybrid Cloud Security)
- Fundusze na zakup gotowego do użycia obrazu w Azure Marketplace

- Podręczniki dla najnowszych wersji Kaspersky Endpoint Security for Linux i Kaspersky Security for Windows Server

Wymagania sprzętowe dla Serwera administracyjnego w środowisku chmury

W celu przeprowadzenia zdalnej instalacji w środowiskach chmury, wymagania Serwera administracyjnego i serwera bazy danych tak samo jak wymagania dla fizycznego Serwera administracyjnego (w zależności od ilości urządzeń, którymi chcesz zarządzać). Więcej informacji można znaleźć w dokumentacji dotyczącej środowiska chmury.

Opcje licencjonowania w środowisku chmury

Praca w środowisku chmury jest poza podstawową funkcjonalnością Kaspersky Security Center, więc wymaga to specjalnej licencji.

Do pracy w środowisku chmury dostępne są dwie opcje licencjonowania Kaspersky Security Center:

- Paid AMI (w Amazon Web Services) / Usage-based monthly billed SKU (w Microsoft Azure).

  Przyznaje to licencję dla Kaspersky Security Center, a także licencje dla Kaspersky Endpoint Security for Linux i Kaspersky Security for Windows Server. Musisz zapłacić zgodnie z regułami środowiska chmury, którego używasz.

  Ten model pozwala na posiadanie nie więcej niż 200 urządzeń klienckich dla jednego Serwera administracyjnego.

- Bezpłatny, gotowy do użycia obraz za pomocą własnościowej licencji, zgodnie z modelem Bring Your Own License (BYOL).

  W przypadku licencjonowania Kaspersky Security Center w AWS lub Azure, należy posiadać licencję dla jednej z następujących aplikacji:

  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

  Model BYOL pozwala na posiadanie do 100 000 urządzeń klienckich dla jednego Serwera administracyjnego. Ten model umożliwia także zarządzanie urządzeniami spoza środowiska chmury AWS, Azure lub Google.

  Model BYOL można wybrać w jednym z następujących przypadków:

  - Jeśli masz już ważną licencję dla Kaspersky Security for Virtualization.
  - Jeśli masz już ważną licencję dla Kaspersky Hybrid Cloud Security.
  - Jeśli chcesz zakupić licencję bezpośrednio przed zdalną instalacją Kaspersky Security Center.

  Na etapie wstępnej konfiguracji Kaspersky Security Center wyświetli okno z prośbą o podanie kodu aktywacyjnego lub pliku klucza.

Jeśli wybierzesz BYOL, nie musisz płacić za Kaspersky Security Center za pośrednictwem Azure Marketplace lub AWS Marketplace.

W obu przypadkach automatycznie aktywowane jest Zarządzanie lukami i poprawkami, a Zarządzanie urządzeniami mobilnymi nie może zostać aktywowane.

Jeżeli podczas próby aktywacji funkcji Wsparcie środowiska chmury przy użyciu licencji dla Kaspersky Hybrid Cloud Security wystąpi błąd, należy użyć pliku klucza.

Po wykupieniu subskrypcji na Kaspersky Security Center, otrzymujesz instancję Amazon Elastic Compute Cloud (Amazon EC2) lub maszynę wirtualną Microsoft Azure z Serwerem administracyjnym Kaspersky Security Center. Pakiety instalacyjne dla Kaspersky Security for Windows Server i Kaspersky Endpoint Security for Linux są dostępne na Serwerze administracyjnym. Możesz zainstalować te aplikacje na urządzeniach w środowisku chmury. Nie musisz licencjonować tych aplikacji.

Jeśli zarządzane urządzenie nie jest widoczne dla Serwera administracyjnego przez ponad tydzień, aplikacja (Kaspersky Security for Windows Server lub Kaspersky Endpoint Security for Linux) na urządzeniu przełączy się do trybu ograniczonej funkcjonalności. Aby aktywować aplikację ponownie, urządzenie, na której zainstalowana jest ta aplikacja, musi ponownie stać się widoczne dla Serwera administracyjnego.

Opcje bazy danych do pracy w środowisku chmury

Musisz mieć bazę danych, aby pracować z Kaspersky Security Center. Podczas instalowania Kaspersky Security Center w AWS, w Microsoft Azure lub Google Cloud masz trzy opcje:

- Utwórz lokalną bazę danych na tym samym urządzeniu co Serwer administracyjny. Kaspersky Security Center jest dostarczany z bazą danych SQL Server Express, która może obsługiwać do 5 000 zarządzanych urządzeń. Wybierz tę opcję, jeśli SQL Server Express Edition jest wystarczający dla Twoich potrzeb.

- Utwórz bazę danych z Relational Database Service (RDS) w środowisku chmury AWS lub z usługi Azure Database w środowisku chmury Microsoft Azure. Wybierz tę opcję, jeśli chcesz system DBMS inny niż SQL Express. Twoje dane zostaną przesłane wewnątrz środowiska chmury, gdzie pozostaną, i nie będziesz ponosił dodatkowych wydatków. Jeśli już pracujesz z Kaspersky Security Center na urządzeniach lokalnych i posiadasz pewne dane w swojej bazie danych, możesz przenieść swoje dane do nowej bazy danych.

  Do pracy na platformie Google Cloud Platform możesz użyć tylko Cloud SQL for MySQL.

- Użyj istniejącego serwera bazy danych. Wybierz tę opcję, jeśli już posiadasz serwer bazy danych i chcesz go używać dla Kaspersky Security Center. Jeśli ten serwer znajduje się poza środowiskiem chmury, Twoje dane zostaną przesłane przez internet, co może generować dodatkowe koszty.

Procedura wdrażania Kaspersky Security Center w środowisku chmury posiada specjalny krok tworzenia (wybierania) bazy danych.

Praca w środowisku chmury Amazon Web Services

Ta sekcja opisuje sposób przygotowania pracy z Kaspersky Security Center w Amazon Web Services.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Informacje o pracy w środowisku chmury Amazon Web Services

Kaspersky Security Center można kupić w sklepie AWS Marketplace w postaci Amazon Machine Image (AMI), która jest gotowym do użycia obrazem wstępnie skonfigurowanej maszyny wirtualnej. Możesz wykupić subskrypcję na płatny obraz AMI lub BYOL AMI i na podstawie tego obrazu utworzyć instancję Amazon EC2 z zainstalowanym Serwerem administracyjnym Kaspersky Security Center.

Aby pracować z platformą AWS, a w szczególności kupić aplikacje w sklepie AWS Marketplace i tworzyć instancje, będziesz potrzebował konta Amazon Web Services. Możesz utworzyć darmowe konto na stronie https://aws.amazon.com. Możesz także użyć istniejącego konta Amazon.

Jeśli wykupiłeś subskrypcję na obraz AMI, dostępny w sklepie AWS Marketplace, otrzymasz instancję z gotowym do użycia Kaspersky Security Center. Nie trzeba instalować aplikacji samodzielnie. W takim przypadku Serwer administracyjny Kaspersky Security Center jest instalowany na instancji bez Twojego udziału. Po instalacji, możesz uruchomić Konsolę administracyjną i połączyć się z Serwerem administracyjnym, aby rozpocząć pracę z Kaspersky Security Center.

W celu uzyskania bardziej szczegółowych informacji na temat obrazu AMI oraz działania AWS Marketplace, odwiedź stronę pomocy AWS Marketplace. Aby uzyskać więcej informacji na temat pracy z platformą AWS, używania instancji oraz powiązanych pojęć, zapoznaj się z dokumentacją Amazon Web Services.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Tworzenie roli IAM i kont użytkowników IAM dla instancji Amazon EC2

Ta sekcja opisuje działania, jakie muszą zostać wykonane w celu zapewnienia poprawnego działania Serwera administracyjnego. Te działania obejmują pracę z rolami AWS Identity i Access Management (IAM) i kontami użytkowników. Opisane są także działania, które muszą zostać wykonane na urządzeniach klienckich w celu zainstalowania na nich Agenta sieciowego, a następnie zainstalowania Kaspersky Security for Windows Server i Kaspersky Endpoint Security for Linux.

Zapewnianie, że Serwer administracyjny Kaspersky Security Center posiada uprawnienia do pracy z AWS

Standardy działania środowiska chmury Amazon Web Services zalecają, aby specjalna rola IAM była przypisywana do instancji Serwera administracyjnego do pracy z usługami AWS. Rola IAM to jednostka IAM, która definiuje zestaw uprawnień do wykonywania żądań wysyłanych do usług AWS. Rola IAM zapewnia uprawnienia dla przeszukiwania segmentu chmury i instalacji aplikacji na instancjach.

Po utworzeniu roli IAM i przypisaniu jej do Serwera administracyjnego, będziesz mógł wdrożyć ochronę instancji przy użyciu tej roli, bez dostarczania jakichkolwiek dodatkowych informacji do Kaspersky Security Center.

Jednakże zalecane jest, aby nie tworzyć roli IAM dla Serwera administracyjnego w następujących przypadkach:

- Urządzenia, których ochroną planujesz zarządzać, to instancje EC2 w środowisku chmury Amazon Web Services, ale Serwer administracyjny znajduje się poza tym środowiskiem.
- Planujesz zarządzać ochroną instancji nie tylko w obrębie swojego segmentu chmury, ale także w innych segmentach chmury, które zostały utworzone z poziomu innego konta w AWS. W tym przypadku będziesz potrzebował roli IAM tylko do ochrony swojego segmentu chmury. Rola IAM nie będzie potrzebna do ochrony innego segmentu chmury.

W tych przypadkach, zamiast utworzenia roli IAM będziesz musiał utworzyć *konto użytkownika IAM*, które będzie używane przez Kaspersky Security Center do pracy z usługami AWS. Przed rozpoczęciem pracy z Serwerem administracyjnym utwórz Konto użytkownika IAM z *Kluczem dostępu IAM AWS* (zwany dalej również *Klucz dostępu IAM*).

Do utworzenia roli IAM oraz konta użytkownika IAM wymagana jest konsola AWS Management Console. Aby pracować z konsolą AWS Management Console, potrzebna jest nazwa użytkownika i hasło dla konta w AWS.

Tworzenie roli IAM dla Serwera administracyjnego

Przed zainstalowaniem Serwera administracyjnego, w konsoli AWS Management Console utwórz rolę IAM z uprawnieniami wymaganymi do zainstalowania aplikacji na instancjach. Więcej informacji znajdziesz w sekcjach pomocy AWS o rolach IAM.

W celu utworzenia roli IAM dla Serwera administracyjnego:

1. Otwórz konsolę AWS Management Console i zaloguj się z poziomu konta AWS.
2. W sekcji **Role** utwórz rolę z następującymi uprawnieniami:
   - **AmazonEC2ReadOnlyAccess**, jeśli planujesz tylko uruchamiać przeszukiwanie segmentów chmury, a nie chcesz instalować aplikacji na instancjach EC2 przy użyciu AWS API.
   - **AmazonEC2ReadOnlyAccess** i **AmazonSSMFullAccess**, jeśli planujesz uruchamiać przeszukiwanie segmentów chmury i chcesz instalować aplikacje na instancjach EC2 przy użyciu AWS API. W tym przypadku konieczne będzie też przypisanie roli IAM z uprawnieniem AmazonEC2RoleforSSM do chronionych instancji EC2.

Będziesz musiał przypisać tę rolę do instancji EC2, której będziesz używał jako Serwera administracyjnego.

Nowo utworzona rola jest dostępna dla wszystkich aplikacji na Serwerze administracyjnym. Dlatego też każda aplikacja uruchomiona na Serwerze administracyjnym posiada możliwość przeszukiwania segmentów chmury lub instalowania aplikacji na instancjach EC2 w segmencie chmury.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Tworzenie konta użytkownika IAM do pracy z Kaspersky Security Center

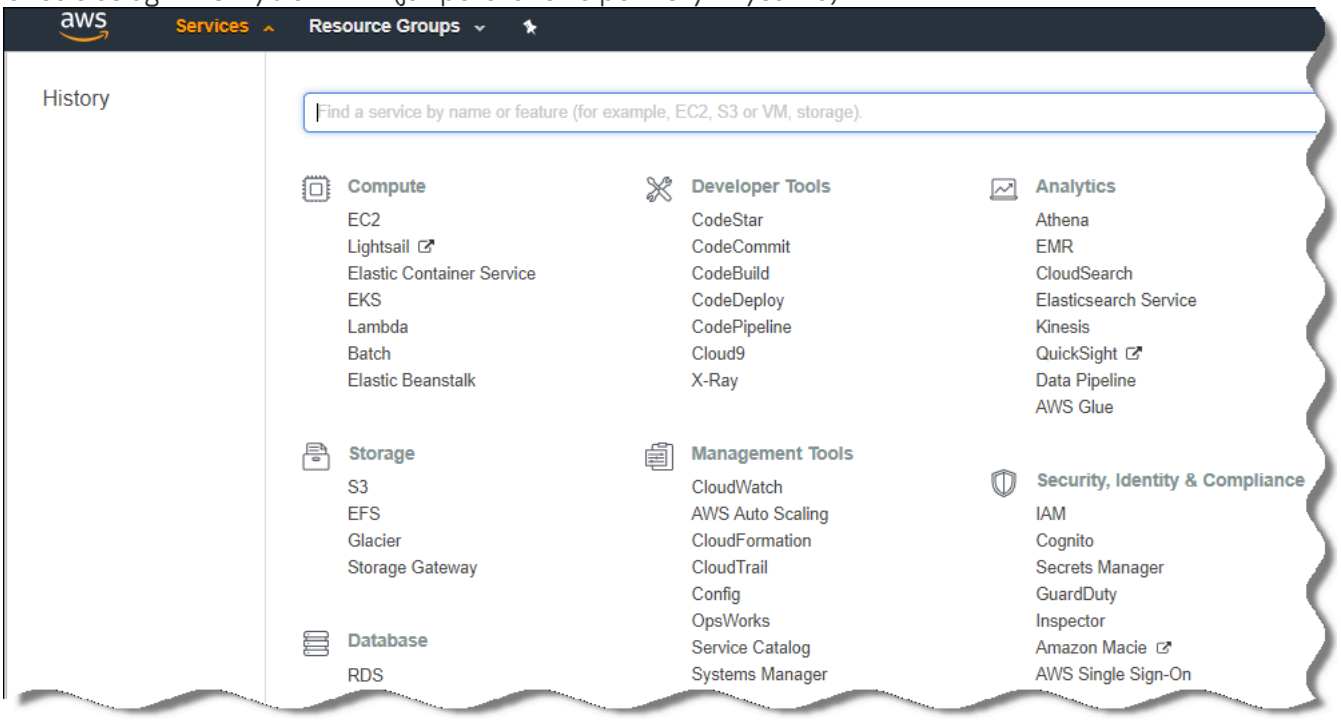
Konto użytkownika IAM jest wymagane do pracy z Kaspersky Security Center, jeśli do Serwera administracyjnego nie przypisano roli IAM z uprawnieniami do wyszukiwania urządzeń i instalacji aplikacji na instancjach. To samo konto lub inne konto jest także wymagane dla zadania tworzenia kopii zapasowej danych Serwera administracyjnego, jeśli używasz komory S3. Możesz utworzyć jedno konto użytkownika IAM ze wszystkimi niezbędnymi uprawnieniami lub możesz utworzyć dwa oddzielne konta użytkownika.

Klucz dostępu IAM, który będziesz musiał dostarczyć Kaspersky Security Center podczas wstępnej konfiguracji, jest automatycznie tworzony dla użytkownika IAM. Klucz dostępu IAM składa się z identyfikatora klucza dostępu i tajnego klucza. Więcej informacji na temat usługi IAM można znaleźć na następujących stronach referencyjnych AWS:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

W celu utworzenia konta użytkownika IAM z potrzebnymi uprawnieniami:

1. Otwórz konsolę AWS Management Console i zaloguj się z poziomu swojego konta.
2. Na liście usług AWS wybierz **IAM** (jak pokazano na poniższym rysunku).



Lista usług w konsoli AWS Management Console

Zostanie otwarte okno zawierające listę nazw użytkowników i menu, które umożliwia pracę z narzędziem.

3. Poruszaj się po obszarach konsoli związanych z kontami użytkownika i dodaj nową nazwę lub nazwy użytkownika.

4. Dla dodawanego użytkownika (użytkowników) określ następujące właściwości AWS:

   - Typ dostępu: **Programmatic Access**.
   - Granice uprawnień nie są określone.
   - Uprawnienia:
     - **ReadOnlyAccess**—jeśli planujesz tylko uruchamiać przeszukiwanie segmentów chmury, a nie chcesz instalować aplikacji na instancjach EC2 przy użyciu AWS API.
     - **ReadOnlyAccess** i **AmazonSSMFullAccess**—jeśli planujesz uruchamiać przeszukiwanie segmentów chmury i chcesz instalować aplikacje na instancjach EC2 przy użyciu AWS API. W tym przypadku konieczne będzie też przypisanie roli IAM z uprawnieniem AmazonEC2RoleforSSM do chronionych instancji EC2.

   Po dodaniu uprawnień sprawdź je pod kątem prawidłowości. W przypadku omyłkowego wyboru wróć do poprzedniego okna i ponownie dokonaj wyboru.

5. Po utworzeniu konta użytkownika, zostanie wyświetlona tabela zawierająca klucz dostępu IAM nowego użytkownika IAM. Identyfikator klucza dostępu zostanie wyświetlony w kolumnie **Access Key ID**. Tajny klucz będzie wyświetlany od postacią gwiazdek w kolumnie **Tajny klucz dostępu**. Aby sprawdzić tajny klucz, kliknij **Pokaż**.

Nowo utworzone konto zostanie wyświetlone na liście kont użytkowników IAM odpowiadających Twojemu kontu w AWS.

Podczas wdrażania Kaspersky Security Center w segmencie chmury musisz określić, że korzystasz z konta użytkownika IAM, oraz dostarczyć identyfikator klucza dostępu i tajny klucz dostępu do Kaspersky Security Center.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Tworzenie roli IAM dla instalacji aplikacji na instancjach Amazon EC2

Przed rozpoczęciem wdrażania ochrony na instancjach EC2 przy użyciu Kaspersky Security Center, utwórz w konsoli zarządzania AWS rolę IAM z uprawnieniami wymaganymi do instalacji aplikacji na instancjach. Więcej informacji o rolach IAM znajdziesz w sekcjach pomocy AWS.

Rola IAM jest potrzebna, aby móc ją przypisać do wszystkich instancji EC2, na których planujesz zainstalować aplikacje zabezpieczające przy użyciu Kaspersky Security Center. Jeśli nie przypiszesz do instancji roli IAM z wymaganymi uprawnieniami, instalacja aplikacji na tej instancji przy użyciu narzędzi AWS API zakończy się błędem.

Aby pracować z konsolą AWS Management Console, potrzebna jest nazwa użytkownika i hasło dla konta w AWS.

W celu utworzenia roli IAM dla instalacji aplikacji na instancjach:

1. Otwórz konsolę AWS Management Console i zaloguj się z poziomu konta AWS.
2. Z menu po lewej stronie wybierz **Roles**.
3. Kliknij przycisk **Create Role**.

4. Na liście usług, która zostanie wyświetlona, wybierz **EC2**, a następnie, na liście **Select Your Use Case** ponownie wybierz **EC2**.

5. Kliknij przycisk **Next: Permissions**.

6. Na otwartej liście zaznacz pole obok **AmazonEC2RoleforSSM**.

7. Kliknij przycisk **Next: Review**.

8. Wprowadź nazwę i opis dla roli IAM i kliknij przycisk **Create role**.

   Utworzona rola pojawi się na liście roli z wprowadzoną nazwą i opisem.

Możesz użyć nowo utworzonej roli IAM do utworzenia nowych instancji EC2, które chcesz chronić poprzez Kaspersky Security Center, a także skojarzyć ją z istniejącymi instancjami.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Praca z Amazon RDS

Ta sekcja opisuje, które akcje muszą zostać podjęte, aby przygotować bazę danych Amazon Relational Database Service (RDS) dla Kaspersky Security Center, umieścić ją w grupie opcji, utworzyć rolę IAM do pracy z bazą danych RDS, przygotować zasobnik S3 do przechowywania i przenieść istniejącą bazę danych do RDS.

Amazon RDS to usługa sieciowa, która pomaga użytkownikom AWS w skonfigurowaniu, działaniu i skalowaniu relacyjnych baz danych w środowisku chmury AWS. Jeśli chcesz, możesz użyć bazy danych Amazon RDS do pracy z Kaspersky Security Center.

Możesz pracować z następującymi bazami danych:

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

Tworzenie instancji Amazon RDS

Jeśli chcesz użyć Amazon RDS jako DBMS, musisz utworzyć instancję bazy danych Amazon RDS. Ta sekcja opisuje sposób wybrania SQL Express Edition; jeśli chcesz pracować z Aurora MySQL lub Standard MySQL (wersje 5.7, 8.0), powinieneś wybrać jeden z tych silników.

W celu utworzenia instancji bazy danych Amazon RDS:

1. Otwórz konsolę AWS Management Console, dostępną pod adresem https://console.aws.amazon.com, a następnie zaloguj się z poziomu swojego konta.

2. Korzystając z interfejsu AWS, utwórz bazę danych z następującymi ustawieniami:

   - Engine: Microsoft SQL Server, SQL Express Edition
   - Wersja silnika DB: SQL Server 2014 12.00.5546.0v1
   - Klasa instancji DB: db.t2.medium
   - Typ magazynu: General purpose
   - Przydzielony magazyn: minimum 50 GiB
   - Grupa bezpieczeństwa: ta sama grupa, w której znajduje się instancja EC2 z Serwerem administracyjnym Kaspersky Security Center

   Dla swojej instancji RDS utwórz identyfikator, nazwę użytkownika i hasło.

   W pozostałych polach możesz zostawić domyślne ustawienia. Lub zmienić domyślne ustawienia, jeśli chcesz dostosować swoją instancję Amazon RDS. Aby uzyskać pomoc, sprawdź strony informacyjne AWS.

3. W ostatnim kroku AWS wyświetli wyniki procesu. Jeśli chcesz przejrzeć szczegóły swojej instancji Amazon RDS, kliknij **View DB instance details**. Jeśli chcesz przejść do kolejnego działania, rozpocznij tworzenie grupy opcji dla swojej instancji Amazon RDS.

Tworzenie nowej instancji Amazon RDS może potrwać kilka minut. Po utworzeniu instancji, możesz jej użyć do pracy z danymi Kaspersky Security Center.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Tworzenie grupy opcji dla instancji Amazon RDS

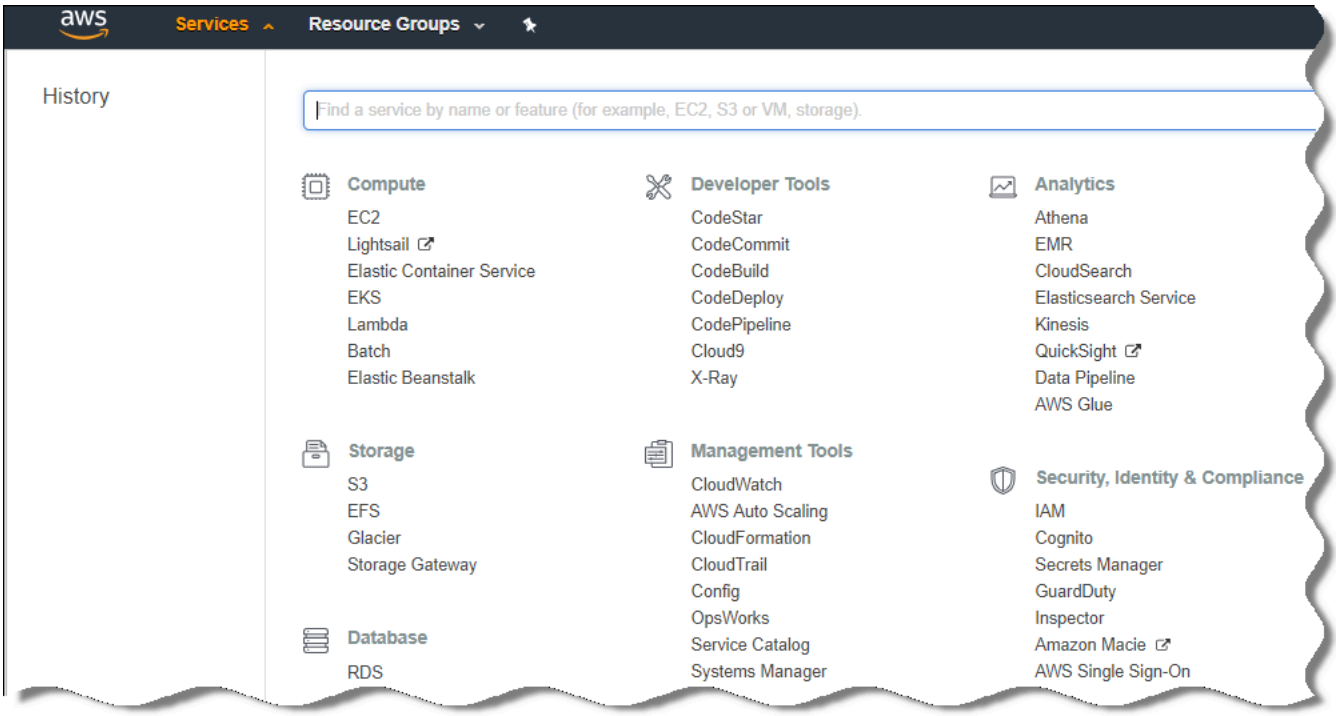
Musisz umieścić swoją instancję Amazon RDS w grupie opcji.

W celu utworzenia grupy opcji dla swojej instancji Amazon RDS:

1. Upewnij się, że jesteś w konsoli AWS Management Console (https://console.aws.amazon.com) i zalogowałeś się do niej z poziomu swojego konta.

2. W wierszu menu kliknij **Usługi**.

   Zostanie wyświetlona lista dostępnych usług (patrz rysunek poniżej).



Lista usług w konsoli AWS Management Console

3. Na liście kliknij **RDS**.
4. W lewym panelu kliknij **Grupy opcji**.
5. Kliknij przycisk **Create group**.
6. Jeśli na etapie tworzenia instancji Amazon RDS wybrałeś serwer SQL, utwórz grupę opcji z następującymi ustawieniami:

   - Engine: SQLserver-ex
   - Major engine version: 12.00

   Jeśli na etapie tworzenia instancji Amazon RDS wybrałeś inną bazę danych SQL, wybierz odpowiedni silnik.

Grupa zostanie utworzona i będzie wyświetlana na liście grup.

Po utworzeniu grupy opcji, umieść swoją instancję Amazon RDS w tej grupie opcji.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Modyfikowanie grupy opcji

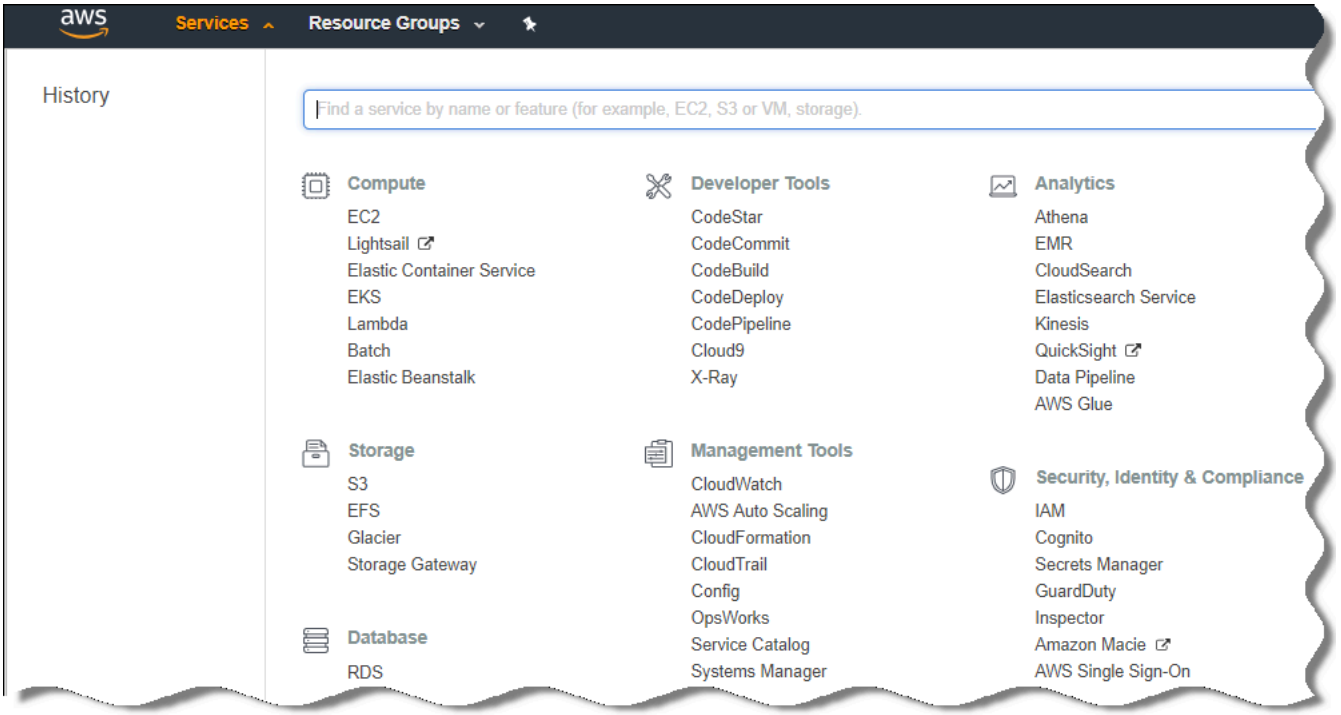
Domyślna konfiguracja grupy opcji, w której umieściłeś instancję Amazon RDS nie jest wystarczająca do pracy z bazą danych Kaspersky Security Center. Musisz dodać opcje do grupy opcji i utworzyć nową rolę IAM do pracy z bazą danych.

W celu zmodyfikowania grupy opcji i utworzenia nowej roli IAM:

1. Upewnij się, że jesteś w konsoli AWS Management Console (https://console.aws.amazon.com) i zalogowałeś się do niej z poziomu swojego konta.

2. W wierszu menu kliknij **Usługi**.

   Zostanie wyświetlona lista dostępnych usług (patrz rysunek poniżej).



Lista usług w konsoli AWS Management Console

3. Na liście wybierz RDS.

4. W lewym panelu kliknij **Grupy opcji**.

   Zostanie wyświetlona lista grup opcji.

5. Wybierz grupę opcji, w której umieściłeś swoją instancję Amazon RDS, i kliknij przycisk **Dodaj opcję**.

   Zostanie otwarte okno **Dodaj opcję**.

6. W sekcji Rola IAM wybierz opcję **Utwórz nową rolę** / **Tak** i wprowadź nazwę nowej roli IAM.

   Rola jest tworzona z domyślnym zestawem uprawnień. Następnie będziesz musiał zmienić jej uprawnienia.

7. W sekcji Komora S3 wykonaj jedną z następujących czynności:

   - Jeśli nie utworzyłeś instancji komory Amazon S3 dla kopii zapasowej danych, wybierz odnośnik **Utwórz nową komorę S3** i utwórz nową komorę S3, korzystając z interfejsu S3.
   - Jeśli już utworzyłeś instancję komory Amazon S3 dla zadania tworzenia kopii zapasowej danych Serwera administracyjnego, wybierz swoją komorę S3 z listy rozwijalnej.

8. Zakończ dodawanie opcji, klikając przycisk **Dodaj opcję** w dolnej części strony.

Zmodyfikowałeś grupę opcji i utworzyłeś nową rolę IAM do pracy z bazą danych RDS.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Modyfikowanie uprawnień dla roli IAM dla instancji bazy danych Amazon RDS

Po dodaniu opcji do grupy opcji, musisz przypisać wymagane uprawnienia do roli IAM, którą utworzyłeś do pracy z instancją bazy danych Amazon RDS.

W celu przypisania wymaganych uprawnień do roli IAM, którą utworzyłeś do pracy z instancją bazy danych Amazon RDS:

1. Upewnij się, że jesteś w konsoli AWS Management Console (https://console.aws.amazon.com) i zalogowałeś się do niej z poziomu swojego konta.
2. Na liście usług wybierz **IAM**.

   Zostanie otwarte okno zawierające listę nazw użytkowników i menu, które umożliwia pracę z narzędziem.
3. W menu wybierz **Role**.
4. Na liście ról IAM, wyświetlonych w obszarze roboczym, wybierz rolę, którą utworzyłeś podczas dodawania opcji do grupy opcji.
5. Korzystając z interfejsu AWS, usuń zasadę **sqlNativeBackup-<date>**.
6. Korzystając z interfejsu AWS, przyłącz zasadę **AmazonS3FullAccess** do roli.

Do roli IAM zostają przypisane wymagane uprawnienia do pracy z Amazon RDS.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Przygotowanie komory Amazon S3 dla bazy danych

Jeśli planujesz korzystać z bazy danych Amazon Relational Database System (Amazon RDS), musisz utworzyć instancję komory Amazon Simple Storage Service (Amazon S3), gdzie będzie przechowywana regularna kopia zapasowa bazy danych. Informacje o komorze Amazon S3 i komorze S3 znajdziesz na stronach pomocy Amazon. Więcej informacji na temat tworzenia instancji Amazon S3 znajdziesz na stronie pomocy Amazon S3.

W celu utworzenia komory Amazon S3:

1. Upewnij się, że konsola AWS Management Console jest otwarta i zalogowałeś się na swoje konto.
2. Na liście usług AWS wybierz S3.
3. Nawiguj po konsoli, aby utworzyć komorę, wykonując instrukcje kreatora.
4. Wybierz ten sam region, w którym znajduje się Serwer administracyjny (lub będzie się znajdował).
5. Jeśli kreator zakończy pracę, upewnij się, że nowa komora pojawi się na liście komór.

Nowa komora S3 została utworzona i pojawiła się na Twojej liście komór. Musisz określić tę komorę podczas dodawania opcji do grupy opcji. Będziesz musiał także określić adres Twojej komory S3 do Kaspersky Security Center, gdy Kaspersky Security Center tworzy zadanie *Kopia zapasowa danych Serwera administracyjnego*.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Przenoszenie bazy danych do Amazon RDS

Możesz przenieść swoją bazę danych Kaspersky Security Center z urządzenia lokalnego do instancji Amazon S3, która obsługuje Amazon RDS. Aby to zrobić, potrzebujesz komory S3 dla bazy danych RDS i konta użytkownika IAM z uprawnieniem AmazonS3FullAccess dla tej komory S3.

W celu przeniesienia bazy danych:

1. Upewnij się, że utworzyłeś instancję RDS (więcej informacji znajdziesz na stronach referencyjnych Amazon RDS).
2. Na swoim fizycznym Serwerze administracyjnym (lokalnym) uruchom narzędzie Kaspersky Backup, aby utworzyć kopię zapasową danych Serwera administracyjnego.

   Musisz upewnić się, że plik nosi nazwę backup.zip.
3. Skopiuj plik backup.zip na instancję EC2, na której jest zainstalowany Serwer administracyjny.

   Upewnij się, że posiadasz wystarczającą ilość miejsca na instancji EC2, na której jest zainstalowany Serwer administracyjny. W środowisku AWS możesz dodać przestrzeń dyskową do swojej instancji, aby ulokować proces migracji bazy danych.
4. Na Serwerze administracyjnym AWS uruchom ponownie narzędzie Kaspersky Backup w trybie interaktywnym.

   Zostanie uruchomiony Kreator tworzenia kopii zapasowej i przywracania.
5. W kroku **Wybierz akcję** wybierz **Przywróć dane Serwera administracyjnego** i kliknij **Dalej**.
6. W kroku **Przywróć ustawienia** kliknij przycisk **Przeglądaj** obok **Folder przechowujący kopie zapasowe**.
7. W otwartym oknie **Zaloguj się do magazynu online** wypełnij następujące pola, a następnie kliknij **OK**:

   - **Nazwa komory S3**

     Nazwa Twojej komory S3.

- **Folder kopii zapasowej**

  Określ lokalizację folderu magazynu, który jest przeznaczony dla kopii zapasowej.

- **Identyfikator klucza dostępu**

  Identyfikator klucza dostępu IAM AWS, który należy do użytkownika IAM posiadającego uprawnienia do korzystania z komory S3 (uprawnienie AmazonS3FullAccess).

- **Tajny klucz**

  Tajny klucz IAM AWS, który należy do użytkownika IAM posiadającego uprawnienia do korzystania z komory S3 (uprawnienie AmazonS3FullAccess).

8. Wybierz opcję **Przenieś z lokalnej kopii zapasowej**. Przycisk **Przeglądaj** stanie się dostępny.
9. Kliknij przycisk **Przeglądaj**, aby wybrać folder na Serwerze administracyjnym AWS, na który skopiowałeś plik backup.zip.
10. Kliknij **Dalej** i zakończ procedurę.

Twoje dane zostaną przywrócone do bazy danych RDS przy użyciu komory S3. Możesz użyć tej bazy danych do dalszej pracy z Kaspersky Security Center w środowisku AWS.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Praca w środowisku chmury Microsoft Azure

Ta sekcja zawiera informacje dotyczące instalacji i obsługi Kaspersky Security Center w środowisku chmury dostarczonym przez Microsoft Azure, a także szczegóły wdrożenia ochrony na maszynach wirtualnych w tym środowisku w chmurze.

W programie Kaspersky Security Center, który został zainstalowany z opcji Usage-based monthly billed SKU, Zarządzanie lukami i poprawkami jest automatycznie aktywowane, a Zarządzanie urządzeniami mobilnymi nie może zostać aktywowane.

Informacje o pracy w Microsoft Azure

Aby pracować z platformą Microsoft Azure, w szczególności, aby kupić aplikacje w Azure Marketplace i utworzyć maszyny wirtualne, będziesz potrzebował subskrypcję Azure. Przed zainstalowaniem Serwera administracyjnego, utwórz ID aplikacji Azure z uprawnieniami wymaganymi do zainstalowania aplikacji na maszynach wirtualnych.

Jeśli kupisz obraz Kaspersky Security Center w sklepie Azure Marketplace, możesz zainstalować maszynę wirtualną z gotowym do użycia Serwerem administracyjnym Kaspersky Security Center. Musisz wybrać ustawienia maszyny wirtualnej, ale nie musisz sam instalować aplikacji. Po instalacji, możesz uruchomić Konsolę administracyjną i połączyć się z Serwerem administracyjnym, aby rozpocząć pracę z Kaspersky Security Center.

Możesz również użyć maszyny wirtualnej Azure, na której jest zainstalowany Serwer administracyjny Kaspersky Security Center, aby chronić urządzenia lokalne (na przykład, jeśli serwer chmury okazuje się być łatwiejszy w obsłudze i utrzymaniu niż fizyczny). W takim przypadku możesz pracować z Serwerem administracyjnym tak samo, jak gdyby Serwer administracyjny był zainstalowany na urządzeniu lokalnym. Jeśli nie planujesz korzystać z narzędzi Azure API, nie potrzebujesz ID aplikacji Azure. W tym przypadku subskrypcja Azure jest wystarczająca.

Tworzenie subskrypcji, identyfikatora aplikacji i hasła

Aby pracować z Kaspersky Security Center w środowisku Microsoft Azure, potrzebujesz subskrypcji Azure, ID aplikacji Azure oraz hasła do aplikacji Azure. Możesz użyć istniejącej subskrypcji, jeśli ją posiadasz.

Subskrypcja Azure daje właścicielowi dostęp do portalu Microsoft Azure Platform Management Portal oraz do usług Microsoft Azure. Właściciel może użyć platformy Microsoft Azure Platform do zarządzania usługami takimi, jak Azure SQL i magazyn Azure.

W celu utworzenia subskrypcji Microsoft Azure:

Przejdź do https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription i postępuj zgodnie z instrukcjami.

Więcej informacji dotyczących tworzenia subskrypcji można znaleźć na stronie internetowej Microsoft. Uzyskasz ID subskrypcji, który później dostarczysz Kaspersky Security Center wraz z ID aplikacji i hasłem.

W celu utworzenia i zapisania ID aplikacji Azure i hasła:

1. Przejdź do https://portal.azure.com i upewnij się, że jesteś zalogowany.
2. Wykonując instrukcje na stronie referencyjnej, utwórz ID aplikacji.
3. Przejdź do sekcji **Klucze** ustawień aplikacji.
4. W sekcji **Klucze** wypełnij pola **Opis** i **Utraci ważność** i pozostaw pole **Wartość** puste.
5. Kliknij **Zapisz**.

   Jeśli klikniesz **Zapisz**, system automatycznie uzupełni pole **Wartość** długą sekwencją znaków. Ta sekwencja to Twoje hasło do aplikacji Azure (na przykład: yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). Opis jest wyświetlany w trakcie wpisywania.
6. Skopiuj hasło i zapisz je, abyś mógł później dostarczyć ID aplikacji i hasło do Kaspersky Security Center.

   Hasło można skopiować, jeśli zostało utworzone. Później hasło nie będzie już wyświetlane i nie będzie można go odzyskać.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Przypisywanie roli do ID aplikacji w Azure

Jeśli chcesz tylko wykrywać maszyny wirtualne przy pomocy wykrywania urządzeń, Twój ID aplikacji Azure musi posiadać rolę Czytelnik. Jeśli chcesz nie tylko wykrywać maszyny wirtualne, ale także wdrożyć ochronę na maszynach wirtualnych, Twój ID aplikacji Azure musi posiadać rolę Współautor maszyny wirtualnej.

Postępuj zgodnie z instrukcjami na stronie internetowej Microsoft, aby przypisać rolę do swojego ID aplikacji Azure.

Instalowanie Serwera administracyjnego w Microsoft Azure i wybieranie bazy danych

W celu zainstalowania Serwera administracyjnego w środowisku Microsoft Azure:

1. Zaloguj się do Microsoft Azure, korzystając ze swojego konta.
2. Przejdź na portal Azure.
3. W lewym panelu kliknij zielony znak plusa.
4. W polu wyszukiwania w menu wpisz „Kaspersky Hybrid Cloud Security”.

   Kaspersky Hybrid Cloud Security to kombinacja Kaspersky Security Center i dwóch aplikacji zabezpieczających do ochrony instancji: Kaspersky Endpoint Security for Linux i Kaspersky Security for Windows Server.
5. Na liście wyników wybierz Kaspersky Hybrid Cloud Security lub Kaspersky Hybrid Cloud Security (BYOL).

   W prawej części okna pojawi się okno z informacjami.
6. Przeczytaj informacje i kliknij przycisk Utwórz u dołu okna z informacjami.
7. Wypełnij wszystkie potrzebne pola. Użyj etykietki narzędzi, aby uzyskać informacje i pomoc.
8. Podczas wybierania rozmiaru wybierz jedną z trzech opcji oznaczonych gwiazdką.

   W większości przypadków wystarcza 8 gigabajtów (GB) pamięci RAM. Jednakże w Azure możesz zwiększyć rozmiar pamięci RAM i inne zasoby maszyny wirtualnej w dowolnym momencie.

9. Podczas wybierania bazy danych wybierz jedną zgodnie ze swoim planem:

   - Lokalna—jeśli chcesz bazę danych na tej samej maszynie wirtualnej, na której jest zainstalowany Serwer administracyjny. Kaspersky Security Center jest dostarczany z bazą danych SQL Server Express. Wybierz tę opcję, jeśli SQL Server Express jest wystarczający dla Twoich potrzeb.

   - Nowa—jeśli chcesz nową bazę danych RDS w środowisku Azure. Wybierz tę opcję, jeśli chcesz system DBMS inny niż SQL Server Express. Twoje dane zostaną przesłane do środowiska chmury, gdzie pozostaną, i nie będziesz ponosił dodatkowych wydatków.

   - Istniejąca—jeśli chcesz, żeby użyć istniejącego serwera bazy danych. W tym przypadku będziesz musiał określić jego lokalizację. Jeśli ten serwer znajduje się poza środowiskiem Azure, Twoje dane zostaną przesłane przez internet, co może generować dodatkowe koszty.

10. Podczas wprowadzania ID subskrypcji użyj subskrypcji, którą utworzyłeś wcześniej.

    Po zainstalowaniu, możesz nawiązać połączenie z Serwerem administracyjnym przy użyciu RDP. Do pracy z Serwerem administracyjnym możesz użyć Konsoli administracyjnej.

Praca z Azure SQL

Ta sekcja opisuje działania, jakie mają zostać podjęte w celu przygotowania bazy danych Microsoft Azure dla Kaspersky Security Center, przygotowania konta magazynu Azure, a także przeniesienia istniejącej bazy danych do Azure SQL.

Baza danych SQL jest zarządzaną usługą bazy danych mającą ogólne przeznaczenie w Microsoft Azure.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Tworzenie konta magazynu Azure

Musisz utworzyć konto magazynu w Microsoft Azure do pracy z bazą danych Azure SQL oraz dla skryptów instalacyjnych.

W celu utworzenia konta magazynu:

1. Zaloguj się do portalu Azure.

2. W lewej części okna wybierz **Konta magazynu**, aby przejść do okna **Konta magazynu**.

3. W oknie **Konta magazynu** kliknij przycisk **Dodaj**, aby przejść do okna **Utwórz konto magazynu**.

4. W celu utworzenia konta magazynu wypełnij wszystkie potrzebne pola:

   - Lokalizacja: musi być taka sama jak lokalizacja Serwera administracyjnego.

   - Pozostałe pola: możesz zostawić domyślne wartości.

   Użyj etykietki narzędzi, aby uzyskać informacje o każdym polu.

   Po utworzeniu konta, zostanie wyświetlona lista Twoich kont magazynu.

5. Na liście kont magazynu kliknij nazwę nowo utworzonego konta, aby zobaczyć informacje o tym koncie.

6. Upewnij się, że znasz nazwę konta, grupę zasobu oraz klucze dostępu dla tego konta magazynu. Będziesz potrzebował tych informacji do pracy z Kaspersky Security Center.

Więcej informacji znajdziesz na stronie Azure.

Jeśli już posiadasz konto magazynu, możesz go użyć do pracy z Kaspersky Security Center.

Tworzenie bazy danych Azure SQL i serwera SQL

W środowisku Azure potrzebujesz bazy danych SQL i serwera SQL.

W celu utworzenia bazy danych Azure SQL i serwera SQL:

1. Postępuj zgodnie z instrukcjami na stronie internetowej Azure.

   Możesz utworzyć nowy serwer, gdy Microsoft Azure wyświetli pytanie o wykonanie tego działania; jeśli już masz serwer Azure SQL Server, możesz użyć go dla Kaspersky Security Center niż do utworzenia nowego.

2. Po utworzeniu bazy danych SQL i serwera SQL, upewnij się, że znasz nazwę zasobu i grupę zasobu:

   a. Przejdź do https://portal.azure.com i upewnij się, że jesteś zalogowany.

   b. W lewej części okna wybierz **bazy danych SQL**.

   c. Kliknij nazwę bazy danych z listy swoich baz danych.

      Zostanie otwarte okno właściwości.

   d. Nazwa bazy danych to nazwa zasobu. Nazwa grupy zasobu jest wyświetlana w sekcji **Podgląd** okna właściwości.

Nazwa zasobu i grupa zasobu bazy danych są potrzebne do przeniesienia bazy danych do Azure SQL.

Przenoszenie bazy danych do Azure SQL

Po wdrożeniu Serwera administracyjnego w środowisku Azure, możesz przenieść swoją bazę danych Kaspersky Security Center z lokalnego urządzenia do Azure SQL. Dla bazy danych Azure SQL potrzebne jest konto magazynu Azure. Musisz także posiadać Microsoft SQL Server Data-Tier Application Framework (DacFx) oraz SQLSysCLRTypes na swoim Serwerze administracyjnym.

W celu przeniesienia bazy danych:

1. Upewnij się, że utworzyłeś konto magazynu Azure.

2. Upewnij się, że posiadasz SQLSysCLRTypes i DacFx na swoim Serwerze administracyjnym.

   Możesz pobrać Microsoft SQL Server Data-Tier Application Framework (17.0.1 DacFx) i SQLSysCLRTypes (wybierz wersję odpowiadającą wersji Twojego serwera SQL Server) z oficjalnej strony internetowej Microsoft.

3. Na swoim fizycznym Serwerze administracyjnym (lokalnym) uruchom narzędzie Kaspersky Backup, aby utworzyć kopię zapasową danych Serwera administracyjnego, z włączoną opcją **Wykonaj migrację do formatu Azure**.

4. Skopiuj plik kopii zapasowej na Serwer administracyjny Azure.

> Upewnij się, że posiadasz wystarczającą ilość miejsca na maszynie wirtualnej Azure, na której jest zainstalowany Serwer administracyjny. W środowisku Azure możesz dodać przestrzeń dyskową do swoich maszyn wirtualnych, aby ulokować proces migracji bazy danych.

5. Na Serwerze administracyjnym znajdującym się w środowisku Microsoft Azure uruchom ponownie narzędzie Kaspersky Backup w trybie interaktywnym.

   Zostanie uruchomiony Kreator tworzenia kopii zapasowej i przywracania.

6. W kroku **Wybierz akcję** wybierz **Przywróć dane Serwera administracyjnego** i kliknij **Dalej**.

7. W kroku **Przywróć ustawienia** kliknij przycisk **Przeglądaj** obok **Folder przechowujący kopie zapasowe**.

8. W otwartym oknie **Zaloguj się do magazynu online** wypełnij następujące pola, a następnie kliknij **OK**:

   - **Nazwa konta magazynu Azure**

     Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

   - **Folder kopii zapasowej**

     Określ lokalizację folderu magazynu, który jest przeznaczony dla kopii zapasowej.

   - **ID subskrypcji Azure**

     Subskrypcję utworzyłeś na portalu Azure.

   - **Hasło do aplikacji Azure**

     Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

     Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

   - **Klucz dostępu do magazynu Azure**

     Dostępne we właściwościach Twojego konta magazynu, w sekcji Klucze dostępu. Możesz użyć dowolnego klucza (key1 lub key2).

   - **Nazwa serwera Azure SQL**

     Dostępne we właściwościach Twojego serwera Azure SQL.

   - **Grupa zasobów serwera Azure SQL**

     Dostępne we właściwościach Twojego serwera Azure SQL.

   - **ID aplikacji Azure**

     Ten ID aplikacji utworzyłeś na portalu Azure.

     Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

9. Wybierz opcję **Przenieś z lokalnej kopii zapasowej**.

   Przycisk **Przeglądaj** stanie się dostępny.

10. Kliknij przycisk **Przeglądaj**, aby wybrać folder na Serwerze administracyjnym Azure, na który skopiowałeś plik kopii zapasowej.

11. Kliknij **Dalej** i zakończ procedurę.

    Twoje dane zostaną przywrócone do bazy danych Azure SQL przy użyciu Twojego magazynu Azure. Możesz użyć tej bazy danych do dalszej pracy z Kaspersky Security Center w środowisku Azure.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Praca w Google Cloud

Ta sekcja zawiera informacje o pracy z Kaspersky Security Center w środowisku chmury udostępnianym przez Google.

Tworzenie adresu e-mail klienta, identyfikatora projektu i klucza prywatnego

Możesz użyć Google API do pracy z Kaspersky Security Center w Google Cloud Platform. Wymagane jest konto Google. Więcej informacji można znaleźć w dokumentacji Google pod adresem https://cloud.google.com.

Konieczne będzie utworzenie i wprowadzenie w Kaspersky Security Center następujących poświadczeń:

- **E-mail klienta**

  Wprowadź adres e-mail klienta, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Identyfikator projektu**

  Identyfikator projektu to identyfikator, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Klucz prywatny**

  Klucz prywatny to sekwencja znaków, które otrzymałeś jako klucz prywatny po zarejestrowaniu projektu w Google Cloud. Możesz skopiować i wkleić tę sekwencję, aby uniknąć błędów.

Praca z Google Cloud SQL dla instancji MySQL

Możesz utworzyć bazę danych w Google Cloud i używać tej bazy danych dla Kaspersky Security Center.

Kaspersky Security Center współpracuje z MySQL 5.7 i 5.6. Inne wersje MySQL nie zostały przetestowane.

W celu utworzenia i skonfigurowania bazy danych MySQL:

W swojej przeglądarce otwórz stronę https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen i postępuj zgodnie z dostępnymi instrukcjami.

Podczas konfigurowania bazy danych MySQL użyj następujących flag:

- **sort_buffer_size** 10000000
- **join_buffer_size** 20000000
- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **lower_case_table_names** 1

Wymagania wstępne urządzeń klienckich w środowisku chmury niezbędnych do pracy z Kaspersky Security Center

Urządzenia, na których zamierzasz zainstalować Serwer administracyjny, Agenta sieciowego i aplikacje zabezpieczające Kaspersky, muszą spełniać następujące warunki:

- Konfiguracja grup zabezpieczeń udostępnia następujące porty na Serwerze administracyjnym (minimalny zestaw portów wymaganych do wdrożenia):
  - 8060 HTTP—do przesyłania pakietów instalacyjnych Agenta sieciowego i pakietów instalacyjnych aplikacji zabezpieczających z Serwera administracyjnego na chronione instancje
  - 8061 HTTPS — do przesyłania pakietów instalacyjnych Agenta sieciowego i pakietów instalacyjnych aplikacji zabezpieczających z Serwera administracyjnego na chronione instancje
  - 13000 TCP—dla przesyłania z chronionych instancji i podrzędnych Serwerów administracyjnych do głównego Serwera administracyjnego przy użyciu SSL
  - 13000 UDP—do przesyłania informacji o zamknięciu instancji na Serwer administracyjny
  - 14000 TCP—dla przesyłania z chronionych instancji i podrzędnych Serwerów administracyjnych do głównego Serwera administracyjnego bez użycia SSL
  - 13291—do łączenia Konsoli administracyjnej z Serwerem administracyjnym
  - 40080—do działania skryptów instalacyjnych

  Możesz skonfigurować grupy bezpieczeństwa w konsoli AWS Management Console lub na portalu Azure. Jeśli zamierzasz używać Kaspersky Security Center w niedomyślnej konfiguracji, zapoznaj się z Bazą wiedzy. Przykłady niedomyślnej konfiguracji obejmują nie instalowanie Konsoli administracyjnej na Serwerze administracyjnym, ale zainstalowanie jej na stacji roboczej lub przy pomocy serwera proxy KSN.
- Port UDP o numerze 15000 jest dostępny na urządzeniach klienckich (do odbierania żądań komunikacji z Serwerem administracyjnym).

- W środowisku chmury AWS:
  - Jeśli planujesz korzystać z AWS API, ustawiona jest rola IAM, pod którą aplikacje zostaną zainstalowane na instancjach.
  - Na każdej instancji Amazon EC2 zainstalowany i uruchomiony jest Agent SSM (Systems Manager Agent).
  - Agent SSM umożliwia Kaspersky Security Center automatyczne instalowanie aplikacji na urządzeniach i grupach urządzeń bez wyświetlania pytania o potwierdzenie administratora za każdym razem.
  - Na instancjach, na których jest zainstalowany system operacyjny Windows i które zostały wdrożone z obrazów AMI później niż w listopadzie 2016 roku, agent SSM jest zainstalowany i uruchomiony. Na wszystkich pozostałych urządzeniach należy ręcznie zainstalować agenta SSM. Więcej informacji na temat instalowania agenta SSM na urządzeniach działających pod kontrolą systemów operacyjnych Windows i Linux można znaleźć na stronie pomocy AWS.
- W środowisku chmury Microsoft Azure:
  - Na każdej maszynie wirtualnej Azure zainstalowany i uruchomiony jest Agent Azure VM.

    Domyślnie, nowa maszyna wirtualna jest tworzona z Agentem Azure VM i nie musisz go ręcznie instalować ani włączać. Więcej informacji o Agencie Azure VM znajdziesz w pomocy firmy Microsoft dla urządzeń Windows i urządzeń Linux.
  - Twój ID aplikacji Azure posiada następujące role:
    - Czytelnik (do wykrywania maszyn wirtualnych przy użyciu przeszukiwania)
    - Współautor maszyny wirtualnej (do wdrażania ochrony na maszynach wirtualnych)
    - Współautor serwera SQL (do używania bazy danych SQL w środowisku Microsoft Azure)

    Jeśli chcesz wykonywać wszystkie te działania, przypisz wszystkie trzy role do swojego ID aplikacji Azure.

Tworzenie pakietów instalacyjnych wymaganych do konfiguracji środowiska chmury

Kreator konfiguracji środowiska chmury w Kaspersky Security Center jest dostępny, jeśli masz pakiety instalacyjne i wtyczki administracyjne dla następujących programów:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

  > Wdrożenie Kaspersky Endpoint Security for Windows w środowisku chmurowym będzie dostępne po nadchodzącej wersji Kaspersky Endpoint Security 12.0 for Windows.

- Kaspersky Security for Windows Server

Te pakiety instalacyjne są wymagane do zainstalowania aplikacji na instancjach lub maszynach wirtualnych, które chcesz chronić. Jeśli nie masz tych pakietów instalacyjnych, musisz je utworzyć. W przeciwnym razie Kreator konfiguracji środowiska chmury nie będzie działać.

W celu utworzenia pakietów instalacyjnych:

1. Pobierz najnowsze wersje aplikacji i wtyczek ze strony internetowej Kaspersky:
   - Instalator i wtyczkę zarządzającą dla Kaspersky Security for Windows Server.
   - Instalator, pliki dla zdalnej instalacji za pośrednictwem Kaspersky Security Center oraz wtyczkę zarządzającą dla Kaspersky Endpoint Security for Linux.
2. Zapisz wszystkie pliki na instancji (lub maszynie wirtualnej), na której jest zainstalowany Serwer administracyjny.
3. Wyodrębnij pliki ze wszystkich pakietów.
4. Uruchom Kaspersky Security Center.
5. W drzewie konsoli przejdź do **Zaawansowane** → **Zdalna instalacja** → **Pakiety instalacyjne** i kliknij **Utwórz pakiet instalacyjny**.
6. Wybierz **Utwórz pakiet instalacyjny Kaspersky**.
7. Określ nazwę pakietu i ścieżkę do instalatora aplikacji: <folder>\<nazwa pliku>.kud, a następnie kliknij **Dalej**.
8. Przeczytaj Umowę licencyjną i zaznacz pole potwierdzające, że zaakceptowałeś jej warunki, a następnie kliknij **Dalej**.

Pakiet instalacyjny zostanie przesłany na Serwer administracyjny i będzie dostępny na liście pakietów instalacyjnych.

Konfiguracja środowiska chmury stanie się dostępna, gdy tylko utworzysz pakiety instalacyjne i zainstalujesz wtyczki administracyjne na Serwerze administracyjnym.

Konfigurowanie środowiska chmury

Aby skonfigurować Kaspersky Security Center przy użyciu Kreatora konfiguracji środowiska chmury, musisz mieć:

- Następujące dane uwierzytelniające środowiska w chmurze:
  - Rolę IAM, której udzielono uprawnienie do przeszukiwania segmentu chmury lub konto użytkownika IAM, któremu udzielono uprawnienia do przeszukiwania segmentu chmury (do pracy z Amazon Web Services)
  - ID aplikacji Azure, hasło i subskrypcję (do pracy z Microsoft Azure)
  - Poczta klienta Google, ID projektu i klucz prywatny (do pracy z Google Cloud)
- Pakiety instalacyjne:
  - Agent sieciowy dla systemu Windows
  - Agent sieciowy dla systemu Linux
  - Kaspersky Endpoint Security for Linux
- Wtyczka sieciowa dla Kaspersky Endpoint Security for Linux

- Wybierz jeden z następujących:
  - Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Endpoint Security for Windows (zalecane)
  - Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Security for Windows Server

Jeśli nie chcesz używać funkcji środowiska chmury (na przykład, jeśli chcesz zarządzać ochroną jedynie fizycznych urządzeń klienckich), możesz zamknąć Kreatora konfiguracji środowiska chmury i ręcznie uruchomić standardowego Kreatora wstępnej konfiguracji Serwera administracyjnego.

Operacja Konfigurowanie środowiska chmury uruchamia się automatycznie przy pierwszym połączeniu z Serwerem administracyjnym za pośrednictwem Konsoli administracyjnej, jeśli instalujesz Kaspersky Security Center z gotowego do użycia obrazu. Kreator konfiguracji środowiska chmury można również uruchomić ręcznie w dowolnym momencie.

Aby ręcznie uruchomić Kreatora konfiguracji środowiska chmury:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego węzła wybierz **All Tasks** → **Konfiguruj środowisko chmury**.

Średni czas pracy wynosi około 15 minut.

Informacje o Kreatorze konfiguracji środowiska chmury

Kreator konfiguracji środowiska chmury umożliwia skonfigurowanie Kaspersky Security Center z uwzględnieniem specyfiki pracy w środowisku chmury.

kreator tworzy następujące obiekty:

- Zasada Agenta sieciowego z ustawieniami domyślnymi
- Zasada dla Kaspersky Endpoint Security for Linux
- Zasada dla Kaspersky Security for Windows Server
- Grupa administracyjna dla instancji i reguła dla automatycznego przenoszenia instancji do tej grupy administracyjnej
- Zadanie tworzenia kopii zapasowej danych Serwera administracyjnego
- Zadania instalowania ochrony na urządzeniach działających pod kontrolą systemu Linux i Windows
- Zadania dla każdego zarządzanego urządzenia:
  - Szybkie skanowanie w poszukiwaniu złośliwego oprogramowania
  - Pobieranie uaktualnień

Jeśli wybrano opcję licencjonowania BYOL, konfigurowanie środowiska chmury aktywuje również Kaspersky Security Center za pomocą pliku klucza lub kodu aktywacyjnego i umieszcza plik klucza lub kod aktywacyjny w magazynie licencji.

Krok 1. Wybieranie metody aktywacji aplikacji

Ten krok nie jest wyświetlany, jeśli zarejestrowano się dla jednego z gotowych do użycia obrazów AMI (w AWS Marketplace) lub dla opcji Usage-based monthly billed SKU (w Azure Marketplace). W takim przypadku kreator natychmiast przechodzi do następnego kroku. Jednakże nie możesz kupić gotowego do użycia obrazu AMI dla Google Cloud.

Jeśli wybrałeś opcję licencjonowania BYOL dla Kaspersky Security Center, kreator wyświetli pytanie o wybór metody aktywacji aplikacji.

Aktywuj aplikację przy użyciu kodu aktywacyjnego / pliku klucza dla Kaspersky Security for Virtualization lub dla Kaspersky Hybrid Cloud Security.

Możesz aktywować aplikację w jeden z następujących sposobów:

- Wprowadzając kod aktywacyjny.

  Rozpocznie się aktywacja online. Ten proces będzie obejmował weryfikację określonego kodu aktywacyjnego, a także wydanie i aktywację pliku klucza.

- Określając plik klucza.

  Aplikacja sprawdzi plik klucza i dokona aktywacji, jeśli zawiera poprawne informacje, lub wyświetli okno z prośbą o określenie innego pliku klucza.

Kaspersky Security Center umieszcza klucz licencyjny w magazynie licencji i oznacza go jako klucz rozsyłany automatycznie na zarządzane urządzenia.

Jeśli łączysz się z instancją przy użyciu standardowego Podłączania pulpitu zdalnego w Microsoft Windows lub podobnej aplikacji, we właściwościach połączenia zdalnego należy określić napęd urządzenia fizycznego, którego używasz do nawiązania połączenia. Zapewnia to dostęp z instancji do plików na urządzeniu fizycznym oraz pozwala wybrać i określić plik klucza.

Podczas pracy z Kaspersky Security Center zainstalowanym z płatnego obrazu AMI lub dla Usage-based monthly billed SKU nie można dodawać plików kluczy lub kodów aktywacyjnych do magazynu licencji.

Krok 2. Wybieranie środowiska chmury

Wybierz środowisko chmury, w którym instalujesz Kaspersky Security Center: AWS, Azure lub Google Cloud.

Krok 3. Autoryzacja w środowisku chmury

AWS

Jeśli wybrałeś AWS, określ, czy posiadasz rolę IAM z wymaganymi uprawnieniami, lub zapewnij Kaspersky Security Center klucz dostępu IAM AWS. Przeszukiwanie segmentu chmury nie jest możliwe bez roli IAM lub klucza dostępu IAM AWS.

Skonfiguruj następujące ustawienia dla połączenia, które będą używane do dalszego przeszukiwania segmentu chmury:

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment", „AWS Segment" lub „Google Segment".

- **Użyj roli AWS IAM**

  Wybierz tę opcję, jeśli już utworzyłeś rolę IAM dla Serwera administracyjnego do korzystania z usług AWS.

- **Użyj konta użytkownika AWS IAM**

  Wybierz tę opcję, jeśli posiadasz konto użytkownika IAM z wymaganymi uprawnieniami oraz możesz wprowadzić ID klucza oraz tajny klucz.

  - **Identyfikator klucza dostępu**

    Identyfikator klucza dostępu IAM to sekwencja znaków alfanumerycznych. Identyfikator klucza otrzymałeś podczas tworzenia konta użytkownika IAM.

    Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

  - **Tajny klucz**

    Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

    Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

    Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

To połączenie zostanie zapisane w ustawieniach aplikacji. Możesz utworzyć tylko jeden klucz dostępu AWS IAM za pomocą konfiguracji środowiska chmury. Możesz określić więcej połączeń do zarządzania innymi segmentami chmury.

Jeśli chcesz zainstalować aplikacje na instancjach poprzez Kaspersky Security Center, upewnij się, że Twoja rola IAM (lub użytkownik IAM, którego konto jest skojarzone z wprowadzanym kluczem) posiada wszystkie wymagane uprawnienia.

Azure

Jeśli wybrałeś Azure, skonfiguruj następujące ustawienia dla połączenia, które będą używane do dalszego przeszukiwania segmentu chmury:

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment", „AWS Segment" lub „Google Segment".

- **ID aplikacji Azure**

  Ten ID aplikacji utworzyłeś na portalu Azure.

  Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **ID subskrypcji Azure**

  Subskrypcję utworzyłeś na portalu Azure.

- **Hasło do aplikacji Azure**

  Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

  Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

- **Nazwa konta magazynu Azure**

  Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

- **Klucz dostępu do magazynu Azure**

  Hasło (klucz) uzyskałeś po utworzeniu konta magazynu Azure do pracy z Kaspersky Security Center.

  Klucz jest dostępny w sekcji „Overview of the Azure storage account", w podsekcji „Keys".

To połączenie zostanie zapisane w ustawieniach aplikacji.

Google Cloud

Jeśli wybrałeś Google Cloud, określ następujące ustawienia dla połączenia, które będą używane do dalszego przeszukiwania segmentu chmury:

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment", „AWS Segment" lub „Google Segment".

- **E-mail klienta**

  Wprowadź adres e-mail klienta, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Identyfikator projektu**

  Identyfikator projektu to identyfikator, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Klucz prywatny**

  Klucz prywatny to sekwencja znaków, które otrzymałeś jako klucz prywatny po zarejestrowaniu projektu w Google Cloud. Możesz skopiować i wkleić tę sekwencję, aby uniknąć błędów.

To połączenie zostanie zapisane w ustawieniach aplikacji.

Krok 4. Konfigurowanie synchronizacji z chmurą i wybieranie dalszych działań

W tym kroku rozpoczyna się przeszukiwanie segmentu chmury i tworzona jest grupa administracyjna dla instancji. Instancje, wykryte podczas przeszukiwania, zostają umieszczone w tej grupie. Konfigurowany jest terminarz przeszukiwania segmentu chmury (domyślnie, co 5 minut).

Tworzona jest także reguła automatycznego przydzielania **Synchronizuj z chmurą**. Dla każdego kolejnego skanowania sieci chmury, wykryte urządzenia wirtualne zostaną przeniesione do odpowiedniej podgrupy w obrębie grupy **Zarządzane urządzenia\Chmura**.

W oknie **Synchronizacja z segmentem chmury** możesz zdefiniować następujące ustawienia:

- **Synchronizuj strukturę grupy administracyjnej z segmentem chmury**

  Jeśli ta opcja jest włączona, grupa **Chmura** jest automatycznie tworzona w obrębie grupy **Zarządzane urządzenia** oraz zostaje uruchomione wyszukiwanie urządzeń w chmurze. Instancje i maszyny wirtualne, które zostały wykryte w trakcie każdego skanowania sieci chmury, zostają umieszczone w grupie Chmura. Struktura podgrup administracyjnych w obrębie tej grupy odpowiada strukturze Twojego segmentu chmury (w AWS, strefy dostępności i grupy położenia nie są przedstawione w strukturze; w Azure, podsieci nie są przedstawione w strukturze). Urządzenia, które nie zostały zidentyfikowane jako instancje w środowisku chmury, znajdują się w grupie **Urządzenia nieprzypisane**. Struktura grupa umożliwia korzystanie z grupowych zadań instalacji do zainstalowania aplikacji antywirusowych na instancjach, a także skonfigurowanie różnych zasad dla różnych grup.

  Jeśli ta opcja jest wyłączona, tworzona jest także grupa **Chmura** oraz uruchamiane jest wyszukiwanie urządzeń; jednakże podgrupy odpowiadające strukturze segmentu chmury nie są tworzone w obrębie tej grupy. Wszystkie wykryte instancje znajdują się w grupie administracyjnej **Chmura**, więc są wyświetlane na jednej liście. Jeśli Twoja praca z Kaspersky Security Center wymaga synchronizacji, możesz zmodyfikować właściwości reguły **Synchronizuj z chmurą** i wymusić ją. Wymuszenie tej reguły zmieni strukturę podgrup w grupie Chmura tak, że będzie ona odpowiadała strukturze segmentu chmury.

  Domyślnie opcja ta jest wyłączona.

- **Roześlij ochronę**

  Jeśli ta opcja jest zaznaczona, kreator tworzy zadanie instalacji aplikacji zabezpieczających na instancjach. Po zakończeniu pracy kreatora, na urządzeniach w Twoich segmentach chmury automatycznie uruchamiany jest Kreator wdrażania ochrony, dzięki czemu możliwe będzie zainstalowanie Agenta sieciowego i aplikacji zabezpieczających na tych urządzeniach.

Kaspersky Security Center może przeprowadzić zdalną instalację przy użyciu swoich narzędzi. Jeśli nie masz uprawnień do instalowania aplikacji na instancjach EC2 lub maszynach wirtualnych Azure, możesz ręcznie skonfigurować zadanie **Zdalna instalacja** oraz określić konto z wymaganymi uprawnieniami. W tym przypadku, zadanie Zdalna instalacja nie będzie działało dl urządzeń wykrytych przy użyciu AWS API lub Azure. To zadanie będzie działało tylko dla urządzeń wykrytych przy użyciu przeszukiwania Active Directory, przeszukiwania domeny Windows lub przeszukiwania zakresu IP.

Jeśli ta opcja nie jest zaznaczona, Kreator wdrażania ochrony nie zostanie uruchomiony, a zadania instalacji aplikacji zabezpieczających na instancjach nie zostaną utworzone. Te działania można wykonać ręcznie w późniejszym czasie.

W przypadku Google Cloud możesz przeprowadzić tylko zdalną instalację natywnych narzędzi Kaspersky Security Center. Jeśli wybrałeś Google Cloud, opcja **Roześlij ochronę** nie jest dostępna.

Krok 5. Konfigurowanie Kaspersky Security Network w środowisku chmury

Określ ustawienia przekazywania informacji o działaniach Kaspersky Security Center do bazy wiedzy Kaspersky Security Network. Wybierz jedną z następujących opcji:

- **Zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje zainstalowane na urządzeniach klienckich automatycznie prześlą szczegóły swoich działań do Kaspersky Security Network. Uczestnictwo w Kaspersky Security Network umożliwia szybsze aktualizowanie baz danych zawierających informacje o wirusach i innych zagrożeniach, co zapewnia szybszą reakcję na pojawiające się zagrożenia bezpieczeństwa.

- **Nie zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje nie dostarczą informacji do Kaspersky Security Network.

  Jeśli wybierzesz tę opcję, korzystanie z Kaspersky Security Network zostanie wyłączone.

Kaspersky zaleca uczestniczenie w Kaspersky Security Network.

Krok 6. Konfigurowanie powiadomień e-mail w środowisku chmury

Skonfiguruj dostarczanie powiadomień o zdarzeniach zarejestrowanych podczas działania aplikacji firmy Kaspersky na wirtualnych urządzeniach klienckich. Ustawienia te będą używane jako ustawienia domyślne dla zasad aplikacji.

W celu skonfigurowania dostarczania powiadomień o zdarzeniach występujących w aplikacjach firmy Kaspersky użyj następujących ustawień:

- **Adresaci (adresy e-mail)**

  Adresy e-mail użytkowników, którym aplikacja będzie wysyłała powiadomienia. Możesz wprowadzić jeden lub więcej adresów; jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami.

- **Serwery SMTP**

  Adres lub adresy serwerów pocztowych Twojej organizacji.

Jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
- Nazwa DNS serwera SMTP

- **Port serwera SMTP**

  Numer portu komunikacji serwera SMTP. Jeśli korzystasz z kilku serwerów SMTP, połączenie z nimi jest nawiązywane przez określony port komunikacyjny. Domyślny numer portu to 25.

- **Użyj uwierzytelniania ESMTP**

  Włącza obsługę autoryzacji ESMTP. Po zaznaczeniu opcji, w polach **Nazwa użytkownika** i **Hasło** możesz określić ustawienia autoryzacji ESMTP. Domyślnie pole to nie jest zaznaczone.

Możesz przetestować nowe ustawienia powiadomień e-mail, klikając przycisk **Wyślij wiadomość testową**. Jeśli wiadomość testowa została pomyślnie odebrana przez odbiorców, których adresy zostały określone w polu **Adresaci (adresy e-mail)**, oznacza to, że ustawienia zostały poprawnie skonfigurowane.

Krok 7. Tworzenie wstępnej konfiguracji ochrony środowiska chmury

W tym kroku Kaspersky Security Center automatycznie tworzy zasady i zadania. Okno **Konfiguracja wstępnej ochrony** wyświetla listę zasad i zadań utworzonych przez aplikację.

Jeśli używasz bazy danych RDS w środowisku chmury AWS, podczas tworzenia zadania wykonywania kopii zapasowej Serwera administracyjnego musisz dostarczyć parę kluczy dostępu IAM do Kaspersky Security Center. W tym przypadku wypełnij następujące pola:

- **Nazwa komory S3**

  Nazwa komory S3, którą utworzyłeś dla Kopii zapasowej.

- **Identyfikator klucza dostępu**

  Identyfikator klucza (sekwencja znaków alfanumerycznych) uzyskałeś podczas tworzenia konta użytkownika IAM do pracy z instancją magazynu komory S3.

  Pole jest dostępne, jeśli w komorze S3 wybrałeś bazę danych RDS.

- **Tajny klucz**

  Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

  Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

  Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

Jeśli używasz bazy danych Azure SQL w środowisku chmury Azure, podczas tworzenia zadania wykonywania kopii zapasowej Serwera administracyjnego musisz dostarczyć informacje o serwerze Azure SQL do Kaspersky Security Center. W tym przypadku wypełnij następujące pola:

- **Nazwa konta magazynu Azure**

  Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

- **ID subskrypcji Azure**

  Subskrypcję utworzyłeś na portalu Azure.

- **Hasło do aplikacji Azure**

  Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

  Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

- **ID aplikacji Azure**

  Ten ID aplikacji utworzyłeś na portalu Azure.

  Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **Nazwa serwera Azure SQL**

  Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

- **Grupa zasobów serwera Azure SQL**

  Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

- **Klucz dostępu do magazynu Azure**

  Dostępne we właściwościach Twojego konta magazynu, w sekcji Klucze dostępu. Możesz użyć dowolnego klucza (key1 lub key2).

Jeśli instalujesz Serwer administracyjny w Google Cloud, musisz wybrać folder, w którym będą przechowywane kopie zapasowe. Wybierz folder na swoim dysku lokalnym lub folder na instancji maszyny wirtualnej.

Przycisk **Dalej** stanie się dostępny po utworzeniu wszystkich zasad i zadań, które są niezbędne dla minimalnej konfiguracji ochrony.

Jeśli urządzenie, na którym zadania powinny zostać uruchomione, nie jest widoczne dla Serwera administracyjnego, zadania zostaną uruchomione dopiero wtedy, gdy urządzenie stanie się widoczne. Jeśli tworzysz nową instancję EC2 lub nową maszynę wirtualną, może zająć trochę czasu zanim stanie się widoczna dla Serwera administracyjnego. Jeśli chcesz, żeby Agent sieciowy i aplikacje zabezpieczające zostali zainstalowani na wszystkich nowo utworzonych urządzeń tak szybko, jak to możliwe, Upewnij się, że opcja **Uruchom pominięte zadania** jest włączona dla zadań **Zdalna instalacja aplikacji**. W przeciwnym razie nowo utworzona instancja / maszyna wirtualna nie uzyska Agenta sieciowego i aplikacji zabezpieczających, dopóki zadanie nie zostanie uruchomione zgodnie z jej terminarzem.

Krok 8. Wybieranie działania, jeśli system operacyjny musi być uruchomiony ponownie podczas instalacji (dla środowiska chmury)

Jeśli wcześniej wybrałeś **Roześlij ochronę**, musisz wybrać, co zrobić, gdy system operacyjny urządzenia docelowego musi zostać uruchomiony ponownie. Jeśli nie wybrałeś opcji **Roześlij ochronę**, ten krok zostanie pominięty.

Wybierz, czy instancje powinny być uruchamiane ponownie, jeśli system operacyjny urządzenia musi być uruchomiony ponownie podczas instalacji aplikacji:

- **Nie uruchamiaj urządzenia ponownie**

  Jeśli ta opcja jest zaznaczona, urządzenie nie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

- **Uruchom urządzenie ponownie**

  Jeśli ta opcja jest zaznaczona, urządzenie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

Jeśli chcesz wymusić zamknięcie wszystkich aplikacji w zablokowanych sesjach na instancjach przed ponownym uruchomieniem, zaznacz pole **Wymuś zamknięcie aplikacji dla zablokowanych sesji**. Jeśli to pole jest odznaczone, będziesz musiał ręcznie zamknąć wszystkie aplikacje działające na zablokowanych instancjach.

Krok 9. Pobieranie uaktualnień przez Serwer administracyjny

W tym kroku możesz zobaczyć postęp pobierania uaktualnień niezbędnych do prawidłowego działania Serwera administracyjnego. Możesz kliknąć przycisk **Dalej** bez czekania na zakończenie pobierania, aby przejść do ostatniego okna kreatora.

kreator zakończy swoje działanie.

Sprawdzanie konfiguracji

W celu sprawdzenia, czy Kaspersky Security Center 15.1 został poprawnie skonfigurowany do pracy w środowisku chmury:

1. Uruchom Kaspersky Security Center i upewnij się, że możesz nawiązać połączenie z Serwerem administracyjnym poprzez Konsolę administracyjną.

2. Z drzewa konsoli wybierz folder **Zarządzane urządzenia****Chmura**.

3. Podczas przeglądania dowolnej podgrupy w grupie **Zarządzane urządzenia****Chmura** upewnij się, że zakładka **Urządzenia** wyświetla wszystkie urządzenia tej podgrupy.

   Jeśli urządzenia nie są wyświetlane, możesz ręcznie przeszukać odpowiednie segmenty chmury, aby je odnaleźć.

4. Upewnij się, że na zakładce **Zasady** są aktywne zasady dla następujących aplikacji:

   - Agent sieciowy Kaspersky Security Center
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   Jeśli ich nie ma, możesz je utworzyć ręcznie.

5. Upewnij się, że zakładka **Zadania** wyświetla następujące zadania:

- **Tworzenie kopii zapasowych danych Serwera administracyjnego**
- **Zadanie aktualizacji dla Windows Server**
- **Konserwacja Serwera administracyjnego**
- **Pobierz aktualizacje do repozytorium Serwera administracyjnego**
- **Wyszukaj luki i wymagane aktualizacje**
- **Zainstaluj ochronę dla systemu Windows**
- **Zainstaluj ochronę dla systemu Linux**
- **Zadanie Szybkie skanowanie dla Windows Server**
- **Szybkie skanowanie**
- **Zainstaluj aktualizacje dla systemu Linux**

Jeśli ich nie ma, możesz je utworzyć ręcznie.

Program Kaspersky Security Center 15.1 został poprawnie skonfigurowany do pracy w środowisku chmury.

Grupa urządzeń w chmurze

Możesz zarządzać urządzeniami w chmurze, łącząc je w grupy. Na etapie wstępnej konfiguracji Kaspersky Security Center, grupa administracyjna **Zarządzane urządzenia\Chmura** jest tworzona domyślnie, a urządzenia w chmurze, wykryte podczas przeszukiwania, zostają umieszczone w tej grupie.

Jeśli po skonfigurowaniu synchronizacji wybrałeś opcję **Synchronizuj strukturę grupy administracyjnej z segmentem chmury**, struktura podgrup w tej grupie administracyjnej jest identyczna jak struktura segmentów chmury (jednakże w AWS strefy dostępności i grupy położenia nie są przedstawione w strukturze; w Microsoft Azure podsieci nie są przedstawione w strukturze). Puste podgrupy w obrębie grupy, które są wykrywane podczas przeszukiwania, są automatycznie usuwane.

Możesz także ręcznie utworzyć grupy administracyjne, łącząc wszystkie lub określone urządzenia.

Domyślnie, grupa **Zarządzane urządzenia\Chmura** dziedziczy zasady i zadania od grupy **Zarządzane urządzenia**. Możesz zmienić ustawienia, jeśli pola **Edytowanie dozwolone** zostały zaznaczone we właściwościach ustawień odpowiednich zasad i zadań.

Przeszukiwanie segmentu sieci

Informacje o strukturze sieci i urządzeniach w tej sieci są otrzymywane przez Serwer administracyjny poprzez regularne przeszukiwanie segmentów chmury przy pomocy narzędzi AWS API, Azure API lub Google API. Kaspersky Security Center używa tych informacji do aktualizacji zawartości folderów: **Urządzenia nieprzypisane** i **Zarządzane urządzenia**. Jeżeli skonfigurowałeś automatyczne przenoszenie urządzeń do grup administracyjnych, wykryte urządzenia zostaną włączone do grup administracyjnych.

Aby zezwolić Serwerowi administracyjnemu na przeszukiwanie segmentów chmury, musisz posiadać uprawnienia dla roli IAM lub dla konta użytkownika IAM (w AWS) lub przy pomocy hasła i ID aplikacji (w Azure) lub przy pomocy poczty klienta Google, identyfikatora projektu Google i klucza prywatnego.

Możesz dodawać i usuwać połączenia, a także ustawić terminarz przeszukiwania dla każdego segmentu chmury.

Dodawanie połączeń dla przeszukiwania segmentu chmury

W celu dodania połączenia dla przeszukiwania segmentu chmury do listy dostępnych połączeń:

1. W drzewie konsoli wybierz węzeł **Wykrywanie urządzeń** → **Chmura**.
2. W obszarze roboczym okna kliknij **Konfiguruj przeszukiwanie**.

   Zostanie otwarte okno właściwości zawierające listę połączeń dostępnych dla przeszukiwania segmentu chmury.
3. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Połączenie**.
4. Określ nazwę środowiska chmury dla połączenia, która będzie używana do dalszego przeszukiwania segmentu chmury:

   Środowisko chmury

   Środowiskiem, w którym znajdują się instancje EC2 / maszyny wirtualne, mogą być Amazon Web Services (AWS), Microsoft Azure lub Google Cloud.

   Jeśli wybrałeś AWS, określ następujące ustawienia:

   - **Nazwa połączenia**

     Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

     Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

     Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment”, „AWS Segment” lub „Google Segment”.

   - **Użyj roli AWS IAM**

     Wybierz tę opcję, jeśli już utworzyłeś rolę IAM dla Serwera administracyjnego do korzystania z usług AWS.

   - **Użyj konta użytkownika AWS IAM**

     Wybierz tę opcję, jeśli posiadasz konto użytkownika IAM z wymaganymi uprawnieniami oraz możesz wprowadzić ID klucza oraz tajny klucz.

     - **Identyfikator klucza dostępu**

       Identyfikator klucza dostępu IAM to sekwencja znaków alfanumerycznych. Identyfikator klucza otrzymałeś podczas tworzenia konta użytkownika IAM.

       Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

     - **Tajny klucz**

       Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

Kreator konfiguracji środowiska chmury umożliwia określenie tylko jednego klucza dostępu AWS IAM. Możesz określić więcej połączeń do zarządzania innymi segmentami chmury.

Jeśli wybrałeś Azure, określ następujące ustawienia:

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment", „AWS Segment" lub „Google Segment".

- **ID aplikacji Azure**

  Ten ID aplikacji utworzyłeś na portalu Azure.

  Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **ID subskrypcji Azure**

  Subskrypcję utworzyłeś na portalu Azure.

- **Hasło do aplikacji Azure**

  Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

  Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

- **Nazwa konta magazynu Azure**

  Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

- **Klucz dostępu do magazynu Azure**

  Hasło (klucz) uzyskałeś po utworzeniu konta magazynu Azure do pracy z Kaspersky Security Center.

  Klucz jest dostępny w sekcji „Overview of the Azure storage account", w podsekcji „Keys".

Jeśli wybrałeś Google Cloud, określ następujące ustawienia:

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment", „AWS Segment" lub „Google Segment".

- **E-mail klienta**

  Wprowadź adres e-mail klienta, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Identyfikator projektu**

  Identyfikator projektu to identyfikator, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Klucz prywatny**

  Klucz prywatny to sekwencja znaków, które otrzymałeś jako klucz prywatny po zarejestrowaniu projektu w Google Cloud. Możesz skopiować i wkleić tę sekwencję, aby uniknąć błędów.

5. Jeśli chcesz, wybierz **Ustaw terminarz przeszukiwania** i zmień ustawienia domyślne.

To połączenie zostanie zapisane w ustawieniach aplikacji.

Po pierwszym przeszukaniu nowego segmentu chmury, w grupie administracyjnej **Zarządzane urządzenia\Chmura** pojawi się podgrupa odpowiadająca temu segmentowi.

Jeśli określisz niepoprawne dane uwierzytelniające, podczas przeszukiwania segmentu chmury nie zostaną wykryte żadne instancje, a nowa podgrupa nie pojawi się w grupie administracyjnej **Zarządzane urządzenia\Chmura**.

Usuwanie połączeń dla przeszukiwania segmentu chmury

Jeśli już nie chcesz przeszukiwać określonego segmentu chmury, możesz usunąć połączenie odpowiadające temu segmentowi z listy dostępnych połączeń. Połączenie można usunąć także wtedy, gdy, na przykład, uprawnienia do przeszukiwania segmentu chmury zostały przeniesione na innego użytkownika AWS IAM z innym kluczem.

W celu usunięcia połączenia:

1. W drzewie konsoli wybierz węzeł **Wykrywanie urządzeń → Chmura**.
2. W obszarze roboczym okna wybierz **Konfiguruj przeszukiwanie**.

   Zostanie otwarte okno zawierające listę połączeń dostępnych dla przeszukiwania segmentu chmury.
3. Wybierz połączenie, które chcesz usunąć, i kliknij przycisk **Usuń** dostępny w prawej części okna.
4. W otwartym oknie kliknij przycisk **OK**, aby potwierdzić swój wybór.

Jeśli usuwasz połączenia z listy dostępnych połączeń, urządzenia, które znajdują się w obrębie odpowiednich segmentów, są automatycznie usuwane z odpowiednich grup administracyjnych.

Konfigurowanie terminarza przeszukiwania

Przeszukiwanie segmentu chmury odbywa się zgodnie z terminarzem. Możesz ustawić częstotliwość przeszukiwania.

Częstotliwość przeszukiwania jest automatycznie ustawiana na 5 minut w ustawieniach konfiguracji środowiska chmury. Możesz zmienić tę wartość w dowolnym momencie i ustawić inny terminarz. Nie jest zalecane konfigurowanie wykonywania przeszukiwania z częstotliwością większą niż co 5 minut, ponieważ może to prowadzić do błędów w działaniu AWS API.

W celu skonfigurowania terminarza przeszukiwania segmentu chmury:

1. W drzewie konsoli wybierz węzeł **Wykrywanie urządzeń** → **Chmura**.
2. W obszarze roboczym kliknij **Konfiguruj przeszukiwanie**.

   Zostanie otwarte okno właściwości chmury.
3. Na liście wybierz żądane połączenie i kliknij przycisk **Właściwości**.

   Zostanie otwarte okno właściwości połączenia.
4. W oknie właściwości kliknij odnośnik **Ustaw terminarz przeszukiwania**.

   Zostanie otwarte okno **Terminarz**.
5. Określ następujące ustawienia:

   - **Zaplanowane uruchomienie**

     Dostępne są następujące opcje terminarza przeszukiwania:

     - **Co N dni**

       Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

       Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

     - **Co N minut**

       Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

       Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

     - **Według dni tygodnia**

       Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

       Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

     - **Co miesiąc, w określone dni wybranych tygodni**

       Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

       Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

   - **Uruchom pominięte zadania**

     Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

     Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

     Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

     Domyślnie opcja ta jest włączona.
6. Kliknij **OK**, aby zachować zmiany.

Terminarz przeszukiwania zostaje skonfigurowany i zapisany.

Instalowanie aplikacji na urządzeniach w środowisku chmury

Na urządzeniach w środowisku chmury możesz zainstalować następujące aplikacje firmy Kaspersky: Kaspersky Security for Windows Server (dla urządzeń Windows) i Kaspersky Endpoint Security for Linux (dla urządzeń Linux).

Urządzenia klienckie, na których chcesz wdrożyć ochronę, muszą spełniać wymagania do działania Kaspersky Security Center w środowisku chmury. Aby zainstalować aplikacje na instancjach AWS, na instancjach maszyn wirtualnych Microsoft Azure lub maszyn wirtualnych Google, musisz posiadać ważną licencję.

Kaspersky Security Center 15.1 obsługuje następujące scenariusze:

- Urządzenie klienckie jest wykrywane przy użyciu API; instalacja odbywa się również przy użyciu API. Ten scenariusz jest obsługiwany dla środowisk w chmurze AWS i Azure.
- Urządzenie klienckie zostaje wykryte przy użyciu przeszukiwania Active Directory, przeszukiwania domen Windows lub przeszukiwania zakresu IP; instalacja odbywa się przy użyciu Kaspersky Security Center.
- Urządzenie klienckie jest wykrywane przy użyciu Google API; instalacja odbywa się przy użyciu Kaspersky Security Center. W przypadku Google Cloud tylko ten scenariusz jest obsługiwany.

Inne sposoby instalacji aplikacji nie są obsługiwane.

Aby zainstalować aplikacje na urządzeniach wirtualnych, użyj pakietów instalacyjnych.

W celu utworzenia zadania zdalnej instalacji aplikacji na instancjach przy użyciu AWS API lub Azure API:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Kliknij przycisk **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.
3. W oknie **Wybierz typ zadania** jako typ zadania wybierz **Zdalna instalacja aplikacji**.
4. W oknie **Wybierz urządzenia**, z grupy **Zarządzane urządzenia\Chmura** wybierz odpowiednie urządzenia.
5. Jeśli Agent sieciowy nie został jeszcze zainstalowany na urządzeniach, na których zamierzasz zainstalować aplikację, w kroku **Wybieranie konta do uruchomienia zadania** wybierz **Konto wymagane (Agent sieciowy nie jest używany)** i kliknij przycisk **Dodaj** dostępny w prawej części okna. Z menu, które zostanie wyświetlone, wybierz jedną z następujących opcji:

   - **Konto w chmurze**

     Wybierz tę opcję, jeśli chcesz zainstalować aplikacje na instancjach w AWS i posiadasz klucz dostępu IAM AWS z wymaganymi uprawnieniami, ale nie posiadasz roli IAM. Dodatkowo, wybierz tę opcję, jeśli chcesz zainstalować aplikacje na urządzeniach w środowisku Azure.

     W otwartym oknie zapewnij Kaspersky Security Center poświadczenia, które nadają uprawnienia do instalowania aplikacji na odpowiednich urządzeniach.

     Wybierz środowisko chmury: AWS lub Azure.

     W polu **Nazwa konta** wprowadź nazwę dla tych poświadczeń. Ta nazwa pojawi się na liście kont do uruchomienia zadania.

     Jeśli wybrałeś AWS, w polach **Identyfikator klucza dostępu** i **Klucz tajny** wprowadź poświadczenia dla konta użytkownika IAM, który posiada uprawnienia do zainstalowania aplikacji na określonych urządzeniach.

Jeśli wybrałeś Azure, w polach **ID subskrypcji Azure** i **Hasło do aplikacji Azure** wprowadź poświadczenia dla konta Azure, który posiada uprawnienia do zainstalowania aplikacji na określonych urządzeniach.

Jeśli określisz niepoprawne poświadczenia, zadanie zdalnej instalacji zakończy się błędem na urządzeniach, dla których zostało to zaplanowane.

- **Konto**

  W przypadku instancji działających pod kontrolą systemu Windows, wybierz tę opcję, jeśli nie chcesz zainstalować aplikacji przy użyciu narzędzi AWS lub Azure API. W tym przypadku upewnij się, że urządzenia w Twoim segmencie chmury spełniają potrzebne warunki. Kaspersky Security Center sam instaluje aplikacje, bez użycia AWS API lub Azure API.

  Jeśli określisz niepoprawne dane, zadanie zdalnej instalacji zakończy się błędem na urządzeniach, dla których zostało to zaplanowane.

- **Rola IAM**

  Wybierz tę opcję, jeśli chcesz zainstalować aplikacje na instancjach w środowisku AWS i posiadasz rolę IAM z wymaganymi uprawnieniami.

  Jeśli wybierzesz tę opcję, ale nie posiadasz roli IAM z wymaganymi uprawnieniami, zadanie zdalnej instalacji zakończy się błędem na urządzeniach, dla których zostało to zaplanowane.

- **Certyfikat SSH**

  W przypadku instancji działających pod kontrolą systemu Linux, wybierz tę opcję, jeśli nie chcesz zainstalować aplikacji przy użyciu narzędzi AWS API lub Azure API. W tym przypadku upewnij się, że urządzenia w Twoim segmencie chmury spełniają potrzebne warunki. Kaspersky Security Center sam instaluje aplikacje, bez użycia AWS API lub Azure API.

  Aby określić klucz prywatny certyfikatu SSH, możesz go wygenerować za pomocą narzędzia ssh-keygen. Należy zauważyć, że Kaspersky Security Center obsługuje format PEM kluczy prywatnych, ale narzędzie ssh-keygen domyślnie generuje klucze SSH w formacie OPENSSH. Format OPENSSH nie jest obsługiwany przez Kaspersky Security Center. Aby utworzyć klucz prywatny w obsługiwanym formacie PEM, dodaj opcję `-m PEM` w poleceniu ssh-keygen. Na przykład:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<adres e-mail użytkownika>"
  ```

Możesz udostępnić kilka poświadczeń, klikając przycisk **Dodaj** za każdym razem, gdy chcesz dodać poświadczenia. Jeśli różne segmenty chmury wymagają różnych poświadczeń, zapewnij poświadczenia dla wszystkich segmentów.

Po zakończeniu pracy kreatora, zadanie zdalnej instalacji aplikacji pojawi się na liście zadań w obszarze roboczym folderu **Zadania**.

W Microsoft Azure zdalna instalacja aplikacji zabezpieczających na maszynie wirtualnej może spowodować usunięcie niestandardowego rozszerzenia skryptu, zainstalowanego na maszynie wirtualnej.

Przeglądanie właściwości urządzeń w chmurze

W celu przejrzenia właściwości urządzenia w chmurze:

1. W drzewie konsoli, w węźle **Wykrywanie urządzeń** → **Chmura** wybierz podwęzeł odpowiadający grupie, w której znajduje się odpowiednia instancja.

Jeśli nie wiesz, w jakiej grupie znajduje się odpowiednie urządzenie wirtualne, skorzystaj z funkcji wyszukiwania:

a. Kliknij prawym klawiszem myszy nazwę węzła **Zarządzane urządzenia** → **Cloud**, a następnie, z menu kontekstowego wybierz **Szukaj**.

b. W otwartym oknie przeprowadź wyszukiwanie.

Jeśli istnieje urządzenie, które odpowiada ustawionym kryteriom, jego nazwa i szczegóły zostaną wyświetlone w dolnej części okna.

2. Kliknij nazwę odpowiedniego węzła prawym klawiszem myszy. Z menu kontekstowego wybierz **Właściwości**.

W otwartym oknie zostaną wyświetlone właściwości obiektu.

Sekcja **Informacje o systemie** → **Ogólne informacje o systemie** zawiera właściwości, które są specyficzne dla urządzeń w środowisku chmury:

- **Urządzenie wykryte za pomocą interfejsu API** (**AWS**, **Azure** lub **Google Cloud**; jeśli urządzenia nie można wykryć za pomocą narzędzi API, wyświetlana jest wartość **No** - Nie).
- **Region chmury**.
- **Cloud VPC** (tylko dla urządzeń AWS i Google Cloud).
- **Strefa dostępności w chmurze** (tylko dla urządzeń AWS i Google Cloud).
- **Podsieć chmury**.
- **Grupa położenia w chmurze** (ta jednostka jest wyświetlana tylko wtedy, gdy instancja należy do grupy położenia; w innym przypadku nie jest wyświetlana).

Możesz kliknąć przycisk **Eksportuj do pliku**, aby wyeksportować te informacje do pliku .csv lub .txt.

Synchronizacja z chmurą

Podczas operacji Konfiguruj środowisko chmurowe automatycznie tworzona jest reguła Synchronizuj z chmurą. Ta reguła umożliwia automatyczne przenoszenie instancji, wykrytych przy każdym przeszukiwaniu, z grupy **Urządzenia nieprzypisane** do grupy **Zarządzane urządzenia****Chmura**, aby te instancje stały się dostępne dla scentralizowanego zarządzania. Domyślnie, reguła jest aktywna po utworzeniu. Regułę można wyłączyć, zmodyfikować lub wymusić w dowolnym momencie.

W celu zmodyfikowania właściwości reguły Synchronizuj z chmurą i/lub wymuszenia reguły:

1. W drzewie konsoli kliknij prawym klawiszem myszy nazwę węzła **Wykrywanie urządzeń**.
2. Z menu kontekstowego wybierz **Właściwości**.
3. W otwartym oknie **właściwości**, w panelu **Sekcje** wybierz **Przenieś urządzenia**.
4. Na liście reguł przenoszenia urządzeń w obszarze roboczym wybierz **Synchronizuj z chmurą**, a następnie kliknij przycisk **Właściwości**, znajdujący się w dolnej części okna.

Zostanie otwarte okno właściwości reguły.

5. W razie potrzeby określ następujące ustawienia w grupie ustawień **Segmenty chmury**:

- **Urządzenie znajduje się w segmencie chmury**

  Reguła jest tylko stosowana do urządzeń, które znajdują się w wybranym segmencie chmury. W innej sytuacji reguła będzie stosowana do wszystkich urządzeń, które zostały wykryte.

  Domyślnie opcja ta jest zaznaczona.

  - **Włączając obiekty potomne**

    Reguła będzie stosowana do wszystkich urządzeń w wybranym segmencie i we wszystkich zagnieżdżonych podsekcjach chmury. W innym przypadku reguła jest tylko stosowana do urządzeń, które znajdują się w głównym segmencie.

    Domyślnie opcja ta jest zaznaczona.

  - **Przenieś urządzenia z obiektów zagnieżdżonych do odpowiednich podgrup**

    Jeśli ta opcja jest włączona, urządzenia z obiektów zagnieżdżonych zostaną automatycznie przeniesione do podgrup, które odpowiadają ich strukturze.

    Jeśli ta opcja jest wyłączona, urządzenia z obiektów zagnieżdżonych zostaną automatycznie przeniesione do głównej podgrupy Chmura bez dalszego rozdzielania.

    Domyślnie opcja ta jest włączona.

    - **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń**

      Jeśli ta opcja jest włączona, gdy struktura grupy **Zarządzane urządzenia\Chmura** nie posiada podgrup, które będą odpowiadały sekcji zawierającej urządzenie, Kaspersky Security Center utworzy takie podgrupy. Na przykład, jeśli nowa podsieć zostanie wykryta podczas wyszukiwania urządzeń, nowa grupa z taką samą nazwą zostanie utworzona w grupie **Zarządzane urządzenia\Chmura**.

      Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie tworzy żadnych nowych podgrup. Na przykład, jeśli nowa podsieć zostanie wykryta podczas przeszukiwania sieci, nowa grupa o tej samej nazwie nie zostanie utworzona w grupie **Zarządzane urządzenia\Chmura**, a urządzenia, które są w tej podsieci, zostaną przeniesione do grupy **Zarządzane urządzenia\Chmura**.

      Domyślnie opcja ta jest włączona.

    - **Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury**

      Jeśli ta opcja jest włączona, aplikacja usunie z grupy Chmura wszystkie podgrupy, które nie odpowiadają żadnym istniejącym obiektom chmury.

      Jeśli ta opcja jest wyłączona, podgrupy, które nie odpowiadają żadnym istniejącym obiektom chmury, zostaną zachowane.

      Domyślnie opcja ta jest włączona.

  Jeśli podczas działania środowiska **Konfiguruj chmurę** włączono opcję **Synchronizuj z chmurą**, reguła **Synchronizuj z chmurą zostanie utworzona z wybranymi opcjami** Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń i Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury.

  Jeśli nie włączyłeś opcji **Synchronizuj z chmurą**, reguła Synchronizuj z chmurą zostanie utworzona z wyłączonymi (odznaczonymi) tymi opcjami. Jeśli Twoja praca z Kaspersky Security Center wymaga, aby struktura podgrup w podgrupie **Zarządzane urządzenia\Chmura** odpowiadała strukturze segmentów chmury, włącz opcje **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń** i **Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury** we właściwościach reguły, a następnie wymuś regułę.

6. Z listy rozwijalnej **Urządzenie odnalezione przy użyciu API** wybierz jedną z następujących wartości:
    - **AWS**. Urządzenie jest wykrywane przy pomocy AWS API, co oznacza, że urządzenie znajduje się w środowisku chmury AWS.
    - **Azure**. Urządzenie jest wykrywane przy pomocy Azure API, co oznacza, że urządzenie znajduje się w środowisku chmury Azure.
    - **Google Cloud.** Urządzenie jest wykrywane przy pomocy Google API, co oznacza, że urządzenie znajduje się w środowisku Google Cloud.
    - **Nie**. Urządzenie nie może zostać wykryte przy użyciu AWS, Azure lub Google API, co oznacza, że znajduje się poza środowiskiem chmury lub znajduje się w środowisku chmury, ale nie może zostać wykryte przy użyciu API.
7. **Brak wartości**. Warunek nie ma zastosowania. Jeśli to konieczne, skonfiguruj inne właściwości reguły w innych sekcjach.
8. Jeśli to konieczne, wymuś regułę, klikając przycisk **Wymuś** znajdujący się w dolnej części okna.

    Zostanie uruchomiony Kreator wykonywania reguły. Postępuj zgodnie z instrukcjami kreatora. Jeśli kreator zakończy swoje działanie, reguła zostanie uruchomiona, a struktura podgrup w podgrupie **Zarządzane urządzenia\Chmura** będzie odpowiadała strukturze segmentów chmury.
9. Kliknij przycisk **OK**.

Właściwości zostały skonfigurowane i zapisane.

W celu wyłączenia reguły Synchronizuj z chmura:

1. W drzewie konsoli kliknij prawym klawiszem myszy nazwę węzła **Wykrywanie urządzeń**.
2. Z menu kontekstowego wybierz **Właściwości**.
3. W otwartym oknie **właściwości**, w panelu **Sekcje** wybierz **Przenieś urządzenia**.
4. Na liście reguł przenoszenia urządzeń w obszarze roboczym wyłącz (odznacz) opcję **Synchronizuj z chmurą** i kliknij **OK**.

Reguła zostanie wyłączona i nie będzie już stosowana.

Wdrożenie Kaspersky Security Center w Yandex.Cloud

Możesz wdrożyć Kaspersky Security Center w Yandex.Cloud. Dostępny jest tylko tryb płatności za użycie; bazy danych w chmurze nie są obsługiwane.

W Yandex.Cloud dostępne są następujące metody wdrażania aplikacji zabezpieczających:

- Przy użyciu podstawowej metody programu Kaspersky Security Center, to znaczy poprzez zadanie *Zdalna instalacja* (wdrażanie programów zabezpieczających jest możliwe tylko wtedy, gdy Serwer administracyjny i maszyny wirtualne, które mają być chronione, znajdują się w tym samym segmencie sieci)
- Za pomocą skryptów instalacji

Aby zainstalować Kaspersky Security Center w Yandex.Cloud, musisz mieć konto usługi w Yandex.Cloud. Musisz nadać temu kontu uprawnienie marketplace.meteringAgent i powiązać to konto z maszyną wirtualną (szczegółowe informacje można znaleźć na stronie https://cloud.yandex.com/en).

Dodatki

Ta sekcja zawiera dodatkowe informacje i fakty związane z korzystaniem z Kaspersky Security Center.

Zaawansowane funkcje

Ta sekcja opisuje zakres dodatkowych opcji Kaspersky Security Center zaprojektowanych do poszerzenia funkcjonalności scentralizowanego zarządzania aplikacjami na urządzeniach.

Automatyzacja działania Kaspersky Security Center. Narzędzie klakaut

Możesz zautomatyzować działanie Kaspersky Security Center przy użyciu narzędzia klakaut. Narzędzie klakaut i jego system pomocy znajdują się w folderze instalacyjnym Kaspersky Security Center.

Narzędzia niestandardowe

Kaspersky Security Center umożliwia utworzenie listy *narzędzi niestandardowych* (zwanych dalej również *narzędziami*), czyli aplikacji aktywowanych dla urządzenia klienckiego w Konsoli administracyjnej przy użyciu grupy **Narzędzia użytkownika** z menu kontekstowego. Każde narzędzie na liście będzie skojarzone z oddzielnym poleceniem menu, którego Konsola administracyjna używa do uruchomienia aplikacji odpowiadającej temu narzędziu.

Aplikacja jest uruchamiana na stacji roboczej administratora. Aplikacja może akceptować atrybuty zdalnego urządzenia klienckiego jako argumenty wiersza poleceń (nazwa NetBIOS, nazwa DNS lub adres IP). Połączenie ze zdalnym urządzeniem można nawiązać przy użyciu połączenia tunelowego.

Domyślnie, lista narzędzi niestandardowych zawiera następujące usługi dla każdego urządzenia klienckiego:

- **Zdalna diagnostyka** to narzędzie do zdalnej diagnostyki programu Kaspersky Security Center.
- **Zdalny pulpit** to standardowy składnik systemu Microsoft Windows o nazwie Podłączanie pulpitu zdalnego.
- **Zarządzanie komputerem** to standardowy komponent systemu Microsoft Windows.

W celu dodania lub usunięcia narzędzi niestandardowych, bądź też zmodyfikowania ich ustawień:

Z menu kontekstowego urządzenia klienckiego wybierz **Narzędzia użytkownika** → **Konfiguruj narzędzia użytkownika**.

Zostanie otwarte okno **Narzędzia użytkownika**. W tym oknie możesz dodawać niestandardowe narzędzia lub edytować ich ustawienia za pomocą przycisków **Dodaj** i **Modyfikuj**. Aby usunąć narzędzie niestandardowe, kliknij przycisk usuwania z ikoną czerwonego krzyżyka ( ).

Tryb klonowania dysku Agenta sieciowego

Klonowanie dysku twardego odpowiedniego urządzenia jest popularną metodą instalacji oprogramowania na nowych urządzeniach. Jeśli Agent sieciowy jest uruchomiony w trybie standardowym na dysku twardym odpowiedniego urządzenia, mogą pojawić się następujące problemy:

Po zainstalowaniu odpowiedniego obrazu dysku przy pomocy Agenta sieciowego na nowych urządzeniach, będą one wyświetlane jako pojedyncza ikona w Konsoli administracyjnej. Ten problem pojawia się, ponieważ procedura klonowania powoduje, że nowe urządzenia przechowują identyczne dane wewnętrzne, które umożliwiają Serwerowi administracyjnemu skojarzenie urządzenia z ikoną w Konsoli administracyjnej.

Specjalny *tryb klonowania dysku Agenta sieciowego* umożliwia uniknięcie problemów z nieprawidłowym wyświetlaniem nowych urządzeń w Konsoli administracyjnej po klonowaniu. Użyj tego trybu podczas instalowania oprogramowania (z Agentem Sieciowym) na nowych urządzeniach za pomocą klonowania dysku.

W trybie klonowania dysku Agent sieciowy pracuje cały czas, ale nie łączy się z Serwerem administracyjnym. Po wyjściu z trybu klonowania, Agent sieciowy usuwa dane wewnętrzne, które umożliwiają Serwerowi administracyjnemu skojarzenie kilku urządzeń z jedną ikona w Konsoli administracyjnej. Po zakończeniu klonowania obrazu odpowiedniego urządzenia, nowe urządzenia są wyświetlane w Konsoli administracyjnej prawidłowo (z indywidualnymi ikonami).

Scenariusz użycia trybu klonowania dysku Agenta sieciowego

1. Administrator instaluje Agenta sieciowego na odpowiednim urządzeniu.
2. Administrator sprawdza połączenie Agenta sieciowego z Serwerem administracyjnym przy użyciu narzędzia klnagchk.
3. Administrator włącza tryb klonowania dysku Agenta sieciowego.
4. Administrator instaluje oprogramowanie i łaty na urządzeniu i uruchamia je ponownie niezbędną ilość razy.
5. Administrator klonuje dysk twardy odpowiedniego urządzenia na dowolnej liczbie urządzeń.
6. Każda sklonowana kopia musi spełniać następujące warunki:
    a. Nazwa urządzenia musi być zmieniona.
    b. Urządzenie musi zostać uruchomione ponownie.
    c. Tryb klonowania dysku musi być wyłączony.

Włączanie i wyłączanie trybu klonowania dysku przy użyciu narzędzia klmover

W celu włączenia / wyłączenia trybu klonowania dysku Agenta sieciowego:

1. Uruchom narzędzie klmover na urządzeniu z zainstalowanym Agentem sieciowym, które potrzebujesz sklonować.

   Narzędzie klmover znajduje się w folderze instalacyjnym Agenta sieciowego.

2. W celu włączenia trybu klonowania dysku, w wierszu poleceń systemu Windows wprowadź następujące polecenie:

   ```
   klmover -cloningmode 1
   ```

   Agent sieciowy przełączy się do trybu klonowania dysku.

3. W celu uzyskania bieżącego stanu trybu klonowania dysku, w wierszu poleceń wprowadź następujące polecenie:

   ```
   klmover -cloningmode
   ```

   Okno narzędzia wskaże, czy tryb klonowania dysku jest włączony czy wyłączony.

4. W celu wyłączenia trybu klonowania dysku, w wierszu poleceń narzędzia wprowadź następujące polecenie:

   ```
   klmover -cloningmode 0
   ```

Przygotowywanie urządzenia referencyjnego z zainstalowanym Agentem sieciowym do utworzenia obrazu systemu operacyjnego

Możesz chcieć utworzyć obraz systemu operacyjnego urządzenia referencyjnego z zainstalowanym Agentem sieciowym, a następnie wdrożyć obraz na urządzeniach w sieci. W tym przypadku możesz utworzyć obraz systemu operacyjnego urządzenia referencyjnego, na którym Agent sieciowy nie został jeszcze uruchomiony. Jeśli uruchomisz Agenta sieciowego na urządzeniu referencyjnym przed utworzeniem obrazu systemu operacyjnego, identyfikacja urządzeń wdrożonych z obrazu systemu operacyjnego urządzenia referencyjnego przez Serwer administracyjny będzie problematyczna.

W celu przygotowania urządzenia referencyjnego do utworzenia obrazu systemu operacyjnego:

1. Upewnij się, że system operacyjny Windows jest zainstalowany na urządzeniu referencyjnym i zainstaluj inne oprogramowanie, którego potrzebujesz na tym urządzeniu.

2. Na urządzeniu referencyjnym, w ustawieniach Połączenia sieciowe systemu Windows odłącz urządzenie referencyjne od sieci, w której zainstalowany jest program Kaspersky Security Center.

3. Na urządzeniu referencyjnym uruchom lokalną instalację Agenta sieciowego przy pomocy pliku setup.exe.

   Zostanie uruchomiony kreator instalacji Agenta sieciowego Kaspersky Security Center. Postępuj zgodnie z instrukcjami kreatora.

4. Na stronie **Serwer administracyjny** kreatora określ adres IP Serwera administracyjnego.

   Jeśli nie znasz dokładnego adresu Serwera administracyjnego, wprowadź localhost. Możesz zmienić adres IP w późniejszym czasie, korzystając z narzędzia klmover z kluczem `-address`.

5. W kroku **Uruchom aplikację** wyłącz opcję **Uruchom aplikację podczas instalacji**.

6. Po zakończeniu instalacji Agenta sieciowego, nie uruchamiaj urządzenia przed utworzeniem obrazu systemu operacyjnego.

   Jeśli uruchomisz urządzenie ponownie, będziesz musiał powtórzyć cały proces przygotowania urządzenia referencyjnego przed utworzeniem obrazu systemu operacyjnego.

7. Na urządzeniu referencyjnym, w wierszu polecenia uruchom narzędzie sysprep i wykonaj następujące polecenie: `sysprep.exe /generalize /oobe /shutdown`.

Urządzenie referencyjne jest gotowe do utworzenia obrazu systemu operacyjnego.

Konfigurowanie odbierania wiadomości od komponentu Monitor integralności pliku

Zarządzane aplikacje, takie jak Kaspersky Security for Windows Server lub Kaspersky Security for Virtualization Light Agent wysyłają wiadomości z Monitora integralności plików do Kaspersky Security Center. Kaspersky Security Center umożliwia także monitorowanie wszelkich zmian wprowadzonych w ogromnie ważnych komponentach systemów (np. Serwery sieciowe i ATM) i natychmiastowe reagowanie na naruszenie integralności tych systemów. Dlatego też możesz otrzymywać wiadomości z komponentu Monitor integralności plików. Komponent Monitor integralności plików umożliwia monitorowanie nie tylko systemu plików urządzenia, ale także gałęzi rejestru, stanu zapory sieciowej i stanu podłączonego sprzętu.

Należy skonfigurować Kaspersky Security Center do odbierania wiadomości od komponentu Monitor integralności plików bez używania Kaspersky Security for Windows Server lub Kaspersky Security for Virtualization Light Agent.

W celu skonfigurowania odbierania wiadomości od komponentu Monitor integralności plików:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).

2. Przejdź do gałęzi:

   - W systemach 32-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - W systemach 64-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Utwórz klucze:

   - Utwórz klucz KLSRV_EVP_FIM_PERIOD_SEC, aby określić przedział czasu dla zliczania liczby przetwarzanych zdarzeń. Określ następujące ustawienia:

     a. Jako nazwę klucza określ KLSRV_EVP_FIM_PERIOD_SEC.

     b. Jako typ klucza określ DWORD.

     c. Określ zakres wartości dla przedziału czasu od 43 200 do 172 800 sekund. Domyślnie przedział czasu wynosi 86 400 sekundy.

- Utwórz klucz KLSRV_EVP_FIM_LIMIT, aby ograniczyć liczbę otrzymanych zdarzeń dla określonego przedziału czasu. Określ następujące ustawienia:

  a. Jako nazwę klucza określ KLSRV_EVP_FIM_LIMIT.

  b. Jako typ klucza określ DWORD.

  c. Określ zakres wartości dla otrzymanych zdarzeń od 2 000 do 50 000. Domyślna liczba zdarzeń to 20 000.

- Utwórz klucz KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC, aby zliczać zdarzenia z dokładnością do określonego przedziału czasu. Określ następujące ustawienia:

  a. Jako nazwę klucza określ KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC.

  b. Jako typ klucza określ DWORD.

  c. Określ zakres wartości od 120 do 600 sekund. Domyślny przedział czasu wynosi 300 sekund.

- Utwórz klucz KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC, aby, po minięciu określonego przedziału czasu, aplikacja mogła sprawdzić, czy liczba zdarzeń przetworzonych w określonym przedziale czasu jest mniejsza niż wskazany limit. To sprawdzanie odbywa się po osiągnięciu limitu liczby otrzymanych zdarzeń. Jeśli ten warunek jest spełniony, aplikacja wznowi zapisywanie zdarzeń w bazie danych. Określ następujące ustawienia:

  a. Jako nazwę klucza określ KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC.

  b. Jako typ klucza określ DWORD.

  c. Określ zakres wartości od 600 do 3 600 sekund. Domyślny przedział czasu wynosi 1 800 sekund.

Jeśli klucze nie zostaną utworzone, używane będą wartości domyślne.

4. Uruchom ponownie usługę Serwera administracyjnego.

Ograniczenia dotyczące liczby otrzymywanych zdarzeń od komponentu Monitor integralności plików zostaną skonfigurowane. Wyniki działania komponentu Monitor integralności plików można przejrzeć w raportach: **10 najważniejszych reguł Monitora integralności plików / Monitorowania integralności systemu, które były najczęściej wywoływane na urządzeniach** and **10 urządzeń z najczęściej wywołanymi regułami Monitora integralności plików / Monitorowania integralności systemu**.

Konserwacja Serwera administracyjnego

Konserwacja Serwera administracyjnego umożliwia zwolnienie miejsca w folderze Serwera administracyjnego i zmniejszenie objętości bazy danych poprzez usunięcie obiektów, które nie są już potrzebne. Pomaga to poprawić wydajność i niezawodność działania aplikacji. Zalecamy przeprowadzanie konserwacji Serwera administracyjnego przynajmniej raz w tygodniu.

Konserwacja Serwera administracyjnego jest wykonywana przy pomocy dedykowanego zadania. Podczas konserwacji Serwera administracyjnego aplikacja wykonuje następujące działania:

- Usuwa niepotrzebne foldery i pliki z folderu przechowywania.
- Usuwa niepotrzebne rekordy z tabel (znane również jako „dangling pointers" (zwisające wskaźniki)).
- Czyści pamięć podręczną.

- Przeprowadza konserwację bazy danych (jeśli używasz SQL Server lub PostgreSQL jako DBMS):
  - Sprawdza bazę danych pod kątem błędów (funkcja dostępna tylko w przypadku SQL Server).
  - Reorganizuje indeksy w bazie danych.
  - Aktualizuje statystyki bazy danych.
  - Zmniejsza bazę danych (jeśli to konieczne).

W celu utworzenia zadania Konserwacja Serwera administracyjnego:

1. W drzewie konsoli należy wybrać węzeł Serwera administracyjnego, dla którego chcesz utworzyć zadanie *Konserwacja Serwera administracyjnego*.
2. Wybierz folder **Zadania**.
3. W obszarze roboczym folderu **Zadania** kliknij przycisk **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
4. W oknie **Wybierz typ zadania** kreatora jako typ zadania wybierz **Konserwacja Serwera administracyjnego** i kliknij **Dalej**.
5. Jeśli podczas konserwacji musisz zmniejszyć bazę danych Serwera administracyjnego, w oknie **Ustawienia** zaznacz pole **Zmniejsz bazę danych**.
6. Wykonaj pozostałe instrukcje kreatora.

Nowo utworzone zadanie będzie wyświetlane na liście zadań, w obszarze roboczym folderu **Zadania**. Dla jednego Serwera administracyjnego można uruchomić tylko jedno zadanie *Konserwacja Serwera administracyjnego*. Jeśli zadanie *Konserwacja Serwera administracyjnego* zostało już utworzone dla Serwera administracyjnego, nie będzie można utworzyć nowego zadania *Konserwacja Serwera administracyjnego*.

Dostęp do publicznych serwerów DNS

Jeśli dostęp do serwerów Kaspersky przy użyciu systemowego DNS nie jest możliwy, Kaspersky Security Center może korzystać z następujących publicznych serwerów DNS w następującej kolejności:

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

Żądania kierowane do tych serwerów DNS mogą zawierać adresy domen oraz publiczny adres IP Serwera administracyjnego, ponieważ aplikacja nawiązuje połączenie TCP/UDP z serwerem DNS. Jeśli Kaspersky Security Center korzysta z publicznego serwera DNS, przetwarzanie danych podlega polityce prywatności odpowiedniej usługi.

Aby skonfigurować korzystanie z publicznego DNS z użyciem narzędzia klscflag:

1. Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Aby wyłączyć korzystanie z publicznego DNS, uruchom następujące polecenie:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Aby włączyć korzystanie z publicznego DNS, uruchom następujące polecenie:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Okno Metoda powiadamiania użytkownika

W oknie **Metoda powiadamiania użytkownika** możesz skonfigurować powiadamianie użytkownika o instalacji certyfikatu na urządzeniu mobilnym:

- **Pokaż kod QR w kreatorze**. Jeśli wybierzesz tę opcję, łącze do pakietu instalacyjnego zostanie wyświetlone w ostatnim kroku kreatora połączeń urządzenia mobilnego.

- **Wyślij kod QR do użytkownika**. Jeśli wybierzesz tę opcję, możesz określić ustawienia powiadamiania użytkownika o podłączeniu urządzenia.

W tej grupie ustawień **Przez e-mail** możesz skonfigurować powiadamianie użytkownika o instalacji nowego certyfikatu na jego urządzeniu mobilnym za pośrednictwem wiadomości e-mail. Ta metoda powiadamiania jest dostępna tylko wtedy, gdy opcja Serwer SMTP jest włączona.

W grupie ustawień **Przez SMS** możesz skonfigurować powiadamianie użytkownika o instalacji certyfikatu na jego urządzeniu mobilnym za pośrednictwem wiadomości SMS. Ta metoda powiadamiania jest dostępna tylko wtedy, gdy opcja Powiadomienia SMS jest włączona.

Kliknij odnośnik **Edytuj wiadomość** w grupach ustawień **Przez e-mail** i **Przez SMS**, aby wyświetlić i edytować powiadomienie (jeśli to konieczne).

Okno Wybór urządzeń

Wskaż wybór na liście **Wybór urządzeń**. Lista zawiera predefiniowane wybory oraz wybory utworzone przez użytkownika.

Możesz wyświetlić szczegóły wyborów urządzeń w obszarze roboczym sekcji **Wybory urządzeń**.

Okno Określ nazwę nowego obiektu

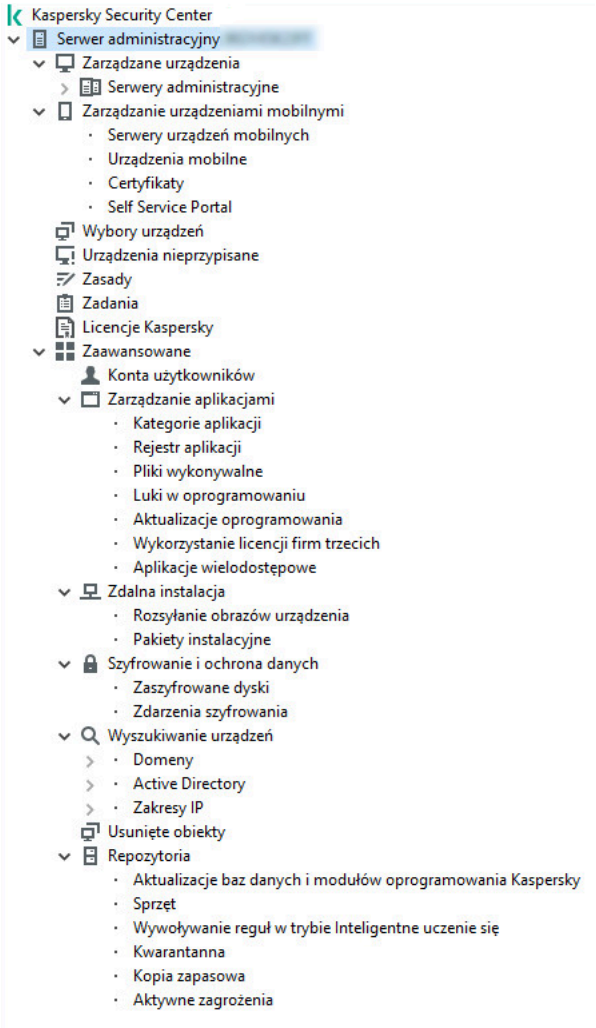
W oknie określ nazwę nowo utworzonego obiektu. Nazwa nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

Funkcje korzystania z interfejsu do zarządzania

Ta sekcja opisuje działania, które można wykonać w oknie głównym Kaspersky Security Center.

Drzewo konsoli

Drzewo konsoli (patrz poniższy rysunek) wyświetla hierarchię Serwerów administracyjnych, które znajdują się w sieci firmowej, strukturę ich grup administracyjnych i inne obiekty aplikacji, takie jak foldery **Repozytoria** lub **Zarządzanie aplikacjami**. Obszar nazw Kaspersky Security Center może zawierać kilka węzłów, włączając nazwy serwerów odpowiadające zainstalowanym Serwerom administracyjnym będącym częścią hierarchii.



Drzewo konsoli

Węzeł Serwer administracyjny

Węzeł **Serwer administracyjny – <Nazwa urządzenia>** jest kontenerem odzwierciedlającym strukturę folderów wybranego Serwera administracyjnego.

Obszar roboczy węzła **Serwer administracyjny** zawiera informacje podsumowujące o bieżącym stanie aplikacji i urządzeń zarządzanych przez Serwer administracyjny. Informacje w obszarze roboczym zostały umieszczone na różnych zakładkach:

- **Monitorowanie**. Wyświetla w czasie rzeczywistym informacje dotyczące działania aplikacji oraz bieżącego stanu urządzeń klienckich. Informacje ważne dla administratora (takie jak wiadomości dotyczące luk, błędów lub wykrytych wirusów) są oznaczone specjalnym kolorem. Możesz użyć odnośników dostępnych na zakładce **Monitorowanie** do wykonywania standardowych zadań administratora (na przykład, do instalowania i konfigurowania aplikacji antywirusowej na urządzeniach klienckich), a także do przejścia do innych folderów drzewa konsoli.

- **Statystyki**. Zawiera zestaw wykresów pogrupowanych według tematów (stan ochrony, statystyki antywirusowe, aktualizacje itd.). Wykresy przedstawiają bieżące informacje dotyczące działania aplikacji i stanu urządzeń klienckich.

- **Raporty**. Zawiera szablony raportów wygenerowanych przez aplikację. Na tej zakładce można utworzyć raporty przy użyciu predefiniowanych szablonów, a także utworzyć swoje własne szablony raportów.

- Okno **Zdarzenia**. Zawiera wpisy dotyczące zdarzeń zarejestrowanych podczas działania aplikacji. Wpisy są podzielone według tematów w celu ułatwienia ich czytania i filtrowania. Na tej zakładce możesz wyświetlić wybory zdarzeń wygenerowane automatycznie, a także utworzyć swoje własne wybory.

Foldery w węźle Serwer administracyjny

Węzeł **Serwer administracyjny – <Nazwa urządzenia>** zawiera następujące foldery:

- **Zarządzane urządzenia**. Ten folder jest przeznaczony do przechowywania, wyświetlania, konfiguracji i modyfikacji struktury grup administracyjnych, zasad grupowych i zadań grupowych.

- **Zarządzanie urządzeniami mobilnymi**. W tym folderze można zarządzać urządzeniami mobilnymi. W folderze **Zarządzanie urządzeniami mobilnymi** znajdują się następujące podfoldery:

  - **Serwery urządzeń mobilnych**. Przeznaczony do zarządzania serwerami iOS MDM.

  - **Urządzenia mobilne**. Ten podfolder umożliwia zarządzanie urządzeniami mobilnymi, KES i iOS MDM.

  - **Certyfikaty**. W tym miejscu można zarządzać certyfikatami urządzeń mobilnych.

- **Wybory urządzeń**. Ten folder jest przeznaczony do szybkiego wyboru urządzeń, które spełniają określone kryteria (wybór urządzeń), spośród wszystkich zarządzanych urządzeń. Na przykład, możesz szybko wybrać urządzenia, na których nie została zainstalowana żadna aplikacja zabezpieczająca, i przejść do tych urządzeń (wyświetlić listę). Na tych wybranych urządzeniach możesz wykonać pewne działania, na przykład, przypisać do nich zadania. Możesz użyć predefiniowanych wyborów lub utworzyć swoje własne wybory.

- **Urządzenia nieprzypisane**. Ten folder zawiera listę urządzeń, które nie zostały włączone do żadnej grupy administracyjnej. Na nieprzypisanych urządzeniach możesz wykonać różne działania, na przykład, przenieść je do grup administracyjnych lub zainstalować na nich aplikacje.

- **Zasady**. W tym folderze można przeglądać i tworzyć zasady.

- **Zadania**. W tym folderze można przeglądać i tworzyć zadania.

- **Licencje Kaspersky**. Zawiera listę kluczy licencyjnych dostępnych dla aplikacji firmy Kaspersky. W obszarze roboczym tego folderu możesz dodać nowe klucze licencyjne do repozytorium kluczy licencyjnych, rozesłać klucze licencyjne na zarządzane urządzenia, a także wyświetlić raport z użycia kluczy licencyjnych.

- **Zaawansowane**. Ten folder zawiera kilka podfolderów odpowiadających różnym grupom funkcji aplikacji.

Folder Zaawansowane. Przenoszenie folderów w drzewie konsoli

Folder **Zaawansowane** zawiera następujące podfoldery:

- **Konta użytkowników**. Zawiera listę sieciowych kont użytkowników.

- **Zarządzanie aplikacjami**. Przeznaczony do zarządzania aplikacjami zainstalowanymi na urządzeniach w sieci. W folderze **Zarządzanie aplikacjami** znajdują się następujące podfoldery:

  - **Kategorie aplikacji**. Przeznaczony do zarządzania niestandardowymi kategoriami aplikacji.

  - **Rejestr aplikacji**. Zawiera listę aplikacji na urządzeniach, na których zainstalowano Agenta sieciowego.

  - **Pliki wykonywalne**. Zawiera listę plików wykonywalnych przechowywanych na urządzeniach klienckich, na których zainstalowano Agenta sieciowego.

  - **Luki w oprogramowaniu**. Zawiera listę luk w aplikacjach na urządzeniach, na których zainstalowano Agenta sieciowego.

  - **Aktualizacje oprogramowania**. Zawiera listę uaktualnień aplikacji pobranych przez Serwer administracyjny, które mogą zostać przesłane na urządzenia.

  - **Wykorzystanie licencji firm trzecich**. Zawiera listę grup licencjonowanych aplikacji. Możesz użyć grup licencjonowanych aplikacji do monitorowania użycia licencji dla oprogramowania firm trzecich (aplikacje, które nie zostały stworzone przez firmę Kaspersky) i możliwych naruszeń ograniczeń licencyjnych.

- **Zdalna instalacja**. Ten folder służy do zarządzania zdalną instalacją systemów operacyjnych i aplikacji. W folderze **Zdalna instalacja** znajdują się następujące podfoldery:

  - **Rozsyłanie obrazów urządzenia**. Służy do instalowania obrazów systemów operacyjnych na urządzeniach.

  - **Pakiety instalacyjne**. Zawiera listę pakietów instalacyjnych, których można użyć do zdalnej instalacji aplikacji na urządzeniach.

- **Szyfrowanie i ochrona danych**. Ten folder służy do zarządzania postępem szyfrowania danych na dyskach i nośnikach wymiennych.

- **Przeszukiwanie sieci**. W tym folderze jest wyświetlana sieć, w której zainstalowany jest Serwer administracyjny. Serwer administracyjny otrzymuje informacje o strukturze sieci i jej urządzeniach poprzez regularne przeszukiwanie sieci Windows, podsieci IP i Active Directory® w sieci korporacyjnej. Wyniki przeszukiwania wyświetlane są w obszarach roboczych odpowiednich folderów: **Domeny**, **Zakresy IP** oraz **Active Directory**.

- **Repozytoria**. Ten folder jest przeznaczony do pracy z obiektami wykorzystywanymi do monitorowania stanu urządzeń klienckich i ich obsługiwania. Folder **Repozytoria** zawiera następujące podfoldery:
  - **Adaptacyjne wykrywanie anomalii**. Zawiera listę elementów wykrytych przez reguły Kaspersky Endpoint Security działające w trybie Inteligentne uczenie na urządzeniach klienckich.
  - **Aktualizacje i poprawki oprogramowania Kaspersky**. Zawiera listę uaktualnień pobranych przez Serwer administracyjny, które mogą zostać przesłane do komputerów klienckich.
  - **Sprzęt**. Zawiera listę sprzętu podłączonego do sieci firmowej.
  - **Kwarantanna**. Zawiera listę obiektów przeniesionych do Kwarantanny przez oprogramowanie antywirusowe znajdujące się na urządzeniach.
  - **Kopia zapasowa**. Zawiera listę kopii zapasowych plików, które w wyniku procesu leczenia zostały usunięte lub zmodyfikowane.
  - **Nieprzetworzone pliki**. Zawiera listę plików przeznaczonych do późniejszego skanowania przez aplikacje antywirusowe.

Możesz zmienić zestaw podfolderów znajdujących się w folderze **Zaawansowane**. Często używane podfoldery można przenieść o jeden poziom wyżej z folderu **Zaawansowane**. Rzadko używane podfoldery można przenieść do folderu **Zaawansowane**.

*W celu przeniesienia podfolderu poza obszar folderu **Zaawansowane**:*

1. W drzewie konsoli wybierz podfolder, który chcesz przenieść poza obszar folderu **Zaawansowane**.
2. W menu kontekstowym podfolderu wybierz **Widok** → **Przenieś z folderu Zaawansowane**.

Podfolder można przenieść poza obszar folderu **Zaawansowane** także z poziomu obszaru roboczego folderu **Zaawansowane**, klikając odnośnik **Przenieś z folderu Zaawansowane** w sekcji z nazwą tego podfolderu.

*W celu przeniesienia podfolderu do folderu **Zaawansowane**:*

1. W drzewie konsoli wybierz podfolder, który chcesz przenieść do folderu **Zaawansowane**.
2. W menu kontekstowym podfolderu wybierz **Widok** → **Przenieś do folderu Zaawansowane**.

Jak zaktualizować dane w obszarze roboczym

W Kaspersky Security Center dane w obszarze roboczym (stany urządzeń, statystyki i raporty) nigdy nie są aktualizowane automatycznie.

W celu zaktualizowania danych w obszarze roboczym:

- Wciśnij klawisz **F5**.
- W menu kontekstowym obiektu z drzewa konsoli wybierz **Odśwież**.
- Kliknij ikonę odśwież ( ) w obszarze roboczym.

Jak poruszać się po drzewie konsoli

Do poruszania się po drzewie konsoli możesz użyć następujących przycisków paska narzędzi:

- – jeden krok wstecz.
- – jeden krok do przodu.
- – jeden poziom wyżej.

Możesz także użyć łańcucha nawigacji znajdującego się w prawym górnym rogu obszaru roboczego. Panel nawigacyjny zawiera pełną ścieżkę do foldera drzewa konsoli, w którym się znajdujesz. Wszystkie elementy panelu (za wyjątkiem ostatniego) są odnośnikami do obiektów w drzewie konsoli.

Jak w obszarze roboczym otworzyć okno właściwości obiektu

Właściwości większości obiektów Konsoli administracyjnej możesz zmienić w oknie właściwości obiektu.

W celu otwarcia okna właściwości obiektu znajdującego się w obszarze roboczym:

- Z menu kontekstowego obiektu wybierz **Właściwości**.
- Zaznacz obiekt i wciśnij **ALT**+**ENTER**.

Jak w obszarze roboczym wybrać grupę obiektów

Grupę obiektów możesz wybrać w obszarze roboczym. Możesz wybrać grupę obiektów, na przykład, do utworzenia zbioru urządzeń, dla których możesz utworzyć zadania w późniejszym czasie.

W celu wybrania zakresu obiektów:

1. Wybierz pierwszy obiekt z zakresu i wciśnij **Shift**.
2. Przytrzymaj wciśnięty klawisz **Shift** i wybierz ostatni obiekt z zakresu.

   Zakres zostanie wybrany.

W celu pogrupowania oddzielnych obiektów:

1. Wybierz pierwszy obiekt z grupy i wciśnij **Ctrl**.
2. Przytrzymaj wciśnięty klawisz **Ctrl** i wybierz inne obiekty, które chcesz uwzględnić w grupie.

Obiekty zostaną pogrupowane.

Jak zmienić zestaw kolumn w obszarze roboczym

Konsola administracyjna umożliwia zmianę zestawu kolumn wyświetlanych w obszarze roboczym.

W celu zmiany zestawu kolumn wyświetlanych w obszarze roboczym:

1. W drzewie konsoli kliknij obiekt, dla którego chcesz zmienić zestaw kolumn.
2. W obszarze roboczym folderu otwórz okno przeznaczone do konfigurowania zestawu kolumn, klikając odnośnik **Dodaj/Usuń kolumny**.
3. W oknie **Dodaj/Usuń kolumny** określ zestaw wyświetlanych kolumn.

Informacje dodatkowe

Tabele w tej sekcji zawierają informacje o menu kontekstowym obiektów Konsoli administracyjnej oraz o stanach obiektów drzewa konsoli i obiektów obszaru roboczego.

Polecenia menu kontekstowego

Ta sekcja wyświetla obiekty Konsoli administracyjnej i odpowiadające im elementy menu kontekstowego (patrz tabela poniżej).

Elementy menu kontekstowego obiektów Konsoli administracyjnej

Obiekt	Element menu	Przeznaczenie elementu menu
Ogólne elementy menu kontekstowego	**Szukaj**	Otwiera okno wyszukiwania urządzeń.
	Odśwież	Odświeża wyświetlanie wybranego obiektu.
	Eksportuj listę	Eksportuje bieżącą listę do pliku.
	Właściwości	Otwiera okno właściwości wybranego obiektu.
	Widok → Dodaj/Usuń kolumny	Dodaje lub usuwa kolumny w tabeli obiektów, w obszarze roboczym.
	Widok → Duże ikony	Wyświetla obiekty w obszarze roboczym jako duże ikony.
	Widok → Małe ikony	Wyświetla obiekty w obszarze roboczym jako małe ikony.
	Widok → Lista	Wyświetla obiekty w obszarze roboczym w postaci listy.
	Widok → Tabela	Wyświetla obiekty w obszarze roboczym w postaci tabeli.
	Widok → Konfiguruj	Konfiguruje wyświetlanie elementów Konsoli administracyjnej.

Obiekt	Element menu	Przeznaczenie elementu menu
Kaspersky Security Center	**Nowa → Serwer administracyjny**	Dodaje Serwer administracyjny do drzewa konsoli.
<Nazwa Serwera administracyjnego>	**Połącz z Serwerem administracyjnym**	Nawiązuje połączenie z Serwerem administracyjnym.
	Odłącz od Serwera administracyjnego	Odłącza od Serwera administracyjnego
Zarządzane urządzenia	**Zainstaluj aplikację**	Uruchamia Kreator zdalnej instalacji.
	Widok → Konfiguruj interfejs	Konfiguruje wyświetlanie elementów interfejsu.
	Usuń	Usuwa Serwer administracyjny z drzewa konsoli.
	Zainstaluj aplikację	Uruchamia Kreator zdalnej instalacji dla grupy administracyjnej.
	Resetuj licznik wirusów	Resetuje licznik wirusów dla urządzeń znajdujących się w grupie administracyjnej.
	Wyświetl raport o zagrożeniach	Tworzy raport o zagrożeniach i aktywności wirusów na urządzeniach znajdujących się w grupie administracyjnej.
	Nowy → Grupa	Tworzy grupę administracyjną.
	Wszystkie zadania → Nowa struktura grupy	Tworzy strukturę grup administracyjnych w oparciu o strukturę domen lub Active Directory.
	Wszystkie zadania → Pokaż wiadomość	Uruchamia Kreator tworzenia nowej wiadomości dla użytkownika, przeznaczony dla użytkowników urządzeń należących do grupy administracyjnej.
Zarządzane urządzenia → Serwery administracyjne	**Nowy → Podrzędny Serwer administracyjny**	Uruchamia Kreator dodawania podrzędnego Serwera administracyjnego.
	Nowy → Wirtualny Serwer administracyjny	Uruchamia Kreator tworzenia nowego wirtualnego Serwera administracyjnego.
Zarządzanie urządzeniami mobilnymi → Urządzenia mobilne	**Nowa → Urządzenie mobilne**	Podłącza nowe urządzenie mobilne użytkownika.
Zarządzanie urządzeniami mobilnymi → Certyfikaty	**Nowy → Certyfikat**	Tworzy certyfikat.
	Utwórz → Urządzenie mobilne	Podłącza nowe urządzenie mobilne użytkownika.
Wybory urządzeń	**Nowy → Nowy wybór**	Tworzy wybór urządzeń.
	Wszystkie zadania → Importuj	Importuje wybór z pliku.
Licencje Kaspersky	**Dodaj kod aktywacyjny lub plik klucza**	Dodaje klucz licencyjny do repozytorium Serwera administracyjnego.
	Aktywuj aplikację	Uruchamia Kreator tworzenia zadania aktywacji aplikacji.
	Raport o użyciu kluczy licencyjnych	Tworzy i wyświetla raport o kluczach licencyjnych na urządzeniach klienckich.
Zarządzanie aplikacjami → Kategorie aplikacji	**Nowy → Kategoria**	Tworzy kategorię aplikacji.
Zarządzanie aplikacjami → Rejestr aplikacji	**Filtr**	Konfiguruje filtr dla listy aplikacji.
	Monitorowane aplikacje	Konfiguruje publikowanie zdarzeń związanych z instalacją aplikacji.
	Usuń aplikacje, które nie są zainstalowane	Tworzy listę wszystkich szczegółów aplikacji, które nie są już zainstalowane na urządzeniach w sieci.
Zarządzanie aplikacjami → Aktualizacje oprogramowania	**Akceptuj warunki Umów licencyjnych aktualizacji**	Akceptuje Umowy licencyjne dla uaktualnień oprogramowania.
Zarządzanie aplikacjami → Wykorzystanie licencji firm trzecich	**Nowy → Grupa licencjonowanych aplikacji**	Tworzy grupę licencjonowanych aplikacji.

Obiekt	Element menu	Przeznaczenie elementu menu
Zdalna instalacja → Pakiety instalacyjne	**Pokaż aktualne wersje aplikacji**	Wyświetla listę aktualnych wersji aplikacji Kaspersky dostępnych na serwerach sieciowych.
	Nowy → Pakiet instalacyjny	Tworzy pakiet instalacyjny.
	Wszystkie zadania → Aktualizuj bazy danych	Aktualizuje bazy danych aplikacji w pakietach instalacyjnych.
	Wszystkie zadania → Pokaż ogólną listę pakietów autonomicznych	Wyświetla listę autonomicznych pakietów utworzonych dla pakietów instalacyjnych.
Wykrywanie urządzeń → Domeny	**Wszystkie zadania → Aktywność urządzenia**	Ustawia odpowiedź Serwera administracyjnego na brak aktywności urządzeń w sieci.
Wykrywanie urządzeń → Zakresy IP	**Nowy → Zakres IP**	Tworzy zakres IP.
Repozytoria → Aktualizacje baz danych i modułów oprogramowania Kaspersky	**Pobierz uaktualnienia**	Otwiera okno właściwości zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego.
	Ustawienia pobierania aktualizacji	Konfiguruje zadanie Pobierz uaktualnienia do repozytorium Serwera administracyjnego.
	Raport o używanych antywirusowych bazach danych	Tworzy i wyświetla raport o wersjach baz danych.
	Wszystkie zadania → Wyczyść repozytorium uaktualnień	Czyści repozytoria aktualizacji na Serwerze administracyjnym.
Repozytoria → Sprzęt	**Nowy → Urządzenie**	Tworzy nowe urządzenie.

Lista zarządzanych urządzeń. Opis kolumn

Poniższa tabela wyświetla nazwy i odpowiednie opisy kolumn listy zarządzanych urządzeń.

Opisy kolumn listy zarządzanych urządzeń

Nazwa kolumny	Wartość
Nazwa	Nazwa NetBIOS urządzenia klienckiego. Opisy ikon nazw urządzeń są podane w dodatku.
Typ systemu operacyjnego	Typ systemu operacyjnego zainstalowanego na urządzeniu klienckim.
Domena Windows	Nazwa domeny Windows, w której znajduje się urządzenie klienckie.
Agent sieciowy jest zainstalowany	Wynik instalacji Agenta sieciowego na urządzeniu klienckim (*Tak*, *Nie*, *Nieznany*).
Agent sieciowy jest uruchomiony	Wynik działania Agenta sieciowego: *Tak*, *Nie*, *Nieznany*.
Ochrona w czasie rzeczywistym	Aplikacja zabezpieczająca jest zainstalowana: (*Tak*, *Nie*, *Nieznany*).
Ostatnie połączenie z Serwerem administracyjnym	Czas, jaki upłynął od momentu połączenia urządzenia klienckiego z Serwerem administracyjnym.
Ostatnia aktualizacja antywirusowych baz danych	Okres, który upłynął od ostatniej aktualizacji zarządzanych urządzeń.
Stan	Bieżący stan urządzenia klienckiego: *OK*, *Krytyczny lub Ostrzeżenie*.

Nazwa kolumny	Wartość
Opis stanu	Przyczyna zmiany stanu urządzenia klienckiego na *Krytyczny* lub *Ostrzeżenie*. Stan urządzenia zmienia się na *Ostrzeżenie* lub *Krytyczny* z następujących powodów: • Aplikacja zabezpieczająca nie jest zainstalowana. • Wykryto zbyt wiele wirusów. • Poziom ochrony w czasie rzeczywistym jest inny niż poziom zdefiniowany przez administratora. • Skanowanie w poszukiwaniu złośliwego oprogramowania nie było wykonywane od dłuższego czasu. • Bazy danych są nieaktualne. • Niepołączony od dłuższego czasu. • Wykryto aktywne zagrożenia. • Wymagane jest ponowne uruchomienie. Powodem ponownego uruchomienia urządzenia może być jedna z poniższych sytuacji: ◦ Uruchomiony ponownie z nieznanego powodu. ◦ Aplikacja nie będzie działała do czasu ponownego uruchomienia. ◦ W celu zakończenia aktualizacji wymagane jest ponowne uruchomienie; aplikacja jest uruchomiona. ◦ W celu zainicjowania aktualizacji wymagane jest ponowne uruchomienie. ◦ W celu zakończenia procesu skanowania lub leczenia wymagane jest ponowne uruchomienie komputera. ◦ W celu zakończenia zdalnej instalacji/dezinstalacji wymagane jest ponowne uruchomienie. ◦ Kończenie szyfrowania danych na dysku. Możesz ustawić powody podczas konfigurowania przełączania stanów urządzeń. • Zainstalowane są niekompatybilne aplikacje. • Wykryto luki w oprogramowaniu. • Wyszukiwanie aktualizacji Windows Update nie było przeprowadzane od dłuższego czasu. • Nieprawidłowy stan szyfrowania. • Ustawienia urządzenia mobilnego nie są zgodne z zasadą. • Wykryto nieprzetworzone incydenty związane z bezpieczeństwem. • Stan urządzenia zdefiniowany przez aplikację. • Brakuje miejsca na dysku urządzenia. • Licencja wkrótce utraci ważność. Stan urządzenia zmienia się tylko na *Krytyczny* z następujących powodów: • Licencja utraciła ważność. • Zarządzanie urządzeniem nie jest możliwe. • Ochrona jest wyłączona. • Aplikacja zabezpieczająca nie jest uruchomiona. Zarządzane aplikacje Kaspersky na urządzeniach klienckich mogą dodawać opisy stanów do listy. Kaspersky Security Center może pobrać opis stanu urządzenia klienckiego od zarządzanych aplikacji Kaspersky, zainstalowanych na tym urządzeniu. Jeśli stan, który został przypisany do urządzenia przez zarządzaną aplikację, różni się od stanu przypisanego przez Kaspersky Security Center, Konsola administracyjna wyświetla stan, który jest najbardziej krytyczny dla bezpieczeństwa urządzenia. Na przykład, jeśli zarządzana aplikacja przypisała do urządzenia stan *Krytyczny*, a Kaspersky Security Center przypisał do niego stan *Ostrzeżenie*, Konsola administracyjna wyświetli dla tego urządzenia stan *Krytyczny* oraz odpowiedni opis dostarczony przez zarządzaną aplikację.
Informacje zaktualizowane	Czas, jaki upłynął od momentu ostatniej pomyślnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym (czyli od ostatniego skanowania sieci).
Nazwa DNS	Nazwa domeny DNS urządzenia klienckiego.
Domena DNS	Główny sufiks DNS.
Adres IP	Adres IP urządzenia klienckiego. Zalecane jest użycie adresu IPv4.
Ostatnio dostępny	Okres, przez jaki urządzenie klienckie było widoczne w sieci.
Ostatnie pełne skanowanie	Data i godzina ostatniego skanowania urządzenia klienckiego, które zostało wykonane przez aplikację antywirusową na żądanie użytkownika.
Łączna liczba wykrytych zagrożeń	Liczba wykrytych zagrożeń.
Stan ochrony w czasie rzeczywistym	Stan ochrony w czasie rzeczywistym: *Uruchamianie*, *Uruchomione*, *Uruchomiona (maksymalna ochrona)*, *Uruchomiona (wysoka wydajność)*, *Uruchomiona (ustawienia zalecane)*, *Uruchomiona (ustawienia niestandardowe)*, *Zatrzymano*, *Wstrzymano*, *Niepowodzenie*.
Adres IP połączenia	Adres IP używany do łączenia z Serwerem administracyjnym Kaspersky Security Center.
Wersja Agenta sieciowego	Wersja Agenta sieciowego.
Wersja aplikacji	Wersja aplikacji zabezpieczającej zainstalowanej na urządzeniu klienckim.
Antywirusowe bazy danych opublikowane	Wersja antywirusowych baz danych.

Nazwa kolumny	Wartość
Ostatnie uruchomienie systemu	Data i godzina, kiedy urządzenie klienckie było ostatnio włączane.
Wymagane jest ponowne uruchomienie	Wymagane jest ponowne uruchomienie urządzenia.
Punkt dystrybucji	Nazwa urządzenia, które pełni rolę punktu dystrybucji dla tego urządzenia klienckiego.
Opis	Opis urządzenia klienckiego otrzymany po przeskanowaniu sieci.
Stan szyfrowania	Stan szyfrowania danych urządzenia klienckiego.
Stan WUA	Stan agenta usługi Windows Update na urządzeniu klienckim. *Tak* odnosi się do urządzeń klienckich, które pobrały aktualizacje poprzez usługę Windows Update z Serwera administracyjnego. *Nie* odnosi się do urządzeń klienckich, które pobrały aktualizacje poprzez usługę Windows Update z innych źródeł.
Typ systemu operacyjnego (bity)	Ilość bitów systemu operacyjnego zainstalowanego na urządzeniu klienckim.
Stan ochrony antyspamowej	Stan ochrony przed spamem: *Uruchamianie, Uruchamianie, Zatrzymano, Wstrzymana, Niepowodzenie, Nieznana*
Stan ochrony przed wyciekiem danych	Stan ochrony przed wyciekiem danych: *Uruchamianie, Uruchamianie, Zatrzymano, Wstrzymana, Niepowodzenie, Nieznana*
Stan ochrony serwerów współpracy	Stan filtrowania zawartości: *Uruchamianie, Uruchamianie, Zatrzymano, Wstrzymana, Niepowodzenie, Nieznana*
Stan ochrony antywirusowej serwerów pocztowych	Stan ochrony antywirusowej serwera pocztowego *Uruchamianie, Uruchamianie, Zatrzymano, Wstrzymana, Niepowodzenie, Nieznana*
Stan czujnika Endpoint Sensor	Stan komponentu Endpoint Detection and Response (KATA): *Uruchamianie, Uruchamianie, Zatrzymano, Wstrzymana, Niepowodzenie, Nieznana*
Utworzono	Godzina utworzenia ikony <Nazwa urządzenia>. Ten atrybut jest używany do porównywania różnych zdarzeń.
Nazwa wirtualnego lub podrzędnego Serwera administracyjnego	Nazwa wirtualnego lub podrzędnego Serwera administracyjnego Ta kolumna jest dostępna tylko na listach, które zawierają urządzenia z różnych Serwerów administracyjnych.
Grupa nadrzędna	Nazwa grupy administracyjnej, w której znajduje się ikona <Nazwa urządzenia>. Ta kolumna jest dostępna tylko na listach, które zawierają urządzenia z różnych Serwerów administracyjnych.
Zarządzane przez inny Serwer administracyjny	Parametr może przyjąć jedną z tych wartości: • True, jeśli podczas zdalnej instalacji aplikacji zabezpieczających na urządzeniu okaże się, że urządzenie jest zarządzane przez inny Serwer administracyjny. • False - w innym przypadku.
Kompilacja systemu operacyjnego	Numer kompilacji systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować wyszukiwanie wszystkich numerów kompilacji, za wyjątkiem określonego.
ID wersji systemu operacyjnego	Identyfikator wydania systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy identyfikator wydania. Możesz także skonfigurować wyszukiwanie wszystkich numerów identyfikatorów wydania, za wyjątkiem określonego.

Stany przypisane do urządzeń, zadań i zasad

Poniższa tabela zawiera listę ikon wyświetlanych w drzewie konsoli i obszarze roboczym Konsoli administracyjnej obok nazw urządzeń, zadań i zasad. Ikony te przedstawiają stany obiektów.

Stany przypisane do urządzeń, zadań i zasad

Ikona	Stan
	Urządzenie z zainstalowanym systemem operacyjnym dla stacji roboczych, wykryte w systemie, ale nie znajdujące się w żadnej grupie administracyjnej.
	Urządzenie z zainstalowanym systemem operacyjnym dla stacji roboczych, należące do grupy administracyjnej, ze stanem *OK*.
	Urządzenie z zainstalowanym systemem operacyjnym dla stacji roboczych, należące do grupy administracyjnej, ze stanem *Ostrzeżenie*.
	Urządzenie z zainstalowanym systemem operacyjnym dla stacji roboczych, należące do grupy administracyjnej, ze stanem *Krytyczny*.
	Urządzenie z zainstalowanym systemem operacyjnym dla stacji roboczych, należące do grupy administracyjnej; jego połączenie z Serwerem administracyjnym zostało zerwane.
	Urządzenie z zainstalowanym systemem operacyjnym dla serwerów, wykryte w systemie, ale nie znajdujące się w żadnej grupie administracyjnej.
	Urządzenie z zainstalowanym systemem operacyjnym dla serwerów, należące do grupy administracyjnej, ze stanem *OK*.
	Urządzenie z zainstalowanym systemem operacyjnym dla serwerów, należące do grupy administracyjnej, ze stanem *Ostrzeżenie*.
	Urządzenie z zainstalowanym systemem operacyjnym dla serwerów, należące do grupy administracyjnej, ze stanem *Krytyczny*.
	Urządzenie z zainstalowanym systemem operacyjnym dla serwerów, należące do grupy administracyjnej; jego połączenie z Serwerem administracyjnym zostało zerwane.
	Urządzenie mobilne wykryte w sieci i nie uwzględnione w żadnej grupie administracyjnej.
	Urządzenie mobilne, znajdujące się w grupie administracyjnej, ze stanem *OK*.
	Urządzenie mobilne, znajdujące się w grupie administracyjnej, ze stanem *Ostrzeżenie*.
	Urządzenie mobilne, znajdujące się w grupie administracyjnej, ze stanem *Krytyczny*.
	Urządzenie mobilne należące do grupy administracyjnej, jego połączenie z Serwerem administracyjnym zostało zerwane.
	Urządzenie chronione UEFI wykryte w sieci, ale nie należące do żadnej grupy administracyjnej. Urządzenie chronione UEFI znajduje się w sieci.
	Urządzenie chronione UEFI wykryte w sieci, ale nie należące do żadnej grupy administracyjnej. Urządzenie chronione UEFI nie znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *OK*. Urządzenie chronione UEFI znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *OK*. Urządzenie chronione UEFI nie znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *Ostrzeżenie*. Urządzenie chronione UEFI znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *Ostrzeżenie*. Urządzenie chronione UEFI nie znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *Krytyczny*. Urządzenie chronione UEFI znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *Krytyczny*. Urządzenie chronione UEFI nie znajduje się w sieci.
	Zasada aktywna.
	Zasada nieaktywna.

	Zasada aktywna dziedziczona od grupy, która została utworzona na głównym Serwerze administracyjnym.
	Zasada aktywna dziedziczony od grupy z wyższego poziomu hierarchii.
	Zadanie (grupowe, Serwera administracyjnego lub dla wskazanych urządzeń) ze stanem *Zaplanowane* lub *Pomyślnie zakończone*.
	Zadanie (grupowe, Serwera administracyjnego lub dla wskazanych urządzeń) ze stanem *Uruchomione*.
	Zadanie (grupowe, Serwera administracyjnego lub dla wskazanych urządzeń) ze stanem *Niepowodzenie*.
	Zadanie dziedziczone od grupy, która została utworzona na głównym Serwerze administracyjnym.
	Zadanie dziedziczone od grupy z wyższego poziomu hierarchii.

Ikony stanów plików w Konsoli administracyjnej

Aby ułatwić zarządzanie plikami w Konsoli administracyjnej Kaspersky Security Center, obok nazw plików wyświetlane są ikony (patrz tabela poniżej). Ikony wskazują stany przypisane do plików przez zarządzane aplikacje Kaspersky na urządzeniach klienckich. Ikony są wyświetlane w obszarach roboczych folderów **Kwarantanna**, **Kopia zapasowa** i **Aktywne zagrożenia**.

Stany są przydzielane do obiektów przez program Kaspersky Endpoint Security zainstalowany na urządzeniu klienckim, na którym znajduje się obiekt.

Zgodność ikon ze stanami plików

Ikona	Stan
	Plik ze stanem *Zainfekowany*.
	Plik ze stanem *Ostrzeżenie* lub *Prawdopodobnie zainfekowany*.
	Plik ze stanem *Dodany przez użytkownika*.
	Plik ze stanem *Fałszywy alarm*.
	Plik ze stanem *Wyleczony*.
	Plik ze stanem *Usunięty*.
	Plik w folderze **Kwarantanna** ze stanem *Niezainfekowany, Zabezpieczony hasłem* lub *Musi zostać przesłany do firmy Kaspersky*. Jeśli obok ikony nie ma opisu stanu, oznacza to, że zarządzana aplikacja firmy Kaspersky na urządzeniu klienckim zgłosiła stan nieznany Kaspersky Security Center.
	Plik w folderze **Kopia zapasowa** ze stanem *Niezainfekowany, Zabezpieczony hasłem* lub *Musi zostać przesłany do firmy Kaspersky*. Jeśli obok ikony nie ma opisu stanu, oznacza to, że zarządzana aplikacja firmy Kaspersky na urządzeniu klienckim zgłosiła stan nieznany Kaspersky Security Center.
	Plik w folderze **Aktywne zagrożenia** ze stanem *Niezainfekowany, Zabezpieczony hasłem* lub *Musi zostać przesłany do firmy Kaspersky*. Jeśli obok ikony nie ma opisu stanu, oznacza to, że zarządzana aplikacja firmy Kaspersky na urządzeniu klienckim zgłosiła stan nieznany Kaspersky Security Center.

Wyszukiwanie i eksportowanie danych

Ta sekcja zawiera informacje o metodach wyszukiwania danych oraz o eksportowaniu danych.

Wyszukiwanie urządzeń

Kaspersky Security Center umożliwia wyszukiwanie urządzeń w oparciu o określone kryteria. Wyniki wyszukiwania można zapisać do pliku tekstowego.

Opcja wyszukiwania pozwala znaleźć następujące urządzenia:

- Urządzenia klienckie w grupach administracyjnych Serwera administracyjnego i jego Serwerów podrzędnych.
- Nieprzypisane urządzenia zarządzane przez Serwer administracyjny i jego Serwery podrzędne.

W celu wyszukania urządzeń klienckich znajdujących się w grupie administracyjnej:

1. W drzewie konsoli wybierz folder grupy administracyjnej.
2. Wybierz **Szukaj** z menu kontekstowego folderu grupy administracyjnej.
3. Na zakładkach w oknie **Szukaj** określ kryteria wyszukiwania urządzeń, a następnie kliknij przycisk **Znajdź teraz**.

   Urządzenia, które spełniają określone kryteria wyszukiwania, są teraz wyświetlane w tabeli, w dolnej części okna **Szukaj**.

W celu wyszukania urządzeń nieprzypisanych:

1. Z drzewa konsoli wybierz folder **Urządzenia nieprzypisane**.
2. Wybierz **Szukaj** z menu kontekstowego folderu **Urządzenia nieprzypisane**.
3. Na zakładkach w oknie **Szukaj** określ kryteria wyszukiwania urządzeń, a następnie kliknij przycisk **Znajdź teraz**.

   Urządzenia, które spełniają określone kryteria wyszukiwania, są teraz wyświetlane w tabeli, w dolnej części okna **Szukaj**.

W celu wyszukania urządzeń niezależnie od tego, czy znajdują się w grupie administracyjnej:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z otwartego menu kontekstowego węzła wybierz **Szukaj**.
3. Na zakładkach w oknie **Szukaj** określ kryteria wyszukiwania urządzeń, a następnie kliknij przycisk **Znajdź teraz**.

   Urządzenia, które spełniają określone kryteria wyszukiwania, są teraz wyświetlane w tabeli, w dolnej części okna **Szukaj**.

W oknie **Szukaj** możesz także wyszukać grupy administracyjne i podrzędne Serwery administracyjne, korzystając z listy rozwijalnej dostępnej w prawym górnym rogu okna. Funkcjonalność wyszukiwania grup administracyjnych i podrzędnych Serwerów administracyjnych nie jest dostępna, jeśli okno **Szukaj** zostało otwarte z poziomu folderu **Urządzenia nieprzypisane**.

Aby wyszukać urządzenia, w oknie **Szukaj** możesz użyć wyrażeń regularnych.

Wyszukiwanie pełnotekstowe jest dostępne w oknie **Szukaj**:

- Na zakładce **Sieć**, w polu **Opis**
- Na zakładce **Sprzęt**, w polach **Urządzenie**, **Producent** i **Opis**

Ustawienia wyszukiwania urządzeń

Poniżej znajdują się opisy ustawień używanych do wyszukiwania zarządzanych urządzeń. Wyniki wyszukiwania są wyświetlane w dolnej części okna.

Sieć

Na zakładce **Sieć** możesz określić kryteria, które będą używane do wyszukiwania urządzeń według ich danych sieciowych:

- **Nazwa urządzenia lub adres IP**

  Nazwa sieciowa systemu Windows (nazwa NetBIOS) urządzenia lub adres IPv4 lub IPv6.

- **Domena Windows**

  Wyświetla wszystkie urządzenia znajdujące się w określonej domenie Windows.

- **Grupa administracyjna**

  Wyświetla urządzenia znajdujące się w określonej grupie administracyjnej.

- **Opis**

  Tekst wyświetlany w oknie właściwości urządzenia: pole **Opis** sekcji **Ogólne**.

  W celu opisania tekstu w polu **Opis** możesz użyć następujących znaków:

  - W słowie:

    - *****. Zastępuje dowolny wiersz dowolną liczbą znaków.

    Na przykład:

    Aby opisać słowa **Serwer** lub **Serwera**, możesz wpisać **Serwer***.

    - **?.** Zastępuje dowolny pojedynczy znak.

    Na przykład:

    Aby opisać słowa **Okno** lub **Okna**, możesz wpisać **Okn?**.

    Gwiazdka (*****) lub znak zapytania (**?**) nie mogą być używane jako pierwsze symbole wyszukiwanego słowa.

  - W celu wyszukania kilku słów użyj:

    - Spacji. Wyświetla wszystkie urządzenia, których opisy zawierają dowolne z wymienionych słów.

    Na przykład:

Aby odszukać frazę zawierającą słowa **Podrzędny** lub **Wirtualny**, wprowadź **Podrzędny Wirtualny** w tekście wyszukiwania.

- **+**. Jeśli przed wyrazem wpisano znak „+”, wszystkie wyniki wyszukiwania będą zawierać ten wyraz.

Na przykład:

Aby odszukać frazę zawierającą zarówno **Podrzędny**, jak i **Wirtualny**, wprowadź **+Podrzędny+Wirtualny**.

- **-**. Jeśli przed wyrazem wpisano znak „-”, żaden z wyników wyszukiwania nie będzie zawierać tego wyrazu.

Na przykład:

Aby odszukać frazę zawierającą **Podrzędny** i nie zawierającą **Wirtualny**, wprowadź **+Podrzędny-Wirtualny**.

- **„<jakikolwiek tekst>”**. Tekst w cudzysłowach musi znajdować się w tekście.

Na przykład:

Aby odszukać frazę zawierającą kombinację słów **Podrzędny Serwer**, wprowadź **Podrzędny Serwer** w tekście wyszukiwania.

- **Zakres IP**

  Jeśli ta opcja jest włączona, możesz wprowadzić początkowy i końcowy adres IP z zakresu adresów IP, do którego muszą zostać włączone odpowiednie urządzenia.

  Domyślnie opcja ta jest wyłączona.

- **Zarządzane przez inny Serwer administracyjny**

  Wybierz jedną z następujących wartości:

  - **Tak**. Brane pod uwagę są tylko urządzenia klienckie zarządzane przez inne Serwery administracyjne.
  - **Nie**. Brane pod uwagę są tylko urządzenia klienckie zarządzane przez ten sam Serwer administracyjny.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

Znaczniki

Na zakładce **Znaczniki** możesz skonfigurować wyszukiwanie urządzeń w oparciu o słowa kluczowe (znaczniki), które wcześniej zostały dodane do opisów zarządzanych urządzeń:

- **Zastosuj, jeśli co najmniej jeden określony znacznik jest zgodny**

  Jeśli ta opcja jest włączona, w wynikach wyszukiwania będą wyświetlane urządzenia z opisami, które zawierają przynajmniej jeden z wybranych znaczników.

  Jeśli ta opcja jest wyłączona, w wynikach wyszukiwania będą wyświetlane tylko urządzeni z opisami, które zawierają wszystkie wybrane znaczniki.

  Domyślnie opcja ta jest wyłączona.

- **Musi zawierać znacznik**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy zawierają wybrany znacznik. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

  Domyślnie opcja ta jest zaznaczona.

- **Nie może zawierać znacznika**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy nie zawierają wybranego znacznika. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

Active Directory

Na zakładce **Active Directory** można określić, że urządzenia mają być wyszukiwane w jednostce organizacyjnej (OU) lub grupie Active Directory. W wyborze można również uwzględnić urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej Active Directory. W celu wybrania urządzeń, zdefiniuj następujące ustawienia:

- **Urządzenie znajduje się w jednostce organizacyjnej Active Directory**

  Jeśli ta opcja jest włączona, wybór będzie zawierał urządzenia z jednostki Active Directory określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

- **Uwzględnij podrzędne jednostki organizacyjne**

  Jeśli ta opcja jest włączona, wybór zawiera urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej domeny.

  Domyślnie opcja ta jest wyłączona.

- **Urządzenie należy do grupy Active Directory**

  Jeśli ta opcja jest włączona, wybór będzie zawierał komputery z grupy Active Directory określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

Aktywność sieciowa

Na zakładce **Aktywność sieciowa** możesz określić kryteria, które będą używane do wyszukiwania urządzeń według ich aktywności sieciowej:

- **Urządzenie jest punktem dystrybucji**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Wybór zawiera urządzenia pełniące role punktów dystrybucji.
  - **Nie**. Urządzenia pełniące role punktów dystrybucji nie będą uwzględniane w wyborze.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Nie odłączaj od Serwera administracyjnego**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Włączona**. Wybór będzie zawierał urządzenia, na których zaznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Wyłączona**. Wybór będzie zawierał urządzenia, na których odznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Przełączanie profilu połączenia**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Wybór będzie zawierał urządzenia, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie**. Wybór nie będzie zawierał urządzeń, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Ostatnie połączenie z Serwerem administracyjnym**

  To pole ustawia kryterium wyszukiwania urządzeń według godziny ostatniego połączenia z Serwerem administracyjnym.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego zostało nawiązane ostatnie połączenie pomiędzy Agentem sieciowym zainstalowanym na urządzeniu klienckim a Serwerem administracyjnym. Wybór będzie zawierał urządzenia mieszczące się w określonym przedziale czasu.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- **Nowe urządzenia odnalezione podczas skanowania sieci**

  Wyszukiwanie nowych urządzeń, które zostały wykryte podczas przeszukiwania sieci w przeciągu kilku ostatnich dni.

  Jeśli ta opcja jest włączona, wybór będzie zawierał nowe urządzenia wykryte podczas wykrywania urządzeń w czasie określonym w polu **Okres wykrywania (dni)**.

  Jeśli ta opcja jest wyłączona, wybór będzie zawierał wszystkie urządzenia wykryte podczas wykrywania urządzeń.

  Domyślnie opcja ta jest wyłączona.

- **Dostępność urządzenia**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie widoczne w sieci.
  - **Nie**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie niewidoczne w sieci.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

Aplikacja

Na zakładce **Aplikacja** możesz określić kryteria, które będą używane do wyszukiwania urządzeń według wybranej zarządzanej aplikacji:

- **Nazwa aplikacji**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji Kaspersky.

  Lista zawiera tylko nazwy aplikacji z wtyczkami administracyjnymi zainstalowanych na stacji roboczej administratora.

  Jeśli żadna aplikacja nie została wybrana, kryterium nie będzie stosowane.

- **Wersja aplikacji**

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według numeru wersji aplikacji Kaspersky.

  Jeśli żaden numer wersji nie został określony, kryterium nie będzie stosowane.

- **Nazwa aktualizacji krytycznej**

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji lub numeru pakietu aktualizacyjnego.

  Jeśli pole będzie puste, kryterium nie będzie stosowane.

- **Ostatnia aktualizacja modułów**

  Ta opcja może zostać użyta do ustawienia kryterium wyszukiwania urządzeń według godziny ostatniej aktualizacji modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego została wykonana ostatnia aktualizacja modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- **Urządzenie jest zarządzane przez Kaspersky Security Center**

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić urządzenia zarządzane poprzez Kaspersky Security Center:

  - **Tak**. Aplikacja uwzględni w wyborze urządzenia zarządzane poprzez Kaspersky Security Center.
  - **Nie**. Aplikacja uwzględni w wyborze urządzenia, jeśli nie są one zarządzane przez Kaspersky Security Center.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Aplikacja zabezpieczająca jest zainstalowana**

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą:

  - **Tak**. Aplikacja uwzględni w wyborze wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą.
  - **Nie**. Aplikacja uwzględni w wyborze wszystkie urządzenia bez zainstalowanej aplikacji zabezpieczającej.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

System operacyjny

Na zakładce **System operacyjny** możesz określić następujące kryteria wyszukiwania urządzeń według typu systemu operacyjnego:

- **Wersja systemu operacyjnego**

  Jeśli pole jest zaznaczone, możesz wybrać system operacyjny z listy. Urządzenia, na których zainstalowany jest określony system operacyjny, są uwzględniane w wynikach wyszukiwania.

- **Typ systemu operacyjnego (bity)**

  Z listy rozwijalnej możesz wybrać architekturę swojego systemu operacyjnego, która określi sposób stosowania reguły przenoszenia do urządzenia (**Nieznany**, **x86**, **AMD64**, or **IA64**). Domyślnie, na liście nie wybrano żadnej opcji i tym samym nie zdefiniowano architektury systemu operacyjnego.

- **Wersja dodatku Service Pack systemu operacyjnego**

  W tym polu możesz określić wersję pakietu systemu operacyjnego (w formacie *X.Y*), która będzie określać sposób stosowania reguły przenoszenia do urządzenia. Domyślnie nie jest zdefiniowana żadna wartość.

- **Kompilacja systemu operacyjnego**

  > To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Numer kompilacji systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować wyszukiwanie wszystkich numerów kompilacji, za wyjątkiem określonego.

- **ID wersji systemu operacyjnego**

  > To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Identyfikator wydania systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy identyfikator wydania. Możesz także skonfigurować wyszukiwanie wszystkich numerów identyfikatorów wydania, za wyjątkiem określonego.

Stan urządzenia

Na zakładce **Stan urządzenia** możesz określić kryteria wyszukiwania urządzeń w oparciu o stan urządzenia z zarządzanej aplikacji:

- **Stan urządzenia**

  Lista rozwijalna, z której możesz wybrać jeden ze stanów urządzenia: *OK*, *Krytyczny*, or *Ostrzeżenie*.

- **Stan ochrony w czasie rzeczywistym**

  Lista rozwijalna, z której możesz wybrać stan ochrony w czasie rzeczywistym. Urządzenia z określonymi stanami ochrony w czasie rzeczywistym są uwzględniane w wyborze.

- **Opis stanu urządzenia**

  W tym polu możesz zaznaczyć pola obok warunków, które, jeśli są spełnione, spowodują przypisanie do urządzenia jednego z następujących stanów: *OK, Krytyczny* lub *Ostrzeżenie*.

- **Stan urządzenia zdefiniowany przez aplikację**

  Lista rozwijalna, z której możesz wybrać stan ochrony w czasie rzeczywistym. Urządzenia z określonymi stanami ochrony w czasie rzeczywistym są uwzględniane w wyborze.

Składniki ochrony

Na zakładce **Składniki ochrony** możesz skonfigurować kryteria wyszukiwania urządzeń klienckich według stanu ochrony.

- **Data opublikowania baz danych**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według daty opublikowania antywirusowej bazy danych. W polach do wprowadzania danych możesz określić przedział czasu, na podstawie którego wykonywane jest wyszukiwanie.

  Domyślnie opcja ta jest wyłączona.

- **Ostatnie skanowanie**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według czasu ostatniego skanowania w poszukiwaniu złośliwego oprogramowania. W polach wejściowych możesz określić przedział czasu, w trakcie którego zostało wykonane ostatnie skanowanie w poszukiwaniu złośliwego oprogramowania.

  Domyślnie opcja ta jest wyłączona.

- **Łączna liczba wykrytych zagrożeń**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według liczby wykrytych wirusów. W polach wejściowych możesz określić niższe i wyższe wartości progowe liczby wykrytych wirusów.

  Domyślnie opcja ta jest wyłączona.

Rejestr aplikacji

Na zakładce **Rejestr aplikacji** możesz skonfigurować wyszukiwanie urządzeń na podstawie aplikacji na nich zainstalowanych:

- **Nazwa aplikacji**

  Lista rozwijalna, z której możesz wybrać aplikację. Urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Wersja aplikacji**

  Pole, w którym możesz określić wersję wybranej aplikacji.

- **Producent**

  Lista rozwijalna, z której możesz wybrać producenta aplikacji zainstalowanej na urządzeniu.

- **Stan aplikacji**

  Lista rozwijalna, z której możesz wybrać stan aplikacji (*Zainstalowana*, *Nie zainstalowana*). Urządzenia, na których określona aplikacja została zainstalowana lub nie została zainstalowana, w zależności od wybranego stanu, zostaną uwzględnione w wyborze.

- **Wyszukaj według aktualizacji**

  Jeśli ta opcja jest włączona, wyszukiwanie będzie się odbywać z użyciem szczegółów aktualizacji dla aplikacji zainstalowanych na odpowiednich urządzeniach. Po zaznaczeniu pola, pola **Nazwa aplikacji**, **Wersja aplikacji** i **Stan aplikacji** zostaną zmienione na **Nazwa aktualizacji**, **Wersja aktualizacji** i **Stan**.

  Domyślnie opcja ta jest wyłączona.

- **Nazwa niekompatybilnej aplikacji zabezpieczającej**

  Lista rozwijalna, z której możesz wybrać aplikacje zabezpieczające firm trzecich. Podczas wyszukiwania, urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Znacznik aplikacji**

  Z listy rozwijalnej możesz wybrać znacznik aplikacji. Wszystkie urządzenia, na których są zainstalowane aplikacje z wybranym znacznikiem w opisie, zostają uwzględnione w wyborze urządzeń.

Hierarchia Serwerów administracyjnych

Na zakładce **Hierarchia Serwerów administracyjnych** zaznacz pole **Uwzględnij dane z podrzędnych Serwerów administracyjnych (do poziomu)**, jeśli chcesz, żeby informacje przechowywane na podrzędnych Serwerach administracyjnych były brane pod uwagę podczas wyszukiwania urządzeń, a w polu wejściowym możesz określić poziom zagnieżdżenia podrzędnego Serwera administracyjnego, z którego informacje są brane pod uwagę podczas wyszukiwania urządzeń. Domyślnie pole to nie jest zaznaczone.

Maszyny wirtualne

Na zakładce **Maszyny wirtualne** możesz skonfigurować wyszukiwanie urządzeń w zależności od tego, czy są to maszyny wirtualne lub czy są one częścią infrastruktury pulpitu wirtualnego (VDI):

- **Jest maszyną wirtualną**

  Z listy rozwijalnej możesz wybrać następujące opcje:

  - **Nieważne**.
  - **Nie**. Wyszukuje urządzenia, które nie są maszynami wirtualnymi.
  - **Tak**. Wyszukuje urządzenia, które są maszynami wirtualnymi.

- **Typ maszyny wirtualnej**

  Z listy rozwijalnej możesz wybrać producenta maszyny wirtualnej.

  Ta lista rozwijalna jest dostępna, jeśli wartość **Tak** lub **Nieważne** została wybrana na liście rozwijalnej **Jest maszyną wirtualną**.

- **Część Virtual Desktop Infrastructure**

  Z listy rozwijalnej możesz wybrać następujące opcje:

  - **Nieważne**.
  - **Nie**. Wyszukuje urządzenia, które nie są częścią Virtual Desktop Infrastructure.
  - **Tak**. Wyszukuje urządzenia, które są częścią Virtual Desktop Infrastructure (VDI).

Sprzęt

Na zakładce **Sprzęt** możesz skonfigurować wyszukiwanie urządzeń klienckich według ich sprzętu:

- **Urządzenie**

  Z listy rozwijalnej możesz wybrać typ jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- **Producent**

  Z listy rozwijalnej możesz wybrać nazwę producenta jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- **Opis**

  Opis urządzenia lub sprzętu. Urządzenia z opisem określonym w tym polu zostaną uwzględnione w wyborze.

  Opis urządzenia w dowolnym formacie może zostać wprowadzony w oknie właściwości tego urządzenia. Pole obsługuje wyszukiwanie pełnotekstowe.

- **Numer ewidencyjny**

  Sprzęt o numerze inwentarzowym podanym w tym polu zostanie uwzględniony w wyborze.

- **Częstotliwość procesora, w MHz**

  Zakres częstotliwości procesora. Urządzenia z procesorami odpowiadającymi zakresowi częstotliwości określonemu w tych polach (wszystkich) zostaną uwzględnione w wyborze.

- **Wirtualne rdzenie procesora**

  Zakres liczby wirtualnych rdzeni w procesorze. Urządzenia z pamięcią RAM odpowiadającą zakresowi określonemu w tych polach (wszystkich) zostaną uwzględnione w wyborze.

- **Pojemność dysku twardego, w GB**

  Zakres wartości rozmiaru dysku twardego urządzenia. Urządzenia z dyskami twardymi odpowiadającymi zakresowi określonemu w tych polach wejściowych (wszystkich) zostaną uwzględnione w wyborze.

- **Rozmiar pamięci RAM, w MB**

  Zakres wartości rozmiaru pamięci RAM urządzenia. Urządzenia z pamięcią RAM odpowiadającą zakresowi określonemu w tych polach wejściowych (wszystkich) zostaną uwzględnione w wyborze.

Luki oraz aktualizacje

Na zakładce **Luki oraz aktualizacje** możesz skonfigurować kryteria wyszukiwania urządzeń zgodnie z ich źródłem Windows Update:

- **WUA został przełączony na Serwer administracyjny**

  Z listy rozwijalnej można wybrać jedną z następujących opcji wyszukiwania:

  - **Tak**. Jeśli wybrano tę opcję, wyniki wyszukiwania będą uwzględniać urządzenia, które uzyskały aktualizacje poprzez Windows Update z Serwera administracyjnego.

  - **Nie**. Jeśli wybrano tę opcję, wyniki będą uwzględniać urządzenia, które uzyskały aktualizacje za pośrednictwem Windows Update z innych źródeł.

Użytkownicy

Na zakładce **Użytkownicy** możesz skonfigurować kryteria wyszukiwania urządzeń według kont użytkowników, którzy logowali się do systemu operacyjnego.

- **Ostatni użytkownik zalogowany do systemu**

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik ostatnio logował się do systemu.

- **Użytkownik zalogowany do systemu co najmniej raz**

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik przynajmniej raz logował się do systemu.

Problemy mające wpływ na stan zarządzanych aplikacji

Na zakładce **Problemy mające wpływ na stan zarządzanych aplikacji** możesz skonfigurować wyszukiwanie urządzeń według opisów ich stanów dostarczonych przez zarządzane aplikacje:

- **Opis stanu urządzenia**

  Możesz zaznaczyć opcje dla opisów stanów z zarządzanej aplikacji. Po odebraniu tych stanów, urządzenia zostaną uwzględnione w wyborze. Jeśli wybierzesz stan wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego stanu na wszystkich listach.

Stan komponentów w zarządzanych aplikacjach

Na zakładce **Stan komponentów w zarządzanych aplikacjach** możesz skonfigurować kryteria wyszukiwania urządzeń według stanów komponentów w zarządzanych aplikacjach:

- **Stan ochrony przed wyciekiem danych**

  Wyszukiwanie urządzeń według stanu Ochrona przed wyciekaniem danych (*Nieznana, Zatrzymano, Uruchamianie, Wstrzymana, Uruchamianie, Niepowodzenie*).

- **Stan ochrony serwerów współpracy**

  Wyszukiwanie urządzeń według stanu ochrony serwerów współpracy (*Nieznana*, *Zatrzymano*, *Uruchamianie, Wstrzymana*, *Uruchamianie*, *Niepowodzenie*).

- **Stan ochrony antywirusowej serwerów pocztowych**

  Wyszukiwanie urządzeń według stanu ochrony dla serwerów pocztowych (*Nieznana, Zatrzymano, Uruchamianie, Wstrzymana, Uruchamianie, Niepowodzenie*).

- **Stan czujnika Endpoint Sensor**

  Wyszukiwanie urządzeń według stanu komponentu Endpoint Sensor (*Nieznana, Zatrzymano, Uruchamianie, Wstrzymana, Uruchamianie, Niepowodzenie*).

Szyfrowanie

- **Szyfrowanie**

  Algorytm blokowego szyfru symetrycznego AES (Advanced Encryption Standard). Z listy rozwijalnej możesz wybrać długość klucza szyfrowania (56-bitowy, 128-bitowy, 192-bitowy lub 256-bitowy).

  Dostępne wartości: *AES56*, *AES128*, *AES192* i *AES256*.

Segmenty chmury

Na zakładce **Segmenty chmury** możesz skonfigurować wyszukiwanie w oparciu o przynależność urządzenia do określonych segmentów chmury:

- **Urządzenie znajduje się w segmencie chmury**

  Jeśli ta opcja jest włączona, możesz kliknąć przycisk **Przeglądaj**, aby określić przeszukiwany segment.

  Jeśli włączono także opcję **Włączając obiekty potomne**, wyszukiwanie jest uruchamiane na wszystkich obiektach potomnych określonego segmentu.

  Wyniki wyszukiwania zawierają tylko urządzenia z wybranego segmentu.

- **Urządzenie wykryte przy pomocy API**

  Z listy rozwijalnej możesz wybrać, czy urządzenie jest wykrywane przez narzędzia API:

  - **AWS**. Urządzenie jest wykrywane przy pomocy AWS API, co oznacza, że urządzenie znajduje się w środowisku chmury AWS.
  - **Azure**. Urządzenie jest wykrywane przy pomocy Azure API, co oznacza, że urządzenie znajduje się w środowisku chmury Azure.
  - **Google Cloud.** Urządzenie jest wykrywane przy pomocy Google API, co oznacza, że urządzenie znajduje się w środowisku Google Cloud.
  - **Nie**. Urządzenie nie może zostać wykryte przy użyciu AWS, Azure lub Google API, co oznacza, że znajduje się poza środowiskiem chmury lub znajduje się w środowisku chmury, ale nie może zostać wykryte przy użyciu API.
  - **Brak wartości**. Warunek nie ma zastosowania.

Składniki aplikacji

Ta sekcja zawiera listę komponentów tych aplikacji, które posiadają odpowiednie wtyczki administracyjne, zainstalowane w Konsoli administracyjnej.

W sekcji **Składniki aplikacji** możesz określić kryteria uwzględniania urządzeń w wyborze zgodnie ze stanami i numerami wersji komponentów, które odpowiadają wybranej aplikacji:

- **Stan**

  Wyszukiwanie urządzeń zgodnie ze stanem komponentu wysłanym przez aplikację do Serwera administracyjnego. Możesz wybrać jeden z następujących stanów: *Brak danych z urządzenia*, *Zatrzymane*, *Uruchamianie*, *Wstrzymane*, *Uruchomione*, *Błąd* lub *Nie zainstalowano*. Jeśli wybrany komponent aplikacji zainstalowanej na zarządzanym urządzeniu posiada określony stan, urządzenie jest uwzględniane w wyborze urządzeń.

Stany wysłane przez aplikacje:

- *Uruchamianie*—komponent jest właśnie w procesie inicjalizacji.
- *Uruchomione*—komponent jest włączony i działa poprawnie.
- *Wstrzymane*—komponent został zawieszony, na przykład, po wstrzymaniu przez użytkownika ochrony w zarządzanej aplikacji.
- *Błąd*—podczas działania komponentu wystąpił błąd.
- *Zatrzymane*—komponent jest wyłączony i nie działa w tym momencie.
- *Nie zainstalowano*—użytkownik nie wybrał komponentu do zainstalowania podczas konfigurowania niestandardowej instalacji aplikacji.

W przeciwieństwie do pozostałych stanów, stan *Brak danych z urządzenia* nie jest wysyłany przez aplikacje. Ta opcja pokazuje, że aplikacje nie posiadają informacji o wybranym stanie komponentu. Na przykład, to może mieć miejsce, gdy wybrany komponent nie należy do żadnej z aplikacji zainstalowanych na urządzeniu lub gdy urządzenie jest wyłączone.

- **Wersja**

  Wyszukiwanie urządzeń zgodnie z numerem wersji komponentu, który wybierasz na liście. Możesz wpisać numer wersji, na przykład `3.4.1.0`, a następnie określić, czy wybrany komponent musi posiadać równą, wcześniejszą lub nowszą wersję. Możesz także skonfigurować wyszukiwanie wszystkich wersji, za wyjątkiem określonej.

Używanie masek w zmiennych typu string

Używanie masek w zmiennych typu string jest dozwolone. Podczas tworzenia masek można użyć następujących wyrażeń regularnych:

- Symbol wieloznaczny (*)—oznacza dowolną sekwencję 0 lub kilku znaków.
- Znak zapytania (?)—zastępuje dowolny pojedynczy znak.
- [<range>]—zastępuje dowolny pojedynczy znak z podanego zakresu lub zbioru.

  Na przykład: [0–9] — dowolna cyfra. [abcdef] — dowolny ze znaków a, b, c, d, e lub f.

Używanie wyrażeń regularnych w polu wyszukiwania

W celu wyszukania określonych słów i znaków, w polu wyszukiwania użyj następujących wyrażeń regularnych:

- *. Zastępuje dowolną sekwencję znaków. Aby wyszukać słowa Serwer, Serwery lub Serwerownia, w polu wyszukiwania wpisz wyrażenie `Server*`.
- ?. Zastępuje dowolny pojedynczy znak. Aby wyszukać słowa Word lub Ward, w polu wyszukiwania wpisz `W?rd`.

  > Tekst znajdujący się w polu wyszukiwania nie może rozpoczynać się od znaku zapytania (?).

- [<zakres>]. Zastępuje dowolny pojedynczy znak z podanego zakresu lub zbioru. Aby wyszukać dowolną cyfrę, w polu wyszukiwania wpisz `[0-9]`. Aby wyszukać jeden ze znaków—a, b, c, d, e lub f— w polu wyszukiwania wpisz `[abcdef]`.

W celu uruchomienia wyszukiwania pełnotekstowego, w polu wyszukiwania użyj następujących wyrażeń regularnych:

- Spacji. Wynikiem są wszystkie urządzenia, których opisy zawierają dowolne z wymienionych słów. Na przykład, aby wyszukać frazę, która zawiera słowo „Podrzędny" lub „Wirtualny": (lub oba te słowa), w polu wyszukiwania wpisz wyrażenie `Secondary Virtual`.
- Znak plusa (+), I lub &&. Jeśli przed wyrazem wpisano znak "+", wszystkie wyniki wyszukiwania będą zawierać ten wyraz. Na przykład, aby wyszukać frazę, która zawiera słowa „Podrzędny" i „Wirtualny", w polu wyszukiwania możesz wpisać jedno z następujących wyrażeń: `+Secondary+Virtual`, `Secondary AND Virtual`, `Secondary && Virtual`.
- LUB lub ||. Jeśli te symbole znajdują się między dwoma słowami, oznacza to, że jedno lub drugie słowo można znaleźć w tekście. Aby wyszukać frazę, która zawiera słowo „Podrzędny" lub „Wirtualny", w polu wyszukiwania wpisz jedno z następujących wyrażeń: `Secondary OR Virtual`, `Secondary || Virtual`.
- Znak minusa (-). Jeśli przed wyrazem wpisano znak "-", żaden z wyników wyszukiwania nie będzie zawierać tego wyrazu. Aby wyszukać frazę, która musi zawierać słowo Podrzędny, a nie może zawierać słowa Wirtualny, w polu wyszukiwania wpisz `+Secondary-Virtual`.
- `"< jakikolwiek tekst >"`. Tekst w cudzysłowach musi znajdować się w tekście. Aby wyszukać frazę, która zawiera kombinację słów Podrzędny Serwer, w polu wyszukiwania wpisz `" Podrzędny Server "`.

Wyszukiwanie pełnotekstowe jest dostępne w następujących sekcjach filtrowania:

- W sekcji filtrowania listy zdarzeń, według kolumn **Zdarzenie** i **Opis**.
- W sekcji filtrowania konta użytkownika, według kolumny **Nazwa**.
- W sekcji filtrowania rejestru aplikacji, według kolumny **Nazwa**, jeśli w sekcji **Pokaż na liście** jako warunek filtrowania wybrano **brak grupowania**.

Eksportowanie list z okien dialogowych

W oknach dialogowych aplikacji możesz wyeksportować listy obiektów do plików tekstowych.

Eksportowanie listy obiektów jest możliwe w sekcjach okien dialogowych, które zawierają przycisk **Eksportuj do pliku**.

Ustawienia zadań

Ta sekcja wyświetla wszystkie ustawienia zadań w Kaspersky Security Center.

Ogólne ustawienia zadania

Ta sekcja zawiera ustawienia, które możesz przeglądać i konfigurować dla większości swoich zadań. Lista dostępnych ustawień zależy od konfigurowanego zadania.

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- Ustawienia ponownego uruchamiania systemu operacyjnego:
  - **Nie uruchamiaj ponownie urządzenia**

    Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

  - **Uruchom urządzenie ponownie**

    Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

  - **Pytaj użytkownika o akcję**

    Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

    Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

- Ustawienia terminarza zadania:

  > Rodzaje harmonogramów mogą się różnić w zależności od zadania.

  - **Ustawienie Zaplanowane uruchomienie:**

    - **Co N godzin**

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

      Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

    - **Co N dni**

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

      Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

    - **Co N minut**

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

      Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

    - **Według dni tygodnia**

      Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

      Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest zaznaczona.

- **Raz**

  Zadanie zostanie uruchomione raz, w określonym dniu i o określonej godzinie (domyślnie w dniu utworzenia zadania).

- **Natychmiast**

  Zadanie uruchamia się natychmiast po zapisaniu ustawień.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po pobraniu nowych uaktualnień do repozytorium**

  Zadanie jest uruchamiane po pobraniu uaktualnień do repozytorium. Na przykład, możesz użyć tego terminarza dla zadania wyszukiwania luk i wymaganych aktualizacji.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

- Urządzenia, do których zadanie zostanie przypisane:
  - **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**

    Zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

    Na przykład, możesz chcieć użyć tej opcji w zadaniu instalowania Agenta sieciowego na nieprzypisanych urządzeniach.

  - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

    Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

    Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

  - **Przypisz zadanie do wyboru urządzeń**

    Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

    Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

  - **Przypisz zadanie do grupy administracyjnej**

    Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

    Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

    Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

- Ustawienia konta:
  - **Konto domyślne**

    Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

    Domyślnie opcja ta jest zaznaczona.

  - **Określ konto**

    Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

  - **Konto**

    Konto, z poziomu którego zadanie jest uruchamiane.

  - **Hasło**

    Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

Jeśli na urządzeniu docelowym nie zainstalowano Agenta sieciowego, należy określić konto, które ma być używane na urządzeniu docelowym w celu uzyskania dostępu do udziału admin$. Wybrane konto będzie przeznaczone wyłącznie do kopiowania danych na Twoje urządzenie. Jeśli na urządzeniu docelowym zainstalowany jest Agent sieciowy, dane zostaną skopiowane za pośrednictwem Agenta sieciowego, a podczas tworzenia zadania nie trzeba określać żadnego konta.

Ustawienia określone po utworzeniu zadania

Następujące ustawienia możesz określić tylko po utworzeniu zadania.

- Ustawienia zadań grupowych:
  - **Roześlij do podgrup**

    Ta opcja jest dostępna tylko w ustawieniach zadań grupowych.

    Kiedy ta opcja jest włączona, zakres zadania obejmuje:
    - Grupa administracyjna, którą wybrano podczas tworzenia zadania.
    - Grupy administracyjne podporządkowane wybranej grupie administracyjnej na dowolnym poziomie niżej w hierarchii grup.

    Gdy ta opcja jest wyłączona, zakres zadania obejmuje tylko grupę administracyjną wybraną podczas tworzenia zadania.

    Domyślnie opcja ta jest włączona.

  - **Wyślij do podrzędnych i wirtualnych Serwerów administracyjnych**

    Gdy ta opcja jest włączona, zadanie działające na głównym serwerze administracyjnym jest również stosowane na drugorzędnych serwerach administracyjnych (w tym wirtualnych). Jeżeli zadanie tego samego typu już istnieje na drugorzędnym serwerze administracyjnym, oba zadania są stosowane na drugorzędnym serwerze administracyjnym — istniejące i odziedziczone z głównego serwera administracyjnego.

    Ta opcja jest dostępna tylko wtedy, gdy włączona jest opcja **Roześlij do podgrup**.

    Domyślnie opcja ta jest wyłączona.

- Zaawansowane ustawienia terminarza:
  - **Włącz urządzenia przed uruchomieniem zadania (min) przy użyciu funkcji Wake-on-LAN**

    System operacyjny na urządzeniu zostanie uruchomiony o określonym czasie przed uruchomieniem zadania. Domyślnie czas ten wynosi pięć minut.

    Włącz tę opcję, jeśli chcesz, aby zadanie było uruchamiane na wszystkich urządzeniach klienckich z obszaru zadania, w tym tych urządzeniach, które są wyłączone, gdy zadanie ma zostać uruchomione.

    Jeśli chcesz, żeby urządzenie było automatycznie wyłączane po zakończeniu zadania, włącz opcję **Wyłącz urządzenia po zakończeniu zadania**. Ta opcja znajduje się w tym samym oknie.

    Domyślnie opcja ta jest wyłączona.

- **Wyłącz urządzenia po zakończeniu zadania**

  Na przykład, możesz chcieć włączyć tę opcję dla zadania instalacji aktualizacji, które instaluje uaktualnienia na urządzeniach klienckich w każdy piątek w godzinach pracy, a następnie wyłącza te urządzenia w weekend.

  Domyślnie opcja ta jest wyłączona.

- **Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż (min)**

  Po minięciu określonego czasu, zadanie jest zatrzymywane automatycznie, niezależnie od tego, czy zostało zakończone.

  Włącz tę opcję, jeśli chcesz przerwać (lub zatrzymać) zadania, których wykonanie zajmuje zbyt dużo czasu.

  Domyślnie opcja ta jest wyłączona. Domyślny czas wykonania zadania to 120 minut.

- Ustawienia powiadomień:

  - Sekcja **Przechowywanie historii zadania**:

    - **Na Serwerze administracyjnym przez (dni)**

      Zdarzenia aplikacji związane z wykonaniem zadania na wszystkich urządzeniach klienckich z obszaru zadania są przechowywane na Serwerze administracyjnym przez określoną liczbę dni. Po upłynięciu tego okresu, informacje są usuwane z Serwera administracyjnego.

      Domyślnie opcja ta jest włączona.

    - **Przechowuj w systemowym dzienniku zdarzeń urządzenia**

      Zdarzenia aplikacji związane z wykonaniem zadania są przechowywane lokalnie w dzienniku zdarzeń systemu Windows każdego urządzenia klienckiego.

      Domyślnie opcja ta jest wyłączona.

    - **Przechowuj w systemowym dzienniku zdarzeń Serwera administracyjnego**

      Zdarzenia aplikacji związane z wykonaniem zadania na wszystkich urządzeniach klienckich z obszaru zadania są przechowywane w sposób scentralizowany w dzienniku zdarzeń Windows systemu operacyjnego Serwera administracyjnego.

      Domyślnie opcja ta jest wyłączona.

    - **Zapisz wszystkie zdarzenia**

      Jeśli ta opcja jest zaznaczona, wszystkie zdarzenia dotyczące zadania zostaną zapisane w dziennikach zdarzeń.

    - **Zapisz zdarzenia dotyczące postępu zadania**

      Jeśli ta opcja jest zaznaczona, tylko zdarzenia dotyczące wykonania zadania zostaną zapisane w dziennikach zdarzeń.

    - **Zapisz jedynie wyniki wykonywania zadania**

      Jeśli ta opcja jest zaznaczona, tylko zdarzenia dotyczące wyników zadania zostaną zapisane w dziennikach zdarzeń.

- **Powiadom administratora o wynikach wykonywania zadania**

  Możesz wybrać metody, przy użyciu których administratorzy otrzymają powiadomienia o wynikach wykonania zadań: za pośrednictwem poczty elektronicznej, przez SMS oraz poprzez uruchomienie pliku wykonywalnego. Aby skonfigurować powiadomienie, kliknij odnośnik **Ustawienia**.

  Domyślnie, wszystkie metody powiadamiania są wyłączone.

- **Powiadom tylko o błędach**

  Jeśli ta opcja jest włączona, administratorzy są powiadamiani tylko wtedy, gdy wykonanie zadania zakończy się błędem.

  Jeśli ta opcja jest wyłączona, administratorzy są powiadamiania po każdym zakończeniu wykonywania zadania.

  Domyślnie opcja ta jest włączona.

- Ustawienia zabezpieczeń

- Ustawienia obszaru zadania

  W zależności od sposobu określenia obszaru zadania, dostępne są następujące ustawienia:

  - **Urządzenia**

    Jeśli obszar zadania jest określany przez grupę administracyjną, możesz przejrzeć tę grupę. Nie ma tutaj dostępnych zmian. Jednakże możesz ustawić **Wykluczenia z zakresu zadania**.

    Jeśli obszar zadania jest określany przez listę urządzeń, możesz zmodyfikować tę listę poprzez dodanie i usunięcie urządzeń.

  - **Wybór urządzeń**

    Możesz zmienić wybór urządzeń, do którego zadanie jest stosowane.

  - **Wykluczenia z zakresu zadania**

    Możesz określić grupę urządzeń, do których zadanie nie jest stosowane. Grupy, które mają zostać wykluczone, mogą być tylko podgrupami grupami administracyjnej, do której zadanie jest stosowane.

- **Historia rewizji**

Ustawienia zadania pobierania aktualizacji do repozytorium serwera administracyjnego

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- **Źródła aktualizacji**

  Jako źródła uaktualnień dla Serwera administracyjnego można użyć następujących zasobów:

  - Serwery aktualizacji Kaspersky

    Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji. Domyślnie, Serwer administracyjny komunikuje się z serwerami aktualizacji Kaspersky i pobiera uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny, aby używał protokołu HTTP zamiast HTTPS.

    Ta opcja jest wybrana domyślnie.

  - Główny Serwer administracyjny

    Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.

  - Folder lokalny lub sieciowy

    Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

    > Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

- **Inne ustawienia**

  Wymuś aktualizację podrzędnych Serwerów administracyjnych

  Jeżeli ta opcja jest włączona, Serwer administracyjny uruchomi zadania aktualizacji na podrzędnych Serwerach administracyjnych zaraz po pobraniu nowych aktualizacji. Zadania aktualizacji są uruchamiane przy użyciu źródła aktualizacji skonfigurowanego we właściwościach zadania na podrzędnych Serwerach administracyjnych.

  Jeśli ta opcja jest wyłączona, zadania aktualizacji na podrzędnych Serwerach administracyjnych będą uruchamiane zgodnie ze swoimi terminarzami.

  Domyślnie opcja ta jest wyłączona.

  Kopiuj pobrane aktualizacje do dodatkowych folderów

  Po otrzymaniu przez Serwer administracyjny uaktualnień skopiuje on je do określonych folderów. Użyj tej opcji, jeśli chcesz ręcznie zarządzać dystrybucją uaktualnień w sieci.

Na przykład, chcesz użyć tej opcji w następującej sytuacji: sieć Twojej organizacji zawiera kilka niezależnych podsieci, a urządzenia z każdej podsieci nie mają dostępu do innych podsieci. Jednakże urządzenia we wszystkich podsieciach mają dostęp do wspólnego udziału sieciowego. W tym przypadku skonfiguruj Serwer administracyjny w jednej z podsieci tak, aby pobierał uaktualnienia z serwerów aktualizacji Kaspersky, włącz tę opcję, a następnie określ ten udział sieciowy. W zadaniach pobierania uaktualnień do repozytorium dla innych Serwerów administracyjnych określ ten sam udział sieciowy jako źródło uaktualnień.

Jeżeli zdecydujesz się na skopiowanie pobranych aktualizacji do folderu lokalnego, musisz wskazać folder na urządzeniu, na którym jest zainstalowany Serwer administracyjny. Ścieżka do folderu zależy od systemu operacyjnego urządzenia. Ponieważ folder lokalny znajduje się na Serwerze administracyjnym opartym na systemie Linux, należy określić ścieżkę POSIX, na przykład: /path/to/dir.

Wybierając folder sieciowy znajdujący się na Serwerze administracyjnym opartym na systemie Linux, należy wcześniej zapewnić dostęp do folderu sieciowego z urządzenia z zainstalowanym Serwerem administracyjnym, montując folder. Dostęp do folderu odbywa się za pomocą protokołu SMB.

Domyślnie opcja ta jest wyłączona.

Nie wymuszaj aktualizacji urządzeń i podrzędnych Serwerów administracyjnych przed zakończeniem kopiowania

Zadania pobierania aktualizacji na urządzenia klienckie i podrzędne Serwery administracyjne zostaną uruchomione dopiero po skopiowaniu aktualizacji z głównego folderu aktualizacji do dodatkowych folderów aktualizacji.

Ta opcja musi być włączona, jeśli urządzenia klienckie i podrzędne Serwery administracyjne pobierają aktualizacje z dodatkowych folderów sieciowych.

Domyślnie opcja ta jest wyłączona.

Ustawienia określone po utworzeniu zadania

Następujące ustawienia możesz określić tylko po utworzeniu zadania.

- Sekcja **Ustawienia**, sekcja **Zawartość aktualizacji**

  Pobierz pliki diff

  Ta opcja włącza funkcję pobierania plików diff.

  Domyślnie opcja ta jest wyłączona.

- Sekcja **Weryfikacja uaktualnień**

  Zweryfikuj uaktualnienia przed rozesłaniem

  Serwer administracyjny pobiera uaktualnienia ze źródła, zapisuje je w tymczasowym repozytorium i uruchamia zadanie określone w polu **Zadanie weryfikacji uaktualnień**. Jeśli zadanie zakończy się pomyślnie, uaktualnienia są kopiowane z tymczasowego repozytorium do folderu współdzielonego na Serwerze administracyjnym, a następnie są rozsyłane do wszystkich urządzeń, dla których Serwer administracyjny pełni rolę źródła uaktualnień (zadania są uruchamiane zgodnie z opcją terminarza - **Po pobraniu nowych uaktualnień do repozytorium**). Zadanie pobierania uaktualnień do repozytorium zostaje zakończone dopiero po zakończeniu zadania *weryfikacji uaktualnień*.

  Domyślnie opcja ta jest wyłączona.

  Zadanie weryfikacji uaktualnień

  To zadanie weryfikuje pobrane uaktualnienia przed ich rozesłaniem na wszystkie urządzenia, dla których Serwer administracyjny pełni rolę źródła uaktualnień.

W tym polu możesz określić utworzone wcześniej zadanie *weryfikacji uaktualnień*. Ewentualnie możesz utworzyć nowe zadanie *weryfikacji uaktualnień*.

Ustawienia zadania Pobierz uaktualnienia do repozytoriów punktów dystrybucji

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- **Źródła aktualizacji**

  Jako źródła uaktualnień dla punktu dystrybucji można użyć następujących zasobów:

  - Serwery aktualizacji Kaspersky

    Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji.

    Opcja ta jest wybrana domyślnie.

  - Główny Serwer administracyjny

    Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.

  - Folder lokalny lub sieciowy

    Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

    > Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

- **Inne ustawienia → Folder do przechowywania aktualizacji**

  Ścieżka do określonego folderu na potrzeby przechowywania zapisanych aktualizacji. Możesz skopiować ścieżkę do określonego folderu do schowka. Nie możesz zmienić ścieżki do określonego folderu w przypadku zadania grupowego.

Ustawienia określone po utworzeniu zadania

Poniższe ustawienie możesz określić w sekcji **Ustawienia**, w bloku **Zawartość aktualizacji** dopiero po utworzeniu zadania.

Pobierz pliki diff

Ta opcja włącza funkcję pobierania plików diff.

Domyślnie opcja ta jest wyłączona.

Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- **Wyszukaj luki i aktualizacje wymienione przez firmę Microsoft**

  Podczas wyszukiwania luk i aktualizacji program Kaspersky Security Center używa informacji o stosowanych aktualizacjach firmy Microsoft ze źródła uaktualnień Microsoft, które są dostępne w danym momencie.

  Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

  Informacje o opcjonalnych aktualizacjach Microsoft Windows nie są wysyłane do Serwera administracyjnego.

  - **Połącz z serwerem aktualizacji, aby zaktualizować dane**

    Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem uaktualnień Microsoft. Następujące serwery mogą pełnić rolę źródeł aktualizacji Microsoft:

    - Serwer administracyjny Kaspersky Security Center (zapoznaj się z ustawieniami zasady Agenta sieciowego)
    - System Windows Server wdrożony w sieci Twojej organizacji wraz z programem Microsoft Windows Server Update Services (WSUS)
    - Serwery aktualizacji Microsoft

    Jeśli ta opcja jest włączona, agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem aktualizacji firmy Microsoft, aby odświeżyć informacje o stosowanych aktualizacjach Microsoft Windows.

    Jeśli ta opcja jest wyłączona, agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła aktualizacji firmy Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia.

    Nawiązywanie połączenia ze źródłem aktualizacji firmy Microsoft może zużywać dużo zasobów. Możesz chcieć wyłączyć tę opcję, jeśli ustawisz regularne nawiązywanie połączenia z tym źródłem uaktualnień w innym zadaniu lub we właściwościach zasady Agenta sieciowego, w sekcji **Aktualizacje oprogramowania i luki**. Jeśli nie chcesz wyłączyć tej opcji, następnie, aby zmniejszyć obciążenie Serwera, możesz skonfigurować terminarz zadania do losowego opóźnienia uruchomienia zadania w ciągu 360 minut.

    Domyślnie opcja ta jest włączona.

Kombinacja następujących opcji ustawień zasady Agenta sieciowego definiuje tryb uzyskiwania aktualizacji:

- Agent usługi Windows Update na zarządzanym urządzeniu łączy się z serwerem aktualizacji w celu pobierania aktualizacji tylko wtedy, gdy opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest włączona we właściwościach zadania *Wyszukiwanie luk i wymaganych aktualizacji*, a opcja **Tryb wyszukiwania aktualizacji systemu Windows** jest ustawiona na **Aktywny** w ustawieniach zasady Agenta sieciowego.

- Jeśli nie potrzebujesz, aby Agent sieciowy nawiązał połączenie ze źródłem aktualizacji systemu Microsoft Windows i pobrał aktualizacje podczas wykonywania zadania *skanowania w poszukiwaniu luk*, możesz ustawić opcję **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, a opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** musi pozostać włączona. Dzięki temu możesz zaoszczędzić zasoby i wykorzystać wcześniej pobrane aktualizacje systemu Windows do skanowania w poszukiwaniu luk w zabezpieczeniach. Możesz użyć trybu pasywnego, jeśli skonfigurujesz otrzymywanie aktualizacji systemu Microsoft Windows w inny sposób. Jeśli odbieranie aktualizacji systemu Microsoft Windows nie zostało skonfigurowane w inny sposób, nie należy ustawiać opcji **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, ponieważ w takim przypadku informacje o aktualizacjach nigdy nie zostaną odebrane.

- Bez względu na stan opcji **Połącz z serwerem aktualizacji, aby zaktualizować dane** (włączona lub wyłączona), jeśli opcja **Tryb wyszukiwania aktualizacji systemu Windows** zostanie ustawiona jako **Wyłączony**, Kaspersky Security Center nie żąda żadnych informacji o aktualizacjach.

- **Wyszukaj luki i aktualizacje innych firm wymienione przez firmę Kaspersky**

  Jeśli ta opcja jest włączona, Kaspersky Security Center wyszukuje luki i wymagane aktualizacje dla aplikacji firm trzecich (aplikacji producentów innych niż Kaspersky i Microsoft) w rejestrze systemu Windows i w folderach określonych pod **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**. Pełna lista obsługiwanych aplikacji firm trzecich jest zarządzana przez Kaspersky.

  Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie szuka luk i wymaganych uaktualnień dla aplikacji firm trzecich. Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft Windows i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

  - **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**

    Foldery, w których Kaspersky Security Center wyszukuje aplikacje firm trzecich, które wymagają naprawienia luk i zainstalowania aktualizacji. Możesz użyć zmiennych systemowych.

    Określ foldery, w których zostaną zainstalowane aplikacje. Domyślnie, lista zawiera foldery systemowe, w których instalowana jest większość aplikacji.

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy zapisywanie plików śledzenia jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

Ustawienia zadania Zainstaluj wymagane aktualizacje i napraw luki

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- **Określ reguły instalacji aktualizacji**

  Te reguły są stosowane do instalacji aktualizacji na urządzeniach klienckich. Jeśli reguły nie zostały określone, zadanie nie zostanie wykonane. Informacje dotyczące działań wykonywanych na regułach znajdziesz w sekcji Reguły instalacji aktualizacji.

- **Uruchom instalację podczas ponownego uruchamiania lub wyłączania urządzenia**

  Jeśli ta opcja jest włączona, aktualizacje są instalowane po ponownym uruchomieniu lub zamknięciu urządzenia. W innym przypadku aktualizacje są instalowane zgodnie z terminarzem.

  Użyj tej opcji, jeśli instalowanie aktualizacji może wpłynąć na działanie urządzenia.

  Domyślnie opcja ta jest wyłączona.

- **Zainstaluj wymagane ogólne składniki systemu**

  Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

  Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

  Domyślnie opcja ta jest wyłączona.

- **Zezwól na instalację nowych wersji aplikacji podczas aktualizacji**

  Jeśli ta opcja jest włączona, aktualizacje są dozwolone, gdy powodują zainstalowanie nowej wersji aplikacji.

  Jeśli ta opcja jest wyłączona, aplikacja nie zostanie zaktualizowana. W takiej sytuacji możesz ręcznie zainstalować nowe wersje aplikacji lub użyć w tym celu innego zadania. Na przykład, możesz użyć tej opcji, jeśli struktura Twojej firmy nie jest obsługiwana przez nową wersję aplikacji lub jeśli chcesz sprawdzić aktualizację w infrastrukturze testowej.

  Domyślnie opcja ta jest włączona.

  > Aktualizowanie aplikacji może spowodować problemy z działaniem powiązanych aplikacji zainstalowanych na urządzeniach klienckich.

- **Pobierz aktualizacje na urządzenie, ale ich nie instaluj**

  Jeśli ta opcja jest włączona, aplikacja pobierze uaktualnienia na urządzenie, ale nie zainstaluje ich automatycznie. Możesz ręcznie zainstalować pobrane aktualizacje.

  Aktualizacje Microsoft są pobierane do folderu systemowego Windows. Aktualizacje aplikacji firm trzecich (aplikacje innych producentów niż Kaspersky i Microsoft) są pobierane do folderu określonego w polu **Pobierz uaktualnienia do**.

  Jeśli ta opcja jest wyłączona, aktualizacje są instalowane na urządzeniu automatycznie.

  Domyślnie opcja ta jest wyłączona.

  - **Pobierz uaktualnienia do**

    Ten folder jest używany do pobierania aktualizacji aplikacji innych firm (aplikacji innych producentów niż Kaspersky i Microsoft).

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy zapisywanie plików śledzenia jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

  - **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

    Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

Ustawienia określone po utworzeniu zadania

Ustawienia w sekcjach wymienionych poniżej można określić dopiero po utworzeniu zadania. Aby uzyskać pełny opis ustawień zadania, zobacz Ogólne ustawienia zadania.

- **Ogólne**. W tej sekcji wyświetlane są ogólne informacje o zadaniu. Możesz także określić, do których urządzeń powinno zostać zastosowane zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.

  - **Roześlij do podgrup**

    Ta opcja jest dostępna tylko w ustawieniach zadań grupowych.

    Kiedy ta opcja jest włączona, zakres zadania obejmuje:

    - Grupa administracyjna, którą wybrano podczas tworzenia zadania.
    - Grupy administracyjne podporządkowane wybranej grupie administracyjnej na dowolnym poziomie niżej w hierarchii grup.

Gdy ta opcja jest wyłączona, zakres zadania obejmuje tylko grupę administracyjną wybraną podczas tworzenia zadania.

Domyślnie opcja ta jest włączona.

- **Wyślij do podrzędnych i wirtualnych Serwerów administracyjnych**

  Gdy ta opcja jest włączona, zadanie działające na głównym serwerze administracyjnym jest również stosowane na drugorzędnych serwerach administracyjnych (w tym wirtualnych). Jeżeli zadanie tego samego typu już istnieje na drugorzędnym serwerze administracyjnym, oba zadania są stosowane na drugorzędnym serwerze administracyjnym — istniejące i odziedziczone z głównego serwera administracyjnego.

  Ta opcja jest dostępna tylko wtedy, gdy włączona jest opcja **Roześlij do podgrup**.

  Domyślnie opcja ta jest wyłączona.

- Aktualizacje do zainstalowania

  W sekcji **Aktualizacje do zainstalowania** możesz przejrzeć listę aktualizacji instalowanych przez zadanie. Wyświetlane są tylko aktualizacje, które odpowiadają zastosowanych ustawieniom zadania.

- Testowa instalacja aktualizacji:

  - **Nie skanuj**. Wybierz tę opcję, jeśli nie chcesz przeprowadzać testowej instalacji aktualizacji.

  - **Uruchom skanowanie na wybranych urządzeniach**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na wybranych urządzeniach. Kliknij przycisk **Dodaj** i wybierz urządzenia, na których chcesz przeprowadzić testową instalację aktualizacji.

  - **Uruchom skanowanie na urządzeniach w określonej grupie**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na grupach urządzeń. W polu **Określ grupę testową** określ grupę urządzeń, na których chcesz przeprowadzić instalację testową.

  - **Uruchom skanowanie na określonym procencie urządzeń**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na określonej liczbie urządzeń. W polu **Procentowy udział urządzeń testowych z wszystkich urządzeń docelowych** określ procentową ilość urządzeń, na których chcesz przeprowadzić testową instalację aktualizacji.

Globalna lista podsieci

Ta sekcja zawiera informacje o globalnej liście podsieci, których możesz użyć w regułach.

Aby przechowywać informacje o podsieciach w Twojej sieci, możesz skonfigurować globalną listę podsieci dla każdego używanego Serwera administracyjnego. Ta lista pomaga w dopasowaniu par {adres IP, maska} i fizycznych jednostek, takich jak oddziały firmy. Możesz użyć podsieci z tej listy w ustawieniach i regułach sieci.

Dodawanie podsieci do globalnej listy podsieci

Możesz dodać podsieci z ich opisami do globalnej listy podsieci.

W celu dodania podsieci do globalnej listy podsieci:

1. W drzewie konsoli wybierz węzeł Serwera administracyjnego, którego potrzebujesz.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W otwartym oknie **właściwości**, w panelu **Sekcje** wybierz **Lista globalnych podsieci**.
4. Kliknij przycisk **Dodaj**.
   Zostanie otwarte okno **Nowa podsieć**.
5. Wypełnij następujące pola:
   - **Ustawienia ogólne**

     Adres IP dodawanej podsieci.
   - **Maska podsieci**

     Maska dodawanej podsieci.
   - **Nazwa**

     Nazwa podsieci. Musi być unikatowa w obrębie globalnej listy podsieci. Jeśli wprowadzisz nazwę, która już istnieje na liście, zostanie dodany indeks, na przykład: ~~1, ~~2.
   - **Opis**

     Opis może zawierać dodatkowe informacje o oddziale firmy, który posiada tę podsieć. Ten tekst pojawi się na wszystkich listach, gdzie ta podsieć jest obecna, na przykład, na liście reguł ograniczających ruch sieciowy.

     To pole nie jest obowiązkowe i może pozostać puste.
6. Kliknij **OK**.

Podsieć pojawi się na liście podsieci.

Przeglądanie i modyfikowanie właściwości podsieci z globalnej listy podsieci

Możesz przejrzeć i zmodyfikować właściwości podsieci na globalnej liście podsieci.

W celu przejrzenia lub zmodyfikowania właściwości podsieci na globalnej liście podsieci:

1. W drzewie konsoli wybierz węzeł Serwera administracyjnego, którego potrzebujesz.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W otwartym oknie **Właściwości**, w lewym panelu **Sekcje** wybierz **Lista globalnych podsieci**.
4. Z listy wybierz żądaną podsieć.
5. Kliknij przycisk **Właściwości**.
   Zostanie otwarte okno **Nowa podsieć**.

6. Jeśli to konieczne, zmień ustawienia podsieci.

7. Kliknij **OK**.

Jeśli wprowadziłeś zmiany, zostaną zachowane.

Korzystanie z Agenta sieciowego dla systemu Windows, Linux i macOS: Porównanie

Korzystanie z Agenta sieciowego różni się w zależności od systemu operacyjnego urządzenia. Ustawienia zasady Agenta sieciowego i pakietu instalacyjnego także różnią się w zależności od systemu operacyjnego. W poniższej tabeli porównano funkcje Agenta sieciowego i scenariusze użycia dostępne dla systemów operacyjnych Windows, macOS i Linux.

Porównanie funkcji Agenta sieciowego

Funkcja Agenta sieciowego	Windows	Linux	macOS
Instalacja			
Automatyczne tworzenie pakietu instalacyjnego Agenta sieciowego po zainstalowaniu Kaspersky Security Center	✓	–	–
Instalowanie w trybie wymuszonym, korzystając ze specjalnych opcji w zadaniu zdalnej instalacji programu Kaspersky Security Center	✓	✓	✓
Instalowanie poprzez wysyłanie do użytkowników urządzeń odnośników do pakietów autonomicznych, wygenerowanych przez Kaspersky Security Center	✓	✓	✓
Instalowanie poprzez klonowanie obrazu dysku twardego administratora z systemem operacyjnym i Agentem sieciowym przy pomocy narzędzi do zarządzania obrazami dysku, dostępnych w Kaspersky Security Center	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	–	–
Instalacja poprzez sklonowanie obrazu dysku twardego administratora z systemem operacyjnym i Agentem sieciowym przy użyciu narzędzi innych firm	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	✓
Instalowanie przy użyciu narzędzi firm trzecich dla zdalnej instalacji aplikacji	✓	✓	✓
Ręczne instalowanie poprzez uruchomienie instalatorów aplikacji na urządzeniach	✓	✓	✓
Instalowanie Agenta sieciowego w trybie cichym	✓	✓	✓

Funkcja Agenta sieciowego	Windows	Linux	macOS
Ręczne łączenie urządzenia klienckiego z Serwerem administracyjnym. Narzędzie klmover	✓	✓	✓
Automatyczne instalowanie aktualizacji i poprawek dla komponentów Kaspersky Security Center	✓	✓	—
Automatyczne rozsyłanie kluczy	✓	✓	✓
Wymuszona synchronizacja	✓	✓	✓ Za wyjątkiem serwera push
Punkt dystrybucji			
Przy użyciu punktu dystrybucji	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	✓
Obliczanie liczby i konfigurowanie punktów dystrybucji	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓ Bez korzystania z funkcji rozpoznawania lokalizacji w sieci (NLA).	✓ Bez korzystania z funkcji rozpoznawania lokalizacji w sieci (NLA).
Przeszukiwanie sieci	✓ • Przeszukiwanie sieci Windows • Przeszukiwanie zakresu IP • Przeszukiwanie kontrolera domeny (Microsoft Active Directory) Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓ • Przeszukiwanie zakresu IP • Przeszukiwanie Zeroconf • Przeszukiwanie kontrolera domeny (Microsoft Active Directory, Samba 4 Active Directory)	—
Uruchamianie usługi KSN proxy po stronie punktu dystrybucji	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	—
Pobieranie aktualizacji za pośrednictwem serwerów aktualizacji Kaspersky do repozytoriów punktów dystrybucji, które dystrybuują aktualizacje do zarządzanych urządzeń	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	— (jeśli co najmniej jedno urządzenie działające pod kontrolą systemu operacyjnego Linux lub macOS znajduje się w zakresie zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji, zadanie zostanie zakończone ze stanem Niepowodzenie nawet wtedy, gdy zostało zakończone pomyślnie na wszystkich urządzeniach z systemem Windows).

Funkcja Agenta sieciowego	Windows	Linux	macOS
Instalowanie aplikacji w trybie push	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	Ograniczone: nie można przeprowadzić instalacji w trybie push na urządzeniach z systemem Windows przy użyciu punktów dystrybucji systemu Linux.	Ograniczone: nie można przeprowadzić instalacji w trybie push na urządzeniach z systemem Windows przy użyciu punktów dystrybucji systemu macOS.
Używanie serwera push	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	—
Informacje o aplikacjach innych firm			
Zdalne instalowanie aplikacji na urządzeniach	✓	—	✓ Więcej szczegółów znajdziesz w poniższym artykule: Instalacja zdalna aplikacji na urządzeniach macOS.
Aktualizacje oprogramowania	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	—	—
Konfigurowanie aktualizacji systemu operacyjnego w zasadzie Agenta sieciowego	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	—	—
Przeglądanie informacji o lukach w oprogramowaniu	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	—	—
Skanowanie aplikacji w poszukiwaniu luk	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	—	—
Inwentaryzacja oprogramowania zainstalowanego na urządzeniach	✓	✓	—
Maszyny wirtualne			
Instalowanie Agenta sieciowego na maszynie wirtualnej	✓	✓	✓
Ustawienia optymalizacji dla Virtual Desktop Infrastructure (VDI)	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	✓

Funkcja Agenta sieciowego	Windows	Linux	macOS
Obsługa dynamicznych maszyn wirtualnych	✓ Ograniczenie: Nieobsługiwane przez Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm.	✓	✓
Inne			
Audyt działań na zdalnym urządzeniu klienckim przy użyciu Udostępniania pulpitu Windows	✓	—	—
Monitorowanie stanu ochrony antywirusowej	✓	✓	✓
Zarządzanie ponownymi uruchomieniami urządzenia	✓	—	—
Obsługa przywracania systemu plików	✓	✓	✓
Używanie Agenta sieciowego jako bramy połączenia	✓	✓	✓
Menedżer połączeń	✓	✓	✓
Przełączanie Agenta sieciowego z jednego Serwera administracyjnego na inny (automatycznie według lokalizacji sieciowej)	✓	—	✓
Sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym. Narzędzie klnagchk	✓	✓	✓
Zdalne połączenie z pulpitem urządzenia klienckiego	✓	—	✓ Korzystając z systemu Virtual Network Computing (VNC).
Pobieranie autonomicznego pakietu instalacyjnego poprzez kreator migracji	✓	✓	✓
Przeszukiwanie Zeroconf	—	✓	—
Wyświetlanie informacji o sprzęcie urządzeń klienckich	✓	✓ Informacje o sprzęcie urządzeń z systemem Linux wysyłane do Serwera administracyjnego przez Agenta sieciowego zainstalowanego na tych urządzeniach ograniczają się do informacji określonych w opisie ustawień zarządzanego urządzenia dla Konsoli administracyjnej i Kaspersky Security Center Web Console.	✓ Informacje o sprzęcie urządzeń z systemem macOS wysyłane do Serwera administracyjnego przez Agenta sieciowego zainstalowanego na tych urządzeniach ograniczają się do informacji określonych w opisie ustawień zarządzanego urządzenia dla Konsoli administracyjnej i Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console

Konsola Kaspersky Security Center Web Console (zwana dalej również Kaspersky Security Center Web Console) to aplikacja internetowa przeznaczona do zarządzania stanem systemu bezpieczeństwa sieci chronionej przez aplikacje firmy Kaspersky.

Przy pomocy aplikacji możesz wykonywać następujące czynności:

- Zarządzać stanem systemu ochrony organizacji.
- Instalować aplikacje firmy Kaspersky na urządzeniach w sieci i zarządzać zainstalowanymi aplikacjami.
- Zarządzać zasadami utworzonymi dla urządzeń w sieci.
- Zarządzać kontami użytkowników.
- Zarządzać zadaniami dla aplikacji zainstalowanych na urządzeniach w sieci.
- Przeglądać raporty dotyczące stanu systemu ochrony.
- Zarządzać dostarczaniem raportów administratorom systemu i innym specjalistom ds. IT.

Informacje o wymaganiach sprzętowych i programowych znajdziesz w wymaganiach dotyczących Web Console.

Kaspersky Security Center Web Console udostępnia interfejs sieciowy, który zapewnia interakcję między urządzeniem a Serwerem administracyjnym poprzez przeglądarkę internetową. Serwer administracyjny to aplikacja przeznaczona do zarządzania aplikacjami firmy Kaspersky zainstalowanymi na urządzeniach w sieci. Serwer administracyjny nawiązuje połączenie z urządzeniami w sieci poprzez kanały chronione przy pomocy Secure Socket Layer (SSL). Jeśli łączysz się z Kaspersky Security Center Web Console przy użyciu przeglądarki internetowej, przeglądarka nawiąże połączenie z serwerem Kaspersky Security Center Web Console Server.

Kaspersky Security Center Web Console obsługuje się w następujący sposób:

1. Użyj przeglądarki internetowej do nawiązania połączenia z Kaspersky Security Center Web Console, gdzie zostanie wyświetlony interfejs portalu internetowego.
2. Użyj kontrolek portalu internetowego do wybrania polecenia, które chcesz uruchomić. Kaspersky Security Center Web Console wykonuje następujące działania:
    - Jeśli wybrano polecenie używane do pobierania informacji (na przykład wyświetlenie listy urządzeń), Kaspersky Security Center Web Console wyśle do Serwera administracyjnego żądanie informacji, odbierze wymagane dane, a następnie wyśle je do przeglądarki w przejrzystym formacie.
    - Jeśli wybrano polecenie używane do zarządzania (na przykład zdalna instalacja aplikacji), Kaspersky Security Center Web Console odbierze polecenie z przeglądarki i wyśle je do Serwera administracyjnego. W następnej kolejności aplikacja pobierze wynik z Serwera administracyjnego i wyśle go do przeglądarki internetowej w przejrzystym formacie.

Kaspersky Security Center Web Console to wielojęzykowa aplikacja. W każdej chwili możesz zmienić język interfejsu, bez ponownego otwierania aplikacji. Podczas instalacji Kaspersky Security Center Web Console razem z Kaspersky Security Center, Kaspersky Security Center Web Console ma ten sam język interfejsu, co plik instalacyjny. Jeśli instalujesz tylko Kaspersky Security Center Web Console, aplikacja ma ten sam język interfejsu co system operacyjny. Jeśli Kaspersky Security Center Web Console nie obsługuje języka pliku instalacyjnego lub systemu operacyjnego, domyślnie jest ustawiany język angielski.

Zarządzanie urządzeniami mobilnymi nie jest obsługiwane w Kaspersky Security Center Web Console. Jednakże, jeśli dodałeś urządzenia mobilne do grupy administracyjnej przy użyciu konsoli Microsoft Management Console, te urządzenia zostaną także wyświetlone w Kaspersky Security Center Web Console.

Diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center i konsoli Kaspersky Security Center Web Console

Rysunek poniżej przedstawia diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center i konsoli Kaspersky Security Center Web Console.

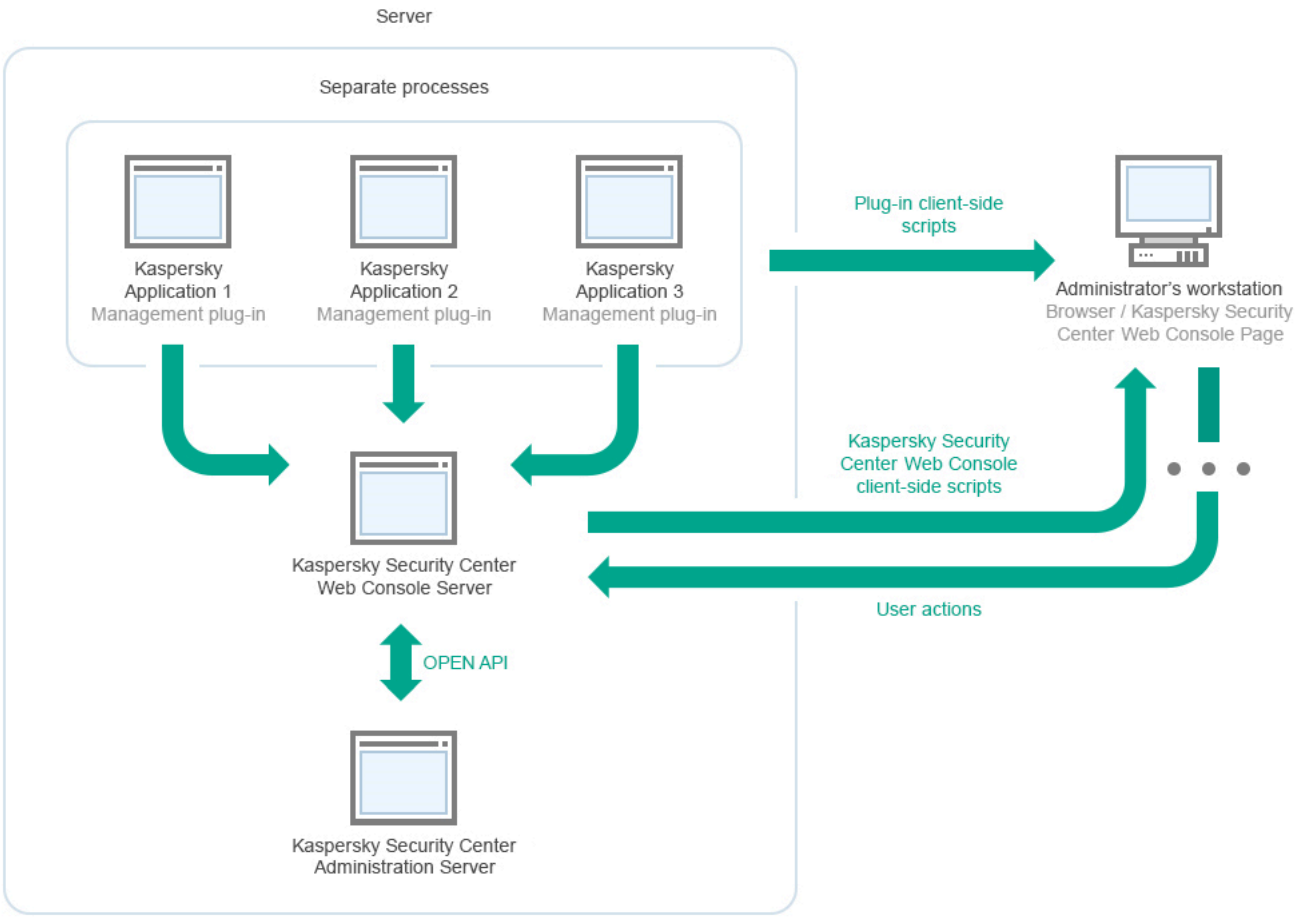


Diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center i konsoli Kaspersky Security Center Web Console

Wtyczki administracyjne dla aplikacji Kaspersky zainstalowanych na chronionych urządzeniach (jedna wtyczka dla każdej aplikacji) są wdrażane razem z Kaspersky Security Center Web Console Server.

Jako administrator uzyskujesz dostęp do Kaspersky Security Center Web Console przy użyciu przeglądarki na swojej stacji roboczej.

Jeśli wykonujesz określone działania w Kaspersky Security Center Web Console, serwer Kaspersky Security Center Web Console Server komunikuje się z serwerem administracyjnym Kaspersky Security Center poprzez interfejs OpenAPI. Serwer Kaspersky Security Center Web Console Server żąda wymaganych informacji z serwera administracyjnego Kaspersky Security Center i wyświetla wyniki Twoich działań w Kaspersky Security Web Console.

Porty używane przez Kaspersky Security Center Web Console

W tabeli poniżej przedstawiono porty, które muszą być otwarte na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console Server (zwany również Kaspersky Security Center Web Console).

Porty używane przez Kaspersky Security Center Web Console

Numer portu	Nazwa usługi	Protokół	Przeznaczenie portu	Obszar
2001	Kaspersky Security Center Product Plugins Server	HTTPS	Port API, który jest używany przez procesy wtyczki zarządzającej do otrzymywania żądań z „Usługi zarządzania Kaspersky Security Center Web Console"	Uruchamianie procesów node.exe wtyczek zarządzania
1329, 2003	Usługa zarządzania Kaspersky Security Center Web Console	HTTPS	Porty API, które są używane do otrzymywania żądań z „Usługi zarządzania Kaspersky Security Center Web Console" działającej na tym samym urządzeniu	Aktualizowanie składników Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	Port API, który jest używany do otrzymywania żądań z „Usługi zarządzania Kaspersky Security Center Web Console" działającej na tym samym urządzeniu	Uruchamianie procesów node.exe Kaspersky Security Center Web Console
3333	Usługa Kaspersky OSMP KAS	HTTPS	Port punktu końcowego autoryzacji OAuth2.0	Identity and Access Manager
4004	Usługa Kaspersky OSMP Facade	HTTPS	Port dostawcy tożsamości OAuth2.0	Identity and Access Manager
4444	Usługa Kaspersky OSMP KAS	HTTPS	Port punktu końcowego introspekcji tokena OAuth2.0	Identity and Access Manager
8200	—	HTTP	Port API, który jest używany do generowania certyfikatów przy użyciu magazynu HashiCorp Vault (więcej informacji znajdziesz na stronie internetowej HashiCorp Vault)	Instalowanie Kaspersky Security Center Web Console i aktualizowanie składników Kaspersky Security Center Web Console
4150, 4151, 4152	Kolejka wiadomości Kaspersky Security Center Web Console	HTTPS	Porty API brokera komunikatów, które są używane do komunikacji między procesami Kaspersky Security Center Web Console oraz wtyczek administracyjnych	Interakcja Kaspersky Security Center Web Console i wtyczek administracyjnych

Poniższa tabela zawiera listę portów, które nie muszą być otwarte na urządzeniu, na którym zainstalowano Kaspersky Security Center Web Console Server. Jednak Kaspersky Security Center Web Console używa tych portów dla Identity and Access Manager.

Porty używane przez Kaspersky Security Center Web Console dla Identity and Access Manager

Numer portu	Nazwa usługi	Protokół	Przeznaczenie portu	Obszar
4445	Usługa Kaspersky OSMP KAS	HTTPS	Główny port Identity and Access Manager, który odbiera konfigurację z Kaspersky Security Center Web Console dla portu punktu końcowego autoryzacji OAuth2.0 (więcej informacji na temat OAuth 2.0 można znaleźć na stronie internetowej OAuth)	Identity and Access Manager
2444	Usługa Kaspersky OSMP Facade	HTTPS	Port do konfiguracji Identity and Access Manager	Identity and Access Manager
2445	Usługa Kaspersky OSMP Facade	HTTPS	Port do połączenia "Kaspersky OSMP KAS Service" z "Kaspersky OSMP Facade Service"	Identity and Access Manager

Interfejs Kaspersky Security Center Web Console

Zarządzanie Kaspersky Security Center odbywa się poprzez interfejs Kaspersky Security Center Web Console.

Okno Kaspersky Security Center Web Console zawiera następujące elementy:

- Menu główne w lewej części okna
- Obszar roboczy w prawej części okna

Menu główne

Menu główne zawiera następujące sekcje:

- **Serwer administracyjny**. Wyświetla nazwę aktualnie połączonego Serwera administracyjnego. Kliknij ikonę ustawień (), aby otworzyć właściwości Serwera administracyjnego.
- **Monitoring & Reporting**. Zapewnia ogląd infrastruktury, stanów ochrony i statystyk.
- **Zasoby (urządzenia)**. Zawiera narzędzia do zasobów, a także zadań i zasad aplikacji Kaspersky.
- **Użytkownicy i role**. Umożliwia zarządzanie użytkownikami i rolami, konfigurowanie praw użytkowników poprzez przypisywanie ról użytkownikom oraz kojarzenie profili zasad z rolami.
- **Operacje**. Zawiera różnorodne operacje, w tym licencjonowanie aplikacji, przeglądanie i zarządzanie zaszyfrowanymi dyskami i zdarzeniami szyfrowania oraz zarządzanie aplikacjami innych firm. Zapewnia to również dostęp do repozytoriów aplikacji.
- **Wykrywanie i wdrażanie**. Umożliwia przeszukiwanie sieci w celu wykrycia urządzeń klienckich i dystrybucję urządzeń do grup administracyjnych ręcznie lub automatycznie. Ta sekcja zawiera także kreator wstępnej konfiguracji i kreator wdrażania ochrony.
- **Platforma handlowa**. Zawiera informacje o całej gamie rozwiązań biznesowych Kaspersky i pozwala wybrać te, których potrzebujesz, a następnie przystąpić do zakupu tych rozwiązań na stronie internetowej Kaspersky.
- **Ustawienia**. Umożliwia wykonanie kopii zapasowej bieżącego stanu wtyczki webowej, aby móc później przywrócić zapisany stan. Zawiera Twoje osobiste ustawienia związane z wyglądem interfejsu, takie jak język lub motyw interfejsu.
- **Menu Twojego konta**. Zawiera łącze do pomocy Kaspersky Security Center. Umożliwia także wylogowanie się z Kaspersky Security Center i przeglądanie wersji Kaspersky Security Center Web Console oraz listy zainstalowanych sieciowych wtyczek zarządzających.

Miejsce pracy

Obszar roboczy wyświetla informacje, które wybrano do przeglądania w sekcjach okna interfejsu Kaspersky Security Center Web Console. Zawiera także elementy sterujące, za pomocą których można skonfigurować sposób wyświetlania informacji.

Przypinanie i odpinanie sekcji menu głównego

Możesz przypiąć sekcje konsoli Kaspersky Security Center Web Console, aby dodać je do ulubionych i uzyskać do nich szybki dostęp z sekcji **Przypięte** w menu głównym.

> Jeżeli nie ma przypiętych elementów, sekcja **Przypięte** nie jest wyświetlana w menu głównym.

Możesz przypiąć sekcje, które wyświetlają tylko strony. Przykładowo, jeśli przejdziesz do **Zasoby (urządzenia)** → **Zarządzane urządzenia**, otworzy się strona z tabelą urządzeń, co oznacza, że możesz przypiąć sekcję **Zarządzane urządzenia**. Jeśli po wybraniu sekcji w menu głównym wyświetli się okno lub nie wyświetli się żaden element, nie będzie możliwości przypięcia takiej sekcji.

Aby przypiąć sekcję:

1. W menu głównym najedź kursorem myszy na sekcję, którą chcesz przypiąć.

   Wyświetlona zostaje ikona pinezki ( ).

2. Kliknij ikonę pinezki ( ).

   Sekcja zostanie przypięta i wyświetlona w sekcji **Przypięte**.

Możesz także usunąć elementy z ulubionych, odpinając je.

Aby odpiąć sekcję:

1. W menu głównym przejdź do sekcji **Przypięte**.

2. Najedź kursorem myszy na sekcję, którą chcesz odpiąć, a następnie kliknij ikonę odepnij ( ).

   Sekcja zostaje usunięta z ulubionych.

Scenariusz: Instalacja i wstępna konfiguracja Kaspersky Security Center Web Console

Ten scenariusz opisuje sposób instalacji Serwera administracyjnego Kaspersky Security Center Kaspersky Security Center Web Console, przeprowadzania wstępnej konfiguracji Serwera administracyjnego przy użyciu kreatora wstępnej konfiguracji, a także instalacji aplikacji Kaspersky na zarządzanych urządzeniach przy użyciu kreatora wdrażania ochrony.

Instalacja i wstępna konfiguracja Kaspersky Security Center Web Console odbywa się w krokach:

1. **Instalowanie systemu zarządzania bazą danych (DBMS)**

   Zainstaluj system DBMS, który będzie używany przez Kaspersky Security Center lub użyj istniejącego systemu.

   Informacje o sposobie zainstalowania wybranego systemu DBMS znajdziesz w tym dokumencie.

2. **Instalowanie Serwera administracyjnego, Konsoli administracyjnej, Agenta sieciowego**

   Konsola administracyjna i wersja serwerowa Agenta sieciowego są instalowane wraz z Serwerem administracyjnym.

   Podczas instalacji Serwera administracyjnego Kaspersky Security Center określ, czy chcesz zainstalować Kaspersky Security Center Web Console na tym samym urządzeniu. Jeśli zdecydujesz się zainstalować oba składniki na tym samym urządzeniu, nie musisz instalować konsoli Kaspersky Security Center Web Console osobno, ponieważ jest ona instalowana automatycznie. Jeśli chcesz zainstalować Kaspersky Security Center Web Console na innym urządzeniu, po zainstalowaniu Serwera administracyjnego Kaspersky Security Center przejdź do instalacji Kaspersky Security Center Web Console.

3. **Instalowanie Kaspersky Security Center Web Console**

   Jeśli nie wybrano instalacji Kaspersky Security Center Web Console wraz z Serwerem administracyjnym Kaspersky Security Center, zainstaluj oddzielnie w pierwszej kolejności Kaspersky Security Center Web Console. Możesz zainstalować Kaspersky Security Center Web Console na innym urządzeniu lub tym samym urządzeniu, na którym zainstalowany jest Serwer administracyjny.

4. **Przeprowadzanie wstępnej konfiguracji**

   Po zakończeniu instalacji Serwera administracyjnego, przy pierwszym połączeniu z Serwerem administracyjnym Kreator wstępnej konfiguracji zostanie uruchomiony automatycznie. Przeprowadź wstępną konfigurację Serwera administracyjnego zgodnie z istniejącymi wymaganiami. Na etapie wstępnej konfiguracji kreator używa domyślnych ustawień do tworzenia zasad i zadań, które są niezbędne do wdrożenia ochrony. Jednakże ustawienia domyślne mogą być mniej niż optymalne dla potrzeb Twojej organizacji. Jeśli to konieczne, możesz edytować ustawienia zasad i zadań.

5. **Licencjonowanie Kaspersky Security Center (opcjonalne)**

   Kaspersky Security Center z obsługą podstawowej funkcjonalności Konsoli administracyjnej nie wymaga licencji. Potrzebujesz licencji komercyjnej, jeśli chcesz używać jednej lub kilku dodatkowych funkcji, w tym Zarządzanie lukami i poprawkami, Zarządzanie urządzeniami mobilnymi i Integracja z systemami SIEM. Możesz ręcznie dodać plik klucza lub kod aktywacyjny dla tych funkcji w odpowiednim kroku kreatora wstępnej konfiguracji.

6. **Wyszukiwanie urządzeń w sieci**

   Ten krok jest częścią kreatora wstępnej konfiguracji. Możesz także ręcznie wyszukiwać urządzenia. Kaspersky Security Center pobiera adresy i nazwy wszystkich urządzeń wykrytych w sieci. Następnie możesz użyć Kaspersky Security Center do zainstalowania aplikacji firmy Kaspersky i oprogramowania innych producentów na wykrytych urządzeniach. Kaspersky Security Center regularnie uruchamia wyszukiwanie urządzeń, co oznacza, że jeśli nowe instancje pojawią się w sieci, zostaną wykryte automatycznie.

7. **Rozmieszczanie urządzeń w grupach administracyjnych**

   Ten krok jest częścią kreatora wstępnej konfiguracji, ale możesz także ręcznie przenieść wykryte urządzenia do grup.

8. **Instalowanie Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci**

   Wdrażanie ochrony w sieci firmowej wiąże się z instalacją Agenta sieciowego i aplikacji zabezpieczających (np. Kaspersky Endpoint Security for Windows) na urządzeniach, które zostały wykryte przez Serwer administracyjny podczas wyszukiwania urządzeń.

   Aby zdalnie zainstalować aplikacje, uruchom Kreator wdrażania ochrony.

Aplikacje zabezpieczające chronią urządzenia przed wirusami i innymi programami stwarzającymi zagrożenie. Agent sieciowy zapewnienia komunikację pomiędzy urządzeniem a Serwerem administracyjnym. Domyślnie ustawienia Agenta sieciowego są konfigurowane automatycznie.

Przed rozpoczęciem instalacji Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci, upewnij się, że te urządzenia są dostępne (włączone).

9. **Rozsyłanie kluczy licencyjnych na urządzenia klienckie**

   Roześlij klucze licencyjne na urządzenia klienckie, aby aktywować zarządzane aplikacje zabezpieczające na tych urządzeniach.

10. **Instalowanie Kaspersky Security for Mobile (opcjonalnie)**

    Jeśli planujesz zarządzać firmowymi urządzeniami mobilnymi, postępuj zgodnie z instrukcjami podanymi w pomocy dla Kaspersky Security for Mobile, aby uzyskać informacje o wdrożeniu Kaspersky Endpoint Security for Android.

11. **Konfigurowanie zasad aplikacji Kaspersky**

    Aby zastosować różne ustawienia aplikacji na różnych urządzeniach, możesz użyć zarządzania ochroną skoncentrowaną na urządzeniu i/lub zarządzania ochroną skoncentrowaną na użytkowniku. Zarządzanie ochroną skoncentrowaną na urządzeniu może zostać zaimplementowane przy użyciu zasad i zadań. Możesz zastosować zadania tylko do tych urządzeń, które spełniają określone warunki. Aby ustawić warunki filtrowania urządzeń, użyj znaczników i wyborów urządzeń.

12. **Monitorowanie stanu ochrony sieci**

    Możesz monitorować swoją sieć przy użyciu widżetów na panelu nawigacyjnym, generować raporty z aplikacji Kaspersky, konfigurować i przeglądać wybory zdarzeń otrzymane z aplikacji na zarządzanych urządzeniach, a także przeglądać listy powiadomień.

Instalacja

Ta sekcja opisuje instalację Kaspersky Security Center i Kaspersky Security Center Web Console.

Instalowanie Kaspersky Security Center (Instalacja standardowa)

Ta procedura opisuje sposób instalacji Kaspersky Security Center. Przed instalacją musisz zainstalować system zarządzania bazą danych.

W celu zainstalowania Kaspersky Security Center:

1. Z poziomu konta z uprawnieniami administracyjnymi uruchom plik wykonywalny ksc_<numer wersji>_full_<język lokalizacji>.exe.
2. W otwartym oknie wyboru aplikacji kliknij **Zainstaluj Kaspersky Security Center**.

   Zostanie uruchomiony kreator instalacji Serwera administracyjnego Kaspersky Security Center.
3. Począwszy od okna Witamy, używaj przycisku **Dalej**, aby przejść przez kroki kreatora.
4. Jeśli Microsoft .NET Framework nie jest zainstalowany, zainstaluj go.
5. Zaakceptuj warunki Umowy licencyjnej i Polityki prywatności.

6. Wybierz typ instalacji. W celu oceny zalecane jest pozostawienie domyślnej wartości **Standardowa**.

7. Jeśli chcesz zainstalować Kaspersky Security Center Web Console na tym samym urządzeniu, zaznacz pole **Zainstaluj Kaspersky Security Center Web Console**.

   W przypadku usunięcia zaznaczenia pola będzie można później zainstalować Kaspersky Security Center Web Console osobno na tym samym lub innym urządzeniu.

8. Wybierz rozmiar sieci. W celu oceny zalecane jest pozostawienie domyślnej wartości **Mniej niż 100 urządzeń w sieci**.

9. Wybierz typ serwera bazy danych, który zainstalowałeś wcześniej.

10. Określ parametry połączenia dla serwera bazy danych, który zainstalowałeś wcześniej.

11. Określ parametry autoryzacji dla serwera bazy danych, który zainstalowałeś wcześniej.

12. Kliknij przycisk **Zainstaluj**, aby uruchomić instalację.

13. Po pomyślnym zakończeniu instalacji, wybierz, czy chcesz uruchomić Konsolę administracyjną od razu po zamknięciu kreatora.

    Jeśli wybierzesz, żeby otworzyć Kaspersky Security Center Web Console, zostanie wyświetlony ekran logowania. Następnie będziesz mógł przeprowadzić wstępną konfigurację Serwera administracyjnego przy użyciu kreatora wstępnej konfiguracji.

    Możesz otworzyć konsolę Kaspersky Security Center Web Console tylko wtedy, gdy jest już zainstalowana. Nie możesz otworzyć konsoli Kaspersky Security Center Web Console, jeśli nie zainstalowano jej podczas instalacji Kaspersky Security Center lub oddzielnie.

14. W otwartej Konsoli administracyjnej kliknij zainstalowany Serwer administracyjny.

15. W otwartym oknie Certyfikat Serwera administracyjnego kliknij przycisk **Tak**, aby kontynuować.

Kreator wstępnej konfiguracji Serwera administracyjnego jest uruchamiany, jeśli nie uruchomiłeś go w internetowej Konsoli administracyjnej.

Rozwiązywanie problemów

Jeśli okno Certyfikat Serwera administracyjnego nie zostanie otwarte, a błędy połączenia są wyświetlane:

1. W systemie Windows otwórz **Usługi** (**Panel sterowania** → **Narzędzia administracyjne** → **Usługi**). Sprawdź, czy usługi Agent sieciowy Kaspersky Security Center i Serwer administracyjny Kaspersky Security Center są uruchomione.

2. W systemie Windows otwórz **Podgląd zdarzeń** (**Panel sterowania** → **Narzędzia administracyjne** → **Narzędzia administracyjne**), a następnie wybierz **Dzienniki aplikacji i usług** → **Dziennik zdarzeń aplikacji Kaspersky**. Upewnij się, że dziennik nie zawiera błędów, a zawiera zdarzenia, takie jak **Serwer administracyjny <numer wersji> jest uruchomiony**.

Instalowanie Kaspersky Security Center Web Console

Ta sekcja opisuje sposób oddzielnego zainstalowania serwera Kaspersky Security Center Web Console Server (zwany również Kaspersky Security Center Web Console). Przed instalacją musisz zainstalować system DBMS i Serwerem administracyjnym Kaspersky Security Center. Możesz zainstalować Kaspersky Security Center Web Console na tym samym urządzeniu, na którym jest zainstalowane Kaspersky Security Center, lub na innym.

W celu zainstalowania Kaspersky Security Center Web Console:

1. Z poziomu konta z uprawnieniami administracyjnymi uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe.

   Zostanie uruchomiony kreator instalacji.

2. Wybierz język kreatora instalacji.

3. W oknie powitalnym kliknij **Dalej**.

4. W oknie **Umowa licencyjna** przeczytaj i zaakceptuj warunki Umowy licencyjnej. Po zaakceptowaniu Umowy licencyjnej użytkownika końcowego instalacja będzie kontynuowana. W innej sytuacji przycisk **Dalej** będzie niedostępny.

5. W oknie **Folder docelowy** wybierz folder, w którym zostanie zainstalowana konsola Kaspersky Security Center Web Console (domyślnie, %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie w trakcie instalacji.

   Można zmienić folder docelowy przy użyciu przycisku **Przeglądaj**.

6. W oknie **Ustawienia połączenia Kaspersky Security Center Web Console** określ następujące informacje:

   - Adres konsoli Kaspersky Security Center Web Console (domyślnie, 127.0.0.1).
   - Port, którego Kaspersky Security Center Web Console będzie używać do połączeń przychodzących, czyli port zapewniający dostęp do konsoli Kaspersky Security Center Web Console z przeglądarki (domyślnie 8080).

   Zalecane jest pozostawienie domyślnych wartości adresu i numeru portu.

   Jeśli chcesz, możesz kliknąć **Sprawdź**, aby upewnić się, że wybrany port jest dostępny.

   Jeśli chcesz włączyć zapisywanie działań Kaspersky Security Center Web Console, zaznacz odpowiednią opcję. Jeśli nie zaznaczysz tej opcji, pliki raportu konsoli Kaspersky Security Center Web Console nie zostaną utworzone.

7. W oknie **Ustawienia konta** określ nazwy kont i hasła.

   Zalecane jest używanie domyślnych kont.

8. W oknie **Certyfikat klienta** wybierz jedną z następujących opcji:

   - **Wygeneruj nowy certyfikat**. Ta opcja jest zalecana, jeśli nie masz certyfikatu przeglądarki.
   - **Wybierz istniejący certyfikat**. Możesz wybrać tę opcję, jeśli już posiadasz certyfikat przeglądarki; w tym przypadku określ ścieżkę do niego.
   - Jeśli wybierzesz wygenerowanie nowego certyfikatu, po otwarciu Kaspersky Security Center Web Console przeglądarka może poinformować Cię, że połączenie z Kaspersky Security Center Web Console nie jest prywatne, a certyfikat Kaspersky Security Center Web Console jest nieważny. Takie ostrzeżenie pojawia się, ponieważ certyfikat Kaspersky Security Center Web Console jest certyfikatem z podpisem własnym i jest automatycznie generowany przez Kaspersky Security Center. Aby usunąć to Ostrzeżenie, utwórz certyfikat, który jest zaufany w Twojej infrastrukturze i spełnia wymagania certyfikatów niestandardowych. Następnie wybierz opcję **Wybierz istniejący certyfikat** w oknie **Certyfikat klienta**, a następnie określ ścieżkę do własnego certyfikatu.

   Certyfikaty w formacie PFX nie są obsługiwane przez konsolę Kaspersky Security Center Web Console. Aby użyć takiego certyfikatu, należy najpierw przekonwertować go do obsługiwanego formatu PEM za pomocą narzędzia wieloplatformowego opartego na OpenSSL, takiego jak OpenSSL dla Windows.

9. W oknie **Zaufane Serwery administracyjne** upewnij się, że Twój Serwer administracyjny znajduje się na liście, a następnie kliknij **Dalej**, aby przejść do ostatniego okna instalatora.

   Jeśli chcesz dodać nowy Serwer administracyjny do listy, kliknij przycisk **Dodaj**. W otwartym oknie określ właściwości nowego zaufanego Serwera administracyjnego:

   - **Nazwa Serwera administracyjnego**

     Nazwa Serwera administracyjnego, która będzie wyświetlana w oknie logowania Kaspersky Security Center Web Console.

   - **Adres Serwera administracyjnego**

     Adres IP urządzenia, na którym instalujesz Serwer administracyjny.

   - **Port Serwera administracyjnego**

     Port OpenAPI, którego Kaspersky Security Center Web Console używa do łączenia się z Serwerem administracyjnym (wartość domyślna to 13299).

   - **Certyfikat Serwera administracyjnego**

     Plik certyfikatu jest przechowywany na urządzeniu, na którym zainstalowany jest Serwer administracyjny. Domyślna ścieżka do certyfikatu Serwera administracyjnego:

     - W systemie Windows —%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
     - W systemie Linux — /var/opt/kaspersky/klnagent_srv/1093/cert/

     Jeśli instalujesz Kaspersky Security Center Web Console na tym samym urządzeniu, na którym zainstalowany jest Serwer administracyjny, użyj jednej ze ścieżek podanych powyżej. W przeciwnym razie skopiuj plik certyfikatu z urządzenia, na którym zainstalowany jest Serwer administracyjny, na urządzenie, na którym instalujesz Kaspersky Security Center Web Console, a następnie określ lokalną ścieżkę do certyfikatu.

10. W oknie **Zarządzanie tożsamością i dostępem (IAM)** określ, czy chcesz zainstalować Identity and Access Manager (zwany również IAM). Jeśli zdecydujesz się zainstalować Identity and Access Manager, określ następujące numery portów:

    - **Port administratora KAS**. Domyślnie, port 4445 jest używany do odbierania konfiguracji z Kaspersky Security Center Web Console dla portu punktu końcowego autoryzacji OAuth2.0.
    - **Port administratora fasady**. Domyślnie, port 2444 jest używany do konfiguracji Identity and Access Manager.
    - **Port interakcji z fasadą**. Domyślnie, port 2445 jest używany do połączenia Kaspersky OSMP KAS Service z Kaspersky OSMP Facade Service.

    Jeśli chcesz, możesz zmienić domyślne numery portów. W przyszłości nie będzie można ich zmienić za pomocą Kaspersky Security Center Web Console.

11. W ostatnim oknie instalatora kliknij **Zainstaluj**, aby rozpocząć instalację.

Po pomyślnym zakończeniu instalacji, skrót pojawi się na Twoim pulpicie i będziesz mógł zalogować się do Kaspersky Security Center Web Console.

Kreator wstępnej konfiguracji Serwera administracyjnego jest uruchamiany, jeśli nie uruchomiono go w Konsoli administracyjnej opartej o konsolę Microsoft Management Console.

Rozwiązywanie problemów

Jeśli konsola Kaspersky Security Center Web Console nie zostanie wyświetlona w przeglądarce pod wpisanym adresem URL:

1. Sprawdź, czy określiłeś poprawną nazwę hosta lub adres IP urządzenia, na którym jest zainstalowana konsola Kaspersky Security Center Web Console.
2. Sprawdź, czy urządzenie, którym chcesz zarządzać, ma dostęp do urządzenia, na którym jest zainstalowana konsola Kaspersky Security Center Web Console.
3. Sprawdź, czy ustawienia zapory sieciowej na urządzeniu, na którym jest zainstalowana konsola Kaspersky Security Center Web Console, zezwala na połączenia przychodzące poprzez port 8080 i dla aplikacji node.exe.
4. W systemie Windows otwórz **Usługi**. Sprawdź, czy usługa Kaspersky Security Center Web Console jest uruchomiona.
5. Sprawdź, czy masz dostęp do Kaspersky Security Center przy użyciu Konsoli administracyjnej.
6. W systemie Windows otwórz **Podgląd zdarzeń**, a następnie wybierz **Dzienniki aplikacji i usług → Dziennik zdarzeń aplikacji Kaspersky**. Upewnij się, że dziennik nie zawiera błędów.

Instalowanie Kaspersky Security Center Web Console połączonej z Serwerem administracyjnym zainstalowanym na węzłach klastra przełączania awaryjnego

Ta sekcja opisuje sposób instalacji Serwera Kaspersky Security Center Web Console Server (zwanego dalej również Kaspersky Security Center Web Console), który łączy się z Serwerem administracyjnym zainstalowanym na węzłach klastra trybu failover Kaspersky Security Center lub Windows Server. Przed zainstalowaniem Kaspersky Security Center Web Console zainstaluj system DBMS i Serwer administracyjny Kaspersky Security Center na węzłach klastra trybu failover Kaspersky Security Center lub na węzłach klastra trybu failover Windows Server.

Jeśli korzystasz z klastra trybu failover Windows Server, nie zalecamy instalowania Kaspersky Security Center Web Console na węźle klastra trybu failover. W przypadku awarii węzła utracisz dostęp do Serwera administracyjnego.

W celu zainstalowania Kaspersky Security Center Web Console, która łączy się z Serwerem administracyjnym zainstalowanym na węzłach klastra przełączania awaryjnego:

1. Wykonaj kroki instalacji Kaspersky Security Center Web Console, zaczynając od kroku 1 do kroku 8.
2. W kroku 9, w oknie **Zaufane Serwery administracyjne** kliknij przycisk **Dodaj**, aby dodać klaster przełączania awaryjnego jako zaufany Serwer administracyjny.

   W otwartym oknie określ następujące właściwości:

   - **Nazwa Serwera administracyjnego**

     Nazwa klastra, która będzie wyświetlana w oknie logowania Kaspersky Security Center Web Console.

   - **Adres Serwera administracyjnego**

     W zależności od typu klastra pracy awaryjnej określ adres klastra:

     - **Klaster trybu failover Kaspersky Security Center**. Określ adres IP dodatkowej karty sieciowej jako adres klastra, jeśli karta została utworzona podczas przygotowywania węzłów klastra. W przeciwnym razie określ adres IP modułu równoważenia obciążenia innej firmy, którego używasz.

     - **Klaster trybu failover Windows Server**. Określ adres klastra uzyskany podczas tworzenia klastra trybu failover Windows Server.

   - **Port Serwera administracyjnego**

     Port OpenAPI, którego Kaspersky Security Center Web Console używa do łączenia się z Serwerem administracyjnym (wartość domyślna to 13299).

   - **Certyfikat Serwera administracyjnego**

     Certyfikat Serwera administracyjnego znajduje się we współdzielonym magazynie danych klastra trybu failover Kaspersky Security Center lub klastra trybu failover Windows Server. Domyślna ścieżka do pliku certyfikatu: <udostępniony folder danych>\1093\cert\klserver.cer. Skopiuj plik certyfikatu ze współdzielonego magazynu danych na urządzenie, na którym instalujesz Kaspersky Security Center Web Console. Określ lokalną ścieżkę do certyfikatu Serwera administracyjnego.

3. Kontynuuj rutynową instalację Kaspersky Security Center Web Console.

Po zakończeniu instalacji, skrót pojawi się na Twoim pulpicie i będzie można zalogować się do Kaspersky Security Center Web Console.

Aktualizowanie Kaspersky Security Center Web Console

Jeśli chcesz użyć nowszej wersji Kaspersky Security Center Web Console bez usuwania aktualnie zainstalowanej instancji, możesz użyć standardowej procedury aktualizacji w instalatorze Kaspersky Security Center Web Console.

W celu zaktualizowania Kaspersky Security Center Web Console:

1. Z poziomu konta z uprawnieniami administratora uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe, gdzie <numer kompilacji> oznacza kompilację Kaspersky Security Center Web Console, której numer jest wyższy niż aktualnie zainstalowanej instancji.

2. W otwartym oknie kreatora instalacji wybierz język, a następnie kliknij **OK**.

3. W oknie powitalnym wybierz opcję **Uaktualnij**, a następnie kliknij **Dalej**.

4. W oknie **Umowa licencyjna** przeczytaj i zaakceptuj warunki Umowy licencyjnej. Po zaakceptowaniu Umowy licencyjnej użytkownika końcowego instalacja będzie kontynuowana. W innej sytuacji przycisk **Dalej** będzie niedostępny.

5. Przejdź przez kroki kreatora instalacji, aż do zakończenia instalacji. W kolejnych krokach możesz zmodyfikować ustawienia Kaspersky Security Center Web Console, które określiłeś podczas poprzedniej instalacji. W kroku **Można rozpocząć modyfikację programu Kaspersky Security Center Web Console** kliknij przycisk **Uaktualnij**. Zaczekaj, aż nowe ustawienia zostaną zastosowane, a w kolejnym kroku kreatora instalacji kliknij **Zakończ**. Możesz także kliknąć odnośnik **Uruchom rozszerzenie Kaspersky Security Center Web Console w przeglądarce**, aby od razu uruchomić zaktualizowaną instancję Kaspersky Security Center Web Console.

   > Modyfikowanie ustawień Kaspersky Security Center Web Console podczas aktualizacji jest dostępne tylko w Kaspersky Security Center Web Console w wersji 12.2 lub nowszej.

   Twoja instancja konsoli Kaspersky Security Center Web Console została zaktualizowana.

Certyfikaty do pracy z Kaspersky Security Center Web Console

Ta sekcja opisuje sposób wystawiania i zastępowania certyfikatów dla konsoli internetowej Kaspersky Security Center Web Console oraz odnawiania certyfikatu dla serwera administracyjnego, jeśli serwer współpracuje z konsolą internetową Kaspersky Security Center Web Console.

Ponowne wystawianie certyfikatu dla Kaspersky Security Center Web Console

Większość przeglądarek nakłada ograniczenie na okres ważności certyfikatu. Okres ważności certyfikatu Kaspersky Security Center Web Console jest ograniczony do 397 dni, aby mógł się zmieścić w nałożonym ograniczeniu. Możesz zastąpić istniejący certyfikat otrzymany z urzędu certyfikacji, ręcznie publikując nowy certyfikat z podpisem własnym. Możesz ponownie opublikować certyfikat Kaspersky Security Center Web Console, który utracił ważność.

Automatyczne ponowne wystawianie certyfikatu dla Kaspersky Security Center Web Console nie jest obsługiwane. Musisz ręcznie wystawić ponownie wygasły certyfikat.

Jeśli już używasz certyfikatu z podpisem własnym, możesz także ponownie opublikować go, aktualizując Kaspersky Security Center Web Console za pośrednictwem standardowej procedury w instalatorze (opcja **Uaktualnij**).

Po otworzeniu Web Console przeglądarka informuje użytkownika, że połączenie z Web Console nie jest prywatne oraz że certyfikat Web Console jest nieprawidłowy. Takie ostrzeżenie pojawia się, ponieważ certyfikat Web Console jest certyfikatem z podpisem własnym i jest automatycznie generowany przez Kaspersky Security Center. Aby usunąć to ostrzeżenie, możesz wykonać jedną z następujących czynności:

- Określ certyfikat niestandardowy podczas jego ponownego wystawiania (opcja zalecana). Utwórz certyfikat, który jest zaufany w Twojej infrastrukturze i spełnia wymagania certyfikatów niestandardowych.
- Dodaj certyfikat Web Console do listy zaufanych certyfikatów przeglądarki po ponownym wystawieniu certyfikatu. Zalecamy korzystanie z tej opcji tylko wtedy, gdy nie można utworzyć certyfikatu niestandardowego.

W celu publikacji nowego certyfikatu po zainstalowaniu Kaspersky Security Center Web Console po raz pierwszy:

1. Uruchom rutynową instalację Kaspersky Security Center Web Console.
2. W kroku **Certyfikat klienta** kreatora instalacji wybierz opcję **Wygeneruj nowy certyfikat**, a następnie kliknij przycisk **Dalej**.
3. Przejdź przez pozostałe kroki kreatora instalacji, aż do zakończenia instalacji.

   Nowy certyfikat dla Kaspersky Security Center Web Console jest publikowany z okresem ważności wynoszącym 397 dni.

W celu ponownego opublikowania certyfikatu Kaspersky Security Center Web Console, który utracił ważność:

1. Na koncie z uprawnieniami administratora uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe.
2. W otwartym oknie kreatora instalacji wybierz język, a następnie kliknij **OK**.
3. W oknie powitalnym wybierz opcję **Wydaj certyfikat ponownie**, a następnie kliknij **Dalej**.
4. W następnym kroku zaczekaj, aż ponowna konfiguracja Kaspersky Security Center Web Console zostanie zakończona, a następnie kliknij **Zakończ**.

   Certyfikat dla Kaspersky Security Center Web Console jest ponownie publikowany dla innego okresu ważności wynoszącego 397 dni.

Jeśli użyjesz Identity and Access Manager, należy również ponownie wystawić wszystkie certyfikaty TLS dla portów, z których korzysta Identity and Access Manager. Kaspersky Security Center Web Console wyświetla powiadomienie po wygaśnięciu certyfikatu. Musisz postępować zgodnie z instrukcjami dotyczącymi powiadomień.

Zastępowanie certyfikatu dla Kaspersky Security Center Web Console

Domyślnie, podczas instalacji Kaspersky Security Center Web Console Server, certyfikat przeglądarki dla aplikacji jest generowany automatycznie. Możesz zastąpić automatycznie wygenerowany certyfikat certyfikatem niestandardowym.

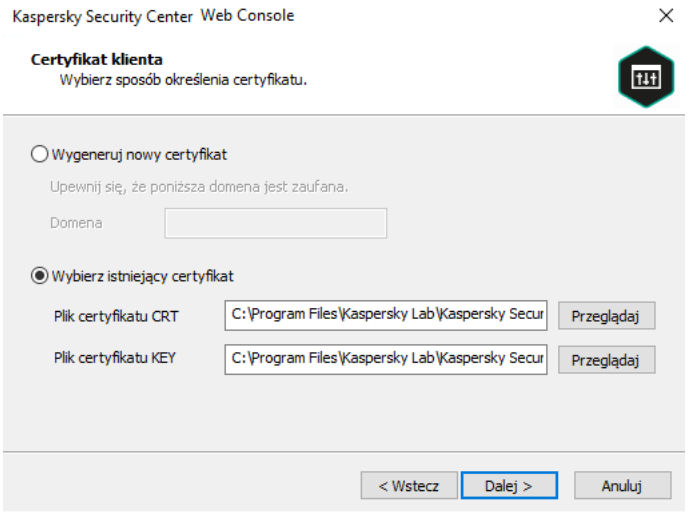
W celu zastąpienia certyfikatu dla Kaspersky Security Center Web Console Server certyfikatem niestandardowym:

1. Na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console Server, uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe z poziomu konta z uprawnieniami administracyjnymi.

   Zostanie uruchomiony kreator instalacji.

2. W pierwszym kroku kreatora wybierz opcję **Aktualizuj**.

3. W kroku **Certyfikat klienta** wybierz opcję **Wybierz istniejący certyfikat** i określ ścieżkę do certyfikatu niestandardowego.



Określanie certyfikatu klienta

4. W ostatnim kroku kreatora kliknij **Modyfikuj**, aby zastosować nowe ustawienia.

5. Po pomyślnym zakończeniu ponownej konfiguracji aplikacji, kliknij przycisk **Zakończ**.

Kaspersky Security Center Web Console działa z określonym certyfikatem.

Określanie certyfikatów dla zaufanych Serwerów administracyjnych w Kaspersky Security Center Web Console

Istniejący certyfikat Serwera administracyjnego jest automatycznie zastępowany nowym przed datą wygaśnięcia certyfikatu. Możesz także zastąpić istniejący certyfikat Serwera administracyjnego innym certyfikatem. Za każdym razem, gdy certyfikat zostanie zmieniony, nowy certyfikat musi zostać określony w ustawieniach Kaspersky Security Center Web Console. W przeciwnym razie Kaspersky Security Center Web Console nie będzie mógł nawiązać połączenia z Serwerem administracyjnym.

W celu określenia nowego certyfikatu dla Serwera administracyjnego:

1. Na urządzeniu, na którym jest zainstalowany Serwer administracyjny, skopiuj plik certyfikatu, na przykład, na urządzenie masowego przechowywania.

   Domyślnie, plik certyfikatu jest przechowywany w następującym folderze:

   - W systemie Windows —%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - W systemie Linux — /var/opt/kaspersky/klnagent_srv/1093/cert/

2. Na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console, umieść plik certyfikatu w folderze lokalnym.

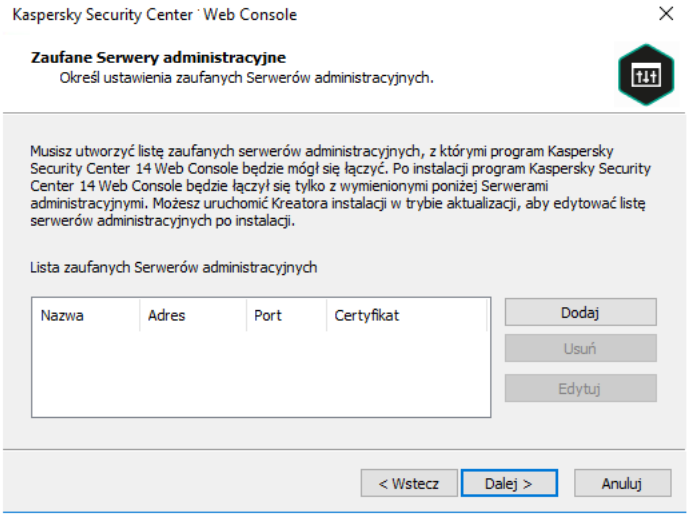
3. Uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe na koncie z uprawnieniami administratora.

   Zostanie uruchomiony kreator instalacji.

4. Na pierwszej stronie kreatora wybierz opcję **Uaktualnij**.

   Postępuj zgodnie z instrukcjami kreatora.

5. Na stronie **Zaufane Serwery administracyjne** wybierz żądany Serwer administracyjny i kliknij przycisk **Edytuj**.



Określanie zaufanych Serwerów administracyjnych

6. W otwartym oknie **Edytuj Serwer administracyjny** kliknij przycisk **Przeglądaj**, określ ścieżkę do pliku nowego certyfikatu, a następnie kliknij przycisk **Aktualizuj**, aby zastosować zmiany.

7. Na stronie **Można rozpocząć modyfikację programu Kaspersky Security Center Web Console** kreatora kliknij przycisk **Uaktualnij**, aby rozpocząć aktualizację.

8. Po pomyślnym zakończeniu ponownej konfiguracji aplikacji, kliknij przycisk **Zakończ**.

9. Zaloguj się do Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console działa z określonym certyfikatem.

Konwersja certyfikatu PFX do formatu PEM

Aby użyć certyfikatu PFX w Kaspersky Security Center Web Console, musisz najpierw przekonwertować go do formatu PEM za pomocą dowolnego wygodnego narzędzia wieloplatformowego opartego na OpenSSL.

Aby przekonwertować certyfikat PFX do formatu PEM w systemie operacyjnym Windows:

1. W wieloplatformowym narzędziu opartym na OpenSSL wykonaj następujące polecenia:

   ```
   openssl pkcs12 -in <nazwa pliku.pfx> -clcerts -nokeys -out server.crt
   openssl pkcs12 -in <nazwa pliku.pfx> -nocerts -nodes -out key.pem
   ```

   W rezultacie otrzymujesz klucz publiczny jako plik .crt i klucz prywatny jako plik .pem chroniony hasłem.

2. Upewnij się, że pliki .crt i .pem są generowane w tym samym folderze, w którym przechowywany jest plik .pfx.

3. Jeśli plik .crt lub .pem zawiera „Atrybuty worka", usuń te atrybuty za pomocą dowolnego wygodnego edytora tekstu, a następnie zapisz plik.

4. Uruchom ponownie usługę Windows.

5. Kaspersky Security Center Web Console nie obsługuje certyfikatów chronionych hasłem. Dlatego uruchom następujące polecenie w wieloplatformowym narzędziu opartym na OpenSSL, aby usunąć hasło z pliku .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Nie używaj tej samej nazwy dla wejściowych i wyjściowych plików .pem.

   W rezultacie nowy plik .pem jest niezaszyfrowany. Nie musisz wpisywać hasła, aby z niego skorzystać.

Pliki .crt i .pem są gotowe do użycia, więc możesz je określić w instalatorze Kaspersky Security Center Web Console.

Aby przekonwertować certyfikat PFX na format PEM w systemie operacyjnym Linux:

1. W wieloplatformowym narzędziu opartym na OpenSSL wykonaj następujące polecenia:

   ```
   openssl pkcs12 -in <nazwapliku.pfx> -clcerts -nokeys | sed -ne '/-BEGIN
   CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   openssl pkcs12 -in <nazwa pliku.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE
   KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Upewnij się, że plik certyfikatu i klucz prywatny są generowane w tym samym katalogu, w którym przechowywany jest plik .pfx.

3. Kaspersky Security Center Web Console nie obsługuje certyfikatów chronionych hasłem. Dlatego uruchom następujące polecenie w wieloplatformowym narzędziu opartym na OpenSSL, aby usunąć hasło z pliku .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Nie używaj tej samej nazwy dla wejściowych i wyjściowych plików .pem.

   W rezultacie nowy plik .pem jest niezaszyfrowany. Nie musisz wpisywać hasła, aby z niego skorzystać.

Pliki .crt i .pem są gotowe do użycia, więc możesz je określić w instalatorze Kaspersky Security Center Web Console.

Migracja z Kaspersky Security Center Windows

Ta sekcja opisuje migrację zarządzanych urządzeń i powiązanych obiektów (zasad, zadań, grup, znaczników i innych obiektów) z Kaspersky Security Center Windows do:

- Kaspersky Next Expert View
- Kaspersky Security Center Linux

Migracja do Kaspersky Next Expert View

Można przeprowadzić migrację z Kaspersky Security Center Web Console do Kaspersky Next Expert View. Następnie uzyskasz dostęp do Serwera administracyjnego i systemu zarządzania bazami danych (DBMS), które są hostowane w infrastrukturze Kaspersky. Nie potrzebujesz fizycznego serwera ani DBMS — oba są utrzymywane przez ekspertów z Kaspersky.

Można przenieść zarządzane urządzenia z systemem operacyjnym Windows, Linux lub macOS pod kontrolę Kaspersky Next Expert View. Jeśli sieć obejmuje hierarchię Serwerów administracyjnych, można ją zachować w Kaspersky Next Expert View. Dodatkowo możesz przenieść:

- Zadania i zasady zarządzanych aplikacji
- Zadania globalne
- Niestandardowe wybory urządzeń
- Strukturę grupy administracyjnej i dołączonych urządzeń
- Znaczniki przypisane do przenoszonych urządzeń

Po zakończeniu migracji można zarządzać urządzeniami za pomocą Kaspersky Next Expert View. Jednocześnie przesłane obiekty są zachowywane, a Agent sieciowy jest ponownie instalowany na wszystkich zarządzanych urządzeniach.

Informacje o sposobie przeprowadzenia migracji oraz listę wymagań wstępnych można znaleźć w *Pomocy Kaspersky Next Expert View*.

Migracja do Kaspersky Next XDR Expert

Postępując zgodnie z tym scenariuszem, możesz przenieść strukturę grupy administracyjnej, dołączone zarządzane urządzenia i inne obiekty grupowe (zasady, zadania, zadania globalne, znaczniki i wybór urządzeń) z Kaspersky Security Center Windows w ramach zarządzania Kaspersky Next XDR Expert.

Ograniczenia:

- Migracja jest możliwa wyłącznie z Kaspersky Security Center 14.2 Windows do Kaspersky Next XDR Expert począwszy od wersji 1.0.
- Możesz wykonać ten scenariusz tylko przy użyciu Kaspersky Security Center Web Console.

Etapy

Scenariusz migracji przebiega etapami:

1. **Wybierz metodę migracji**

   Migracji do Kaspersky Next XDR Expert dokonujesz za pomocą Kreatora migracji. Kroki kreatora migracji zależą od tego, czy Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Next XDR Expert są ułożone w hierarchię:

   - Migracja z użyciem hierarchii Serwerów administracyjnych

     Wybierz tę opcję, jeśli Serwer administracyjny Kaspersky Security Center Windows działa jako serwer pomocniczy w stosunku do Serwera administracyjnego Kaspersky Next XDR Expert. Zarządzasz procesem migracji i przełączasz się pomiędzy Serwerami w konsoli Kaspersky Security Center. Jeśli wolisz tę opcję, możesz ustawić Serwery administracyjne w hierarchię, aby uprościć procedurę migracji. Aby to zrobić, utwórz hierarchię przed rozpoczęciem migracji.

   - Migracja za pomocą pliku eksportu (archiwum ZIP)

     Wybierz tę opcję, jeśli Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Next XDR Expert nie są ułożone w hierarchię. Do zarządzania procesem migracji służą dwie Konsole — instancja dla Kaspersky Security Center Windows i konsoli Kaspersky Security Center. W takim przypadku użyjesz pliku eksportu, który utworzyłeś i pobrałeś podczas eksportu z Kaspersky Security Center Windows i zaimportujesz ten plik do Kaspersky Next XDR Expert.

2. **Eksportowanie danych z Kaspersky Security Center Windows**

   Otwórz Kaspersky Security Center Windows, a następnie uruchom Kreatora migracji.

3. **Import danych do Kaspersky Next XDR Expert**

   Kontynuuj działanie Kreatora migracji, aby zaimportować wyeksportowane dane do Kaspersky Next XDR Expert.

   Jeśli Serwery są ułożone w hierarchię, import rozpoczyna się automatycznie po pomyślnym eksporcie w tym samym kreatorze. Jeśli Serwery nie są ułożone w hierarchię, po przełączeniu się do Kaspersky Next XDR Expert będziesz kontynuować działanie Kreatora migracji.

4. **Wykonaj dodatkowe działania, aby ręcznie przesłać obiekty i ustawienia z Kaspersky Security Center Windows do Kaspersky Next XDR Expert (krok opcjonalny)**

   Możesz także chcieć przenieść obiekty i ustawienia, których nie można przenieść za pomocą Kreatora migracji. Na przykład możesz dodatkowo wykonać następujące czynności:

   - Skonfiguruj zadania globalne Serwera administracyjnego
   - Skonfiguruj Ustawienia zasady Agenta sieciowego
   - Utwórz pakiety instalacyjne aplikacji
   - Utwórz wirtualne Serwery

- Przypisz i skonfiguruj punkty dystrybucji
- Skonfiguruj reguły przenoszenia urządzeń
- Skonfiguruj reguły automatycznego znakowania urządzeń
- Utwórz kategorie aplikacji

5. **Przenieś zaimportowane zarządzane urządzenia do zarządzania przez Kaspersky Next XDR Expert**

   Aby zakończyć migrację, przenieść zaimportowane zarządzane urządzenia do zarządzania przez Kaspersky Next XDR Expert. Można to zrobić przy użyciu jednej z następujących metod:

   - Poprzez zadanie z grupy Kaspersky Security Center Web Console

     Użyj zadania Zmień Serwer administracyjny, aby zmienić Serwer administracyjny na inny w przypadku określonych urządzeń klienckich.

   - Za pomocą narzędzia klmover

     Użyj narzędzia klmover i określ ustawienia połączenia dla nowego Serwera administracyjnego.

   - Poprzez instalację lub ponowną instalację Agenta sieciowego na zarządzanych urządzeniach

     Utwórz nowy pakiet instalacyjny Agenta sieciowego i określ ustawienia połączenia dla nowego Serwera administracyjnego we właściwościach pakietu instalacyjnego. Użyj pakietu instalacyjnego, aby zainstalować Agenta sieciowego na zaimportowanych zarządzanych urządzeniach poprzez zadanie zdalnej instalacji.

     Można także utworzyć autonomiczny pakiet instalacyjny i używać go do lokalnej instalacji Agenta sieciowego.

6. **Zaktualizuj Agenta sieciowego do najnowszej wersji**

   Zalecamy aktualizację Agenta sieciowego do tej samej wersji co konsola Kaspersky Security Center.

7. **Upewnij się, że zarządzane urządzenia są widoczne na nowym Serwerze administracyjnym**

   Na Serwerze administracyjnym Kaspersky Next XDR Expert otwórz listę zarządzanych urządzeń (**Zasoby (urządzenia)** → **Zarządzane urządzenia** i sprawdź wartości w kolumnach **Widoczny**, **Agent sieciowy jest zainstalowany** i **Ostatnie połączenie z Serwerem administracyjnym**.

Inne metody migracji danych

Oprócz Kreatora migracji możesz także przenieść określone zadania i zasady:

- Wyeksportuj zadania z Kaspersky Security Center Windows, a następnie zaimportuj zadania do Kaspersky Next XDR Expert.
- Wyeksportuj zasady z Kaspersky Security Center Windows, a następnie zaimportuj zasady do Kaspersky Next XDR Expert. Powiązane profile zasad są eksportowane i importowane razem z wybranymi zasadami.

Migracja do Kaspersky Security Center Linux

Migrację z Kaspersky Security Center Windows do Kaspersky Security Center Linux można wykonać przy użyciu kopii zapasowej danych Serwera administracyjnego (z narzędziem klbackup) i Kreatora migracji.

Poniższa tabela umożliwia porównanie głównych funkcji i ograniczeń migracji przy użyciu kopii zapasowej danych Serwera administracyjnego i Kreatora migracji, aby zdecydować, które podejście jest bardziej odpowiednie dla Twojej organizacji.

Porównanie podejść migracyjnych

Parametry	Kopia zapasowa danych Serwera administracyjnego	Kreator migracji
Proces migracji	Tworzenie pełnej kopii zapasowej danych Serwera administracyjnego Kaspersky Security Center Windows i przywracanie ich na Serwerze administracyjnym Kaspersky Security Center Linux	Wybieranie i eksportowanie danych Serwera administracyjnego do migracji, importowanie tych danych do Serwera administracyjnego Kaspersky Security Center Linux i przełączanie zarządzanych urządzeń w ramach zarządzania Kaspersky Security Center Linux
Funkcje metody migracji	• Migracja wszystkich danych Serwera administracyjnego • Migracja dowolnej liczby zarządzanych urządzeń • Służy do uzyskania kompletnej kopii danych Serwera administracyjnego Kaspersky Security Center Windows i przesłania ich do Serwera administracyjnego Kaspersky Security Center Linux	• Częściowa migracja danych Serwera administracyjnego • Dostępny jest wybór obiektów do migracji • Grupa lub podgrupa administracyjna podlegająca migracji nie może zawierać więcej niż 10 000 urządzeń • Służy do częściowego przesyłania danych Serwera administracyjnego, obejmujących wyłącznie obiekty grupowe w zakresie migracji; obiekty grupowe spoza zakresu migracji muszą zostać przywrócone ręcznie
Zakres migracji	Pełne przesyłanie danych Serwera administracyjnego z nieograniczoną liczbą zarządzanych urządzeń	• Struktura grupy administracyjnej • Urządzenia zarządzane zawarte w grupach administracyjnych (**nie więcej niż 10 000 urządzeń**) • Znaczniki przypisane do urządzeń klienckich • Globalne zadania Agenta sieciowego i zarządzanych aplikacji (nie dla Serwera administracyjnego) • Zadania grupowe Agenta sieciowego i zarządzanych aplikacji • Licencjonowanie zarządzanych aplikacji • Szablony raportów • Użytkownicy i role • Użytkownicy wewnętrzni i grupy zabezpieczeń • Kategorii aplikacji niestandardowych z zawartością dodaną ręcznie • Niestandardowe wybory urządzeń
Zakres nie podlegający migracji	—	• Zadania globalne Serwera administracyjnego • Wydarzenia zapisane na Serwerze administracyjnym • Repozytorium pakietów dystrybucyjnych aplikacji przeznaczonych do zdalnego zainstalowania • Certyfikatu Serwera administracyjnego • Klucze licencyjne używane przez Serwer administracyjny i zarządzane aplikacje • Wirtualne Serwery administracyjne • Ustawienia zasady Agenta sieciowego • Reguły przenoszenia urządzeń • Reguły automatycznego znakowania urządzeń • Punkty dystrybucji • Ustawienia aplikacji Kaspersky zapisane na Serwerze administracyjnym
Wersje Kaspersky Security Center obsługujące migrację	• Dowolna obsługiwana wersja Kaspersky Security Center Windows • Kaspersky Security Center Linux w wersji 15.2 lub nowszej	• Kaspersky Security Center Windows w wersji 14.2 lub nowszej • Kaspersky Security Center Linux w wersji 15 lub nowszej
Systemy DBMS, pomiędzy którymi można przeprowadzić migrację	• Microsoft SQL Server → MySQL, MariaDB • Microsoft SQL Server → PostgreSQL, Postgres Pro (tylko w przypadku migracji z Kaspersky Security Center Windows w wersji 14.2 lub nowszej z zainstalowaną poprawką do Kaspersky Security Center Linux w wersji 15.3 lub nowszej) • MySQL → MySQL, MariaDB • MariaDB → MySQL, MariaDB • PostgreSQL → PostgreSQL Postgres Pro → Postgres Pro (tylko w przypadku migracji z Kaspersky Security Center Windows w wersji 15.1 lub nowszej do Kaspersky Security Center Linux w wersji 16 lub nowszej)	Migracja pomiędzy obsługiwanymi systemami DBMS bez ograniczeń

Migracja do Kaspersky Security Center Linux przy użyciu kopii zapasowej danych Serwera administracyjnego

Za pomocą kopii zapasowej danych możesz przenieść dane z Serwera administracyjnego Kaspersky Security Center Windows do Kaspersky Security Center Linux. Przed migracją upewnij się, że wymagane funkcje Kaspersky Security Center Windows są obsługiwane w Kaspersky Security Center Linux.

Ograniczenia:

- Migrację można przeprowadzić pomiędzy następującymi systemami DBMS:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- Migracja danych Serwera administracyjnego przechowywanych w bazie danych Microsoft SQL Server, MySQL lub MariaDB do bazy danych MySQL lub MariaDB jest obsługiwana w przypadku migracji z dowolnej obsługiwanej wersji programu Kaspersky Security Center Windows do Kaspersky Security Center Linux w wersji 15.2 lub nowszej.
- Migracja danych Serwera administracyjnego przechowywanych w bazie danych PostgresSQL do bazy danych PostgreSQL lub Postgres Pro jest obsługiwana w przypadku migracji z Kaspersky Security Center Windows w wersji 15.1 lub nowszej do Kaspersky Security Center Linux w wersji 16 lub nowszej.
- Migracja danych Serwera administracyjnego przechowywanych w bazie danych Microsoft SQL Server do bazy danych PostgreSQL lub Postgres Pro jest obsługiwana w przypadku migracji z Kaspersky Security Center Windows w wersji 14.2 lub nowszej do Kaspersky Security Center Linux w wersji 15.3 lub nowszej.

  Aby obsługiwać migrację do PostgreSQL lub Postgres Pro, możesz wykonać jedną z następujących czynności:
  - Zainstaluj poprawkę 15.1.0.20748-pf2 dla Serwera administracyjnego Kaspersky Security Center Windows. Skontaktuj się z pomocą techniczną Kaspersky, aby uzyskać tę poprawkę.
  - Zaktualizuj Kaspersky Security Center Windows do wersji 15.1.0.22239.
- Jeśli używasz MySQL lub MariaDB jako systemu DBMS dla Kaspersky Security Center Windows i Kaspersky Security Center Linux, parametr `lower_case_table_names` musi być taki sam dla bieżącego i nowego systemu DBMS.

  Przed utworzeniem kopii zapasowej danych sprawdź parametr `lower_case_table_names`. Następnie podczas instalacji MySQL lub MariaDB dla Kaspersky Security Center Linux należy ustawić ten parametr na taką samą wartość, jaka została określona dla tego parametru w systemie Windows.

Etapy

Migracja z wykorzystaniem kopii zapasowej danych Serwera administracyjnego przebiega etapami:

1. **Sprawdzenie, czy posiadasz wewnętrzne konto użytkownika administratora, za pomocą którego możesz zalogować się do Serwera administracyjnego**

   Konto administratora będzie wykorzystywane do logowania się do Serwera administracyjnego Kaspersky Security Center Linux. Jeśli nie posiadasz tego konta i jesteś zalogowany tylko na lokalnym koncie systemu Windows lub koncie domenowym, nie będziesz mógł zalogować się do Serwera administracyjnego Kaspersky Security Center Linux po przywróceniu kopii zapasowej. Serwer administracyjny Kaspersky Security Center Linux nie obsługuje logowania przy użyciu lokalnego konta systemu Windows. Zalogowanie się na konto domenowe jest możliwe, ale może wymagać dodatkowej konfiguracji Serwera administracyjnego.

   Jeśli nie posiadasz konta administratora, będziesz musiał je utworzyć po przywróceniu kopii zapasowej, korzystając z narzędzia kladduser.

2. **Tworzenie aktualnej kopii zapasowej danych Serwera administracyjnego Kaspersky Security Center Windows**

   W zależności od typu systemu DBMS używanego w Kaspersky Security Center Windows i Kaspersky Security Center Linux wykonaj jedną z następujących czynności:

   - Aby przeprowadzić migrację MySQL lub MariaDB do MySQL lub MariaDB: utwórz kopię zapasową za pomocą narzędzia klbackup lub zadania tworzenia kopii zapasowej danych na urządzeniu z zainstalowanym Serwerem administracyjnym.
   - W celu migracji PostgresSQL do PostgresSQL i PostgresPro do PostgresPro: utwórz kopię zapasową korzystając z narzędzia klbackup lub zadania tworzenia kopii zapasowej danych na urządzeniu, na którym zainstalowano Serwer administracyjny.
   - W celu migracji Microsoft SQL Server do MySQL lub MariaDB: utwórz kopię zapasową korzystając z narzędzia klbackup, z włączoną opcją **Wykonaj migrację do formatu MySQL/MariaDB**.
   - W celu migracji Microsoft SQL Server do PostgreSQL lub Postgres Pro:

     1. Zwróć się do pomocy technicznej Kaspersky i zainstaluj poprawkę 15.1.0.20748-pf2 dla Serwera administracyjnego, aby umożliwić migrację do PostgreSQL i Postgres Pro.

        Alternatywnie możesz zaktualizować Kaspersky Security Center Windows do wersji 15.1.0.22239.

     2. Utwórz kopię zapasową za pomocą narzędzia klbackup.

        Jeśli uruchamiasz klbackup z wiersza poleceń, użyj flagi `-migrate postgres`.

        Jeśli używasz interfejsu klbackup, włącz opcję **Migruj do formatu Postgres**.

   Po utworzeniu kopii zapasowej odłącz Serwer administracyjny Kaspersky Security Center Windows od sieci.

3. **Przygotowanie nowego urządzenia do instalacji Kaspersky Security Center Linux**

Na tym etapie scenariusza wykonaj następujące czynności:

1. Wybierz nowe urządzenie, na którym chcesz zainstalować Serwer administracyjny. Urządzenie musi spełniać wymagania sprzętowe i programowe. Sprawdź również, czy porty używane na Serwerze administracyjnym są dostępne.

2. Przypisz ten sam adres do nowego urządzenia.

   Nowy Serwer administracyjny może mieć przypisaną nazwę NetBIOS, FQDN i statyczny adres IP. Zależy to od tego, który adres Serwera administracyjnego został ustawiony w pakiecie instalacyjnym Agenta sieciowe w momencie instalacji Agenta sieciowego. Alternatywnie można użyć adresu połączenia, który określa Serwer administracyjny, z którym łączy się Agent sieciowy (możesz uzyskać ten adres na zarządzanych urządzeniach korzystając z narzędzia klnagchk).

4 Instalowanie i konfigurowanie systemu DBMS

Na tym etapie scenariusza wykonaj następujące czynności:

1. Wybierz typ systemu DBMS zapewniający optymalną wydajność. Należy wziąć pod uwagę liczbę urządzeń sieciowych, topologię sieci oraz obciążenie sieci. Możesz wybrać jeden z obsługiwanych DBMS.

2. Zainstaluj system DBMS zgodnie z typem systemu DBMS wybranym podczas tworzenia kopii zapasowej. Informacje o sposobie zainstalowania wybranego systemu DBMS znajdziesz w tym dokumencie.

   > Nowa wersja bazy danych nie może być starsza od obecnej.

3. Skonfiguruj system DBMS do pracy z Kaspersky Security Center Linux.

5 Instalowanie Kaspersky Security Center Linux

Zainstaluj Kaspersky Security Center Linux na nowym urządzeniu.

Wewnętrzne konto użytkownika administratora utworzone podczas instalacji, a także inne obiekty (grupy, zasady, zadania, użytkownicy) utworzone przed przywróceniem danych Serwera administracyjnego z kopii zapasowej zostaną utracone po przywróceniu. Obiekty te zostaną zastąpione obiektami zawartymi w kopii zapasowej.

6 Przywracanie danych Serwera administracyjnego z kopii zapasowej

Na tym etapie scenariusza wykonaj następujące czynności:

1. Przywróć dane Serwera administracyjnego na nowym urządzeniu, korzystając z narzędzia klbackup.

2. Jeśli nie posiadasz wewnętrznego konta użytkownika administratora, na którym zalogowałeś się do Serwera administracyjnego Kaspersky Security Center Windows i używasz lokalnego konta systemu Windows lub konta domenowego, utwórz konto administratora, korzystając z narzędzia kladduser w następujący sposób:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

   gdzie parametr `<password>` spełnia następujące wymagania:

   - Hasło użytkownika nie może mieć mniej niż 8 ani więcej niż 256 znaków.
   - Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
     - Wielkie litery (A-Z)
     - Małe litery (a-z)

- Cyfry (0-9)
- Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7. **Instalacja Kaspersky Security Center Web Console i konfiguracja Serwera administracyjnego**

   Na tym etapie scenariusza wykonaj następujące czynności:

   1. Zainstaluj Kaspersky Security Center Web Console.

      Jeśli Kaspersky Security Center Web Console została zainstalowana wcześniej, zainstaluj ją ponownie z tym samym plikiem odpowiedzi.

      Zaloguj się do Kaspersky Security Center Web Console na koncie użytkownika wewnętrznego administratora.

      Proces inicjalizacji danych trwa zazwyczaj do 15 minut po przywróceniu danych Serwera administracyjnego, lecz czas ten zależy od wydajności sprzętu i rozmiaru danych Serwera administracyjnego. W tym czasie Kaspersky Security Center Web Console może nie nawiązać połączenia i mogą zostać wyświetlone błędy.

   2. Sprawdź działanie głównych funkcji Serwera administracyjnego po zakończeniu inicjalizacji danych w bazie danych. Sprawdź, czy Serwer administracyjny synchronizuje się z zarządzanymi urządzeniami i czy dane Serwera administracyjnego zostały odzyskane.

   3. Przeprowadź przeszukiwanie kontrolerów domeny w celu przywrócenia informacji o strukturze domeny, kontach użytkowników, grupach zabezpieczeń i nazwach DNS urządzeń uwzględnionych w domenach.

   4. W razie konieczności odinstaluj Serwer administracyjny i serwer bazy danych z poprzedniego urządzenia.

      W tej samej sieci nie może być kilku Serwerów administracyjnych z tym samym adresem połączenia i certyfikatem Serwera administracyjnego.

Administrator ma dostęp do danych Serwera administracyjnego i zarządzanych urządzeń, do których dostęp jest możliwy w Kaspersky Security Center Windows, z uwzględnieniem funkcjonalności obsługiwanych w Kaspersky Security Center Linux.

Migracji do Kaspersky Security Center Linux za pomocą Kreatora migracji

Postępując zgodnie z tym scenariuszem, możesz przenieść strukturę grupy administracyjnej, dołączone zarządzane urządzenia i inne obiekty grupowe (profile, zadania, zadania globalne, znaczniki i wybór urządzeń) z Kaspersky Security Center Windows w ramach zarządzania Kaspersky Security Center Linux. Przed migracją upewnij się, że wymagane funkcje Kaspersky Security Center Windows są obsługiwane w Kaspersky Security Center Linux.

Ograniczenia:

- Migracja jest możliwa wyłącznie z Kaspersky Security Center Windows w wersji 14.2 lub nowszej do Kaspersky Security Center Linux w wersji 15 lub nowszej.
- Możesz wykonać ten scenariusz tylko przy użyciu Kaspersky Security Center Web Console.

Etapy

Scenariusz migracji przebiega etapami:

1. **Wybierz metodę migracji**

Migracji do Kaspersky Security Center Linux dokonujesz za pomocą Kreatora migracji. Kroki kreatora migracji zależą od tego, czy Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Security Center Linux są ułożone w hierarchię:

- Migracja z użyciem hierarchii Serwerów administracyjnych

  Wybierz tę opcję, jeśli Serwer administracyjny Kaspersky Security Center Windows działa jako serwer pomocniczy w stosunku do Serwera administracyjnego Kaspersky Security Center Linux. Zarządzasz procesem migracji i przełączasz się między serwerami w jednej instancji Kaspersky Security Center Web Console. Jeśli wolisz tę opcję, możesz ustawić Serwery administracyjne w hierarchię, aby uprościć procedurę migracji. Aby to zrobić, utwórz hierarchię przed rozpoczęciem migracji.

- Migracja za pomocą pliku eksportu (archiwum ZIP)

  Wybierz tę opcję, jeśli Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Security Center Linux nie są ułożone w hierarchię. Procesem migracji zarządzasz za pomocą dwóch instancji Kaspersky Security Center Web Console — instancji dla Kaspersky Security Center Windows i drugiej dla Kaspersky Security Center Linux. W takim przypadku użyjesz pliku eksportu, który utworzyłeś i pobrałeś podczas eksportu z Kaspersky Security Center Windows i zaimportujesz ten plik do Kaspersky Security Center Linux.

2. **Utwórz kopię zapasową certyfikatu i klucza prywatnego Serwera administracyjnego Kaspersky Security Center Windows (krok opcjonalny)**

   Możesz poddać zarządzane urządzenia zarządzaniu przez Serwer administracyjny Kaspersky Security Center Linux poprzez przywrócenie certyfikatu i klucza prywatnego Serwera administracyjnego z kopii zapasowej. W takim przypadku wykonaj kopię zapasową certyfikatu i klucza prywatnego Serwera administracyjnego Kaspersky Security Center Windows. Następnie w etapie 6 przywróć certyfikat i klucz prywatny.

3. **Eksportowanie danych z Kaspersky Security Center Windows**

   Otwórz Kaspersky Security Center Windows, a następnie uruchom Kreatora migracji.

4. **Import danych do Kaspersky Security Center Linux**

   Kontynuuj działanie Kreatora migracji, aby zaimportować wyeksportowane dane do Kaspersky Security Center Linux. Jeśli Serwery są ułożone w hierarchię, import rozpoczyna się automatycznie po pomyślnym eksporcie w tym samym kreatorze. Jeśli Serwery nie są ułożone w hierarchię, po przełączeniu do Kaspersky Security Center Linux będziesz kontynuować działanie Kreatora migracji.

5. **Wykonaj dodatkowe czynności, aby ręcznie przenieść obiekty i ustawienia z Kaspersky Security Center Windows do Kaspersky Security Center Linux (krok opcjonalny)**

   Możesz także chcieć przenieść obiekty i ustawienia, których nie można przenieść za pomocą Kreatora migracji. Na przykład możesz dodatkowo wykonać następujące czynności:

   - Przenieś klucze licencyjne używane przez Serwer administracyjny i zarządzane aplikacje
   - Skonfiguruj zadania globalne Serwera administracyjnego
   - Skonfiguruj Ustawienia zasady Agenta sieciowego
   - Utwórz pakiety instalacyjne aplikacji
   - Utwórz wirtualne Serwery
   - Przypisz i skonfiguruj punkty dystrybucji
   - Skonfiguruj reguły przenoszenia urządzeń

- Skonfiguruj reguły automatycznego znakowania urządzeń
- Utwórz kategorie aplikacji

6. **Przenieś zaimportowane zarządzane urządzenia do zarządzania przez Kaspersky Security Center Linux**

   Aby zakończyć migrację, przenieść zaimportowane zarządzane urządzenia do zarządzania przez Kaspersky Security Center Linux. Można to zrobić przy użyciu jednej z następujących metod:

   - Za pomocą narzędzia klmover

     Użyj narzędzia klmover i określ ustawienia połączenia dla nowego Serwera administracyjnego.

   - Poprzez zadanie *Zmień Serwer administracyjny*

     Utwórz zadanie *Zmień Serwer administracyjny*, określ zaimportowane zarządzane urządzenia, nowy Serwer administracyjny i inne ustawienia zadania. Następnie uruchom zadanie, aby przenieść zarządzane urządzenia pod zarządzanie Serwera administracyjnego Kaspersky Security Center Linux.

   - Poprzez usunięcie (jeśli jest już zainstalowany) i ponowną instalację Agenta sieciowego na zarządzanych urządzeniach

     Utwórz nowy pakiet instalacyjny Agenta sieciowego i określ ustawienia połączenia dla nowego Serwera administracyjnego we właściwościach pakietu instalacyjnego. Usuń Agenta sieciowego na zaimportowanych urządzeniach zarządzanych, a następnie użyj pakietu instalacyjnego, aby zainstalować Agenta sieciowego na zaimportowanych urządzeniach zarządzanych za pomocą zadania instalacji zdalnej. Można także utworzyć autonomiczny pakiet instalacyjny i używać go do lokalnej instalacji Agenta sieciowego. Aby uzyskać więcej informacji, zobacz punkt Przełączanie zarządzanych urządzeń na zarządzane przez Kaspersky Security Center Linux.

   - Poprzez przywrócenie certyfikatu i klucza prywatnego Serwera administracyjnego z kopii zapasowej (tylko w przypadku migracji do Kaspersky Security Center Linux 15.1 lub nowszej wersji)

     Przypisz urządzeniu z Serwerem administracyjnym Kaspersky Security Center Linux ten sam adres sieciowy, co urządzeniu z Serwerem administracyjnym Kaspersky Security Center Windows. Uruchom narzędzie klbackup z parametrem `-cert_only`, aby przywrócić certyfikat oraz klucz prywatny Serwera administracyjnego z kopii zapasowej, którą zapisałeś w etapie 2. W wierszu poleceń wykonaj następujące polecenie: `/opt/kaspersky/ksc64/sbin/klbackup -path <ścieżka do kopii zapasowej certyfikatu Serwera administracyjnego> -restore -cert_only`. Aby uzyskać więcej informacji, zobacz Używanie narzędzia klbackup w celu przełączania zarządzanych urządzeń na zarządzenie przez inny Serwer administracyjny.

7. **Zaktualizuj Agenta sieciowego do najnowszej wersji**

   Zalecamy aktualizację Agenta sieciowego dla systemu Linux do tej samej wersji, co Kaspersky Security Center.

8. **Upewnij się, że zarządzane urządzenia są widoczne na nowym Serwerze administracyjnym**

   Na Serwerze administracyjnym Kaspersky Security Center Linux otwórz listę zarządzanych urządzeń (**Zasoby (urządzenia)** → **Zarządzane urządzenia**) i sprawdź wartości w kolumnach **Widoczny**, **Agent sieciowy jest zainstalowany** i **Ostatnie połączenie z Serwerem administracyjnym**.

Inne metody migracji danych

Oprócz Kreatora migracji możesz także przenieść określone zadania i zasady:

- Wyeksportuj zadania z Kaspersky Security Center Windows, a następnie zaimportuj zadania do Kaspersky Security Center Linux.
- Wyeksportuj określone zasady z Kaspersky Security Center Windows, a następnie zaimportuj zasady do Kaspersky Security Center Linux. Powiązane profile zasad są eksportowane i importowane razem z wybranymi zasadami.

Eksportowanie obiektów grupowych z Kaspersky Security Center Windows

Struktura grupy administracyjnej migracji, dołączone zarządzane urządzenia i inne obiekty grupowe z Kaspersky Security Center Windows do Kaspersky Security Center Linux wymaga uprzedniego wybrania danych do eksportu i utworzenia pliku eksportu. Plik eksportu zawiera informacje o wszystkich obiektach grupowych, których migrację chcesz przeprowadzić. Plik eksportowania zostanie użyty do następnego zaimportowania do konsoli Kaspersky Security Center Linux.

Możesz wyeksportować następujące obiekty:

- Zadania i zasady zarządzanych aplikacji
- Zadania globalne
- Niestandardowe wybory urządzeń
- Strukturę grupy administracyjnej i dołączonych urządzeń
- Znaczniki przypisane do przenoszonych urządzeń

Przed rozpoczęciem eksportu przeczytaj ogólne informacje o migracji do Kaspersky Security Center Linux. Wybierz metodę migracji — używając lub nie używając hierarchii Serwerów administracyjnych Kaspersky Security Center Windows i Kaspersky Security Center Linux.

Aby wyeksportować zarządzane urządzenia i powiązane obiekty grupowe za pomocą kreatora migracji:

1. W zależności od tego, czy Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Security Center Linux są ułożone w hierarchię, wykonaj jedną z następujących czynności:
   - Jeśli Serwery są ułożone w hierarchię, otwórz Kaspersky Security Center Web Console, a następnie przełącz się do Serwera Kaspersky Security Center Windows.
   - Jeśli Serwery nie są ułożone w hierarchię, otwórz Kaspersky Security Center Web Console połączoną z Kaspersky Security Center Windows.
2. W menu głównym przejdź do **Operacje** → **Migracja**.

3. Aby uruchomić kreatora i postępować zgodnie z jego instrukcjami, wybierz miejsce, do którego chcesz przenieść swoje dane i ustawienia.

   - Jeśli chcesz przenieść swoje dane i ustawienia do Kaspersky Security Center Cloud Console, wybierz **Migruj do Kaspersky Security Center Cloud Console**.

   - Jeśli chcesz przenieść swoje dane i ustawienia do Kaspersky Security Center Linux lub Kaspersky Next XDR Expert, wybierz **Migracja do Kaspersky Security Center Linux lub platformy Open Single Management Platform**.

4. Wybierz grupę administracyjną lub podgrupę do wyeksportowania. Upewnij się, że wybrana grupa lub podgrupa administracyjna zawiera nie więcej niż 10 000 urządzeń.

5. Wybierz zarządzane aplikacje, których zadania i zasady zostaną wyeksportowane. Wybierz tylko te aplikacje, które są obsługiwane przez Kaspersky Security Center Linux. Obiekty nieobsługiwanych aplikacji będą nadal eksportowane, ale nie będą działać.

6. Użyj linków po lewej stronie, aby wybrać zadania globalne, wybrane urządzenia i raporty do wyeksportowania. Łącze **Obiekty grupy** umożliwia wykluczenie niestandardowych ról, użytkowników wewnętrznych i grup zabezpieczeń oraz niestandardowych kategorii aplikacji z eksportu.

Zostanie utworzony plik eksportu (archiwum ZIP). W zależności od tego, czy przeprowadzasz migrację z obsługą hierarchii Serwera administracyjnego, plik eksportu jest zapisywany w następujący sposób:

- Jeśli serwery są ułożone w hierarchię, plik eksportu jest zapisywany w folderze tymczasowym na serwerze Kaspersky Security Center Web Console Server.

- Jeśli Serwery nie są ułożone w hierarchię, plik eksportu zostanie pobrany na Twoje urządzenie.

W przypadku migracji z obsługą hierarchii Serwera administracyjnego import rozpoczyna się automatycznie po udanym eksporcie. W przypadku migracji bez obsługi hierarchii Serwera administracyjnego możesz ręcznie zaimportować zapisany plik eksportu do Kaspersky Security Center Linux.

Importowanie pliku eksportowania do Kaspersky Security Center Linux

Aby przesłać informacje o zarządzanych urządzeniach, obiektach i ich ustawieniach, które zostały wyeksportowane z Kaspersky Security Center Windows, musisz zaimportować je do Kaspersky Security Center Linux lub Kaspersky Next XDR Expert.

Aby zaimportować zarządzane urządzenia i powiązane obiekty grupowe za pomocą kreatora migracji:

1. W zależności od tego, czy Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Security Center Linux są ułożone w hierarchię, wykonaj jedną z następujących czynności:

   - Jeśli serwery są ustawione hierarchicznie, po zakończeniu eksportu przejdź do następnego kroku kreatora migracji. Import rozpoczyna się automatycznie po pomyślnym eksporcie w tym kreatorze (patrz krok 2 tej instrukcji).

   - Jeśli serwery nie są ustawione hierarchicznie:

     a. Otwórz program Kaspersky Security Center Web Console połączony z oprogramowaniem Kaspersky Security Center Linux lub Kaspersky Next XDR Expert.

     b. W menu głównym przejdź do **Operacje** → **Migracja**.

     c. Wybierz plik eksportu (archiwum ZIP), który utworzono i pobrano podczas eksportu z Kaspersky Security Center Windows. Rozpocznie się przesyłanie pliku eksportu.

2. Po pomyślnym przesłaniu pliku eksportu możesz kontynuować importowanie. Jeśli chcesz wskazać inny plik eksportu, kliknij łącze **Zmień**, a następnie wybierz żądany plik.

3. Wyświetlana jest cała hierarchia grup administracyjnych Kaspersky Security Center Linux.

   Zaznacz pole wyboru obok docelowej grupy administracyjnej, w której mają zostać przywrócone obiekty wyeksportowanej grupy administracyjnej (zarządzane urządzenia, zasady, zadania i inne obiekty grupowe).

4. Rozpoczyna się import obiektów grupy. Nie będzie można zminimalizować kreatora migracji i wykonać jakichkolwiek równoczesnych działań w trakcie importowania. Zaczekaj, aż ikony odświeżenia (🔄), znajdujące się obok wszystkich elementów na liście obiektów zostaną zastąpione zielonymi znacznikami wyboru (✓), a importowanie zostanie zakończone.

5. Po zakończeniu importowania, wyeksportowana struktura grup administracyjnych, w tym szczegóły urządzeń, pojawi się pod wybraną docelową grupą administracyjną. Jeśli nazwa obiektu, który przywracasz, jest taka sama jak nazwa istniejącego obiektu, do przywracanego obiektu zostanie dodany sufiks przyrostowy.

> Jeżeli w migrowanym zadaniu podane są dane konta, na którym zadanie jest uruchamiane, po zakończeniu importu należy otworzyć zadanie i ponownie wprowadzić hasło.

Jeśli import zakończył się błędem, możesz wykonać jedną z następujących czynności:

- W przypadku migracji z obsługą hierarchii Serwera administracyjnego możesz ponownie rozpocząć importowanie pliku eksportu.

- W przypadku migracji bez obsługi hierarchii Serwera administracyjnego możesz uruchomić Kreator migracji, aby wybrać inny plik eksportu, a następnie zaimportować go ponownie.

Możesz sprawdzić, czy obiekty grupy zawarte w zakresie eksportu zostały pomyślnie zaimportowane do programu Kaspersky Security Center Linux. W tym celu przejdź do sekcji **Zasoby (urządzenia)** i upewnij się, czy zaimportowane obiekty są wyświetlane w odpowiednich podsekcjach.

Zwróć uwagę, że zaimportowane zarządzane urządzenia są wyświetlane w podsekcji **Zarządzane urządzenia**, ale są niewidoczne w sieci, a Agent sieciowy nie jest na nich zainstalowany i uruchomiony (wartość *Nie* w kolumnach **Widoczny**, **Agent sieciowy jest zainstalowany** oraz **Agent sieciowy jest uruchomiony**).

Aby zakończyć migrację, musisz przełączyć zarządzane urządzenia na zarządzanie przez Kaspersky Security Center Linux.

Przełączanie zarządzanych urządzeń na zarządzane przez Kaspersky Security Center Linux

Po pomyślnym zaimportowaniu informacji o zarządzanych urządzeniach, obiektach i ich ustawieniach do Kaspersky Security Center Linux, musisz przełączyć zarządzane urządzenia, aby były zarządzane przez Kaspersky Security Center Linux, aby zakończyć migrację.

Możesz przenieść zarządzane urządzenia do Kaspersky Security Center Linux, korzystając z jednej z następujących metod:

- Użycie narzędzia klmover.
- Użycie zadania *Zmień Serwer administracyjny*.
- Przywracanie certyfikatu i klucza prywatnego Serwera administracyjnego z kopii zapasowej (tylko w przypadku migracji do Kaspersky Security Center Linux 15.1 lub nowszego).

  Aby uzyskać szczegółowe informacje, zapoznaj się z etapem 6 głównego scenariusza migracji.
- Zainstalowanie Agenta sieciowego na zarządzanych urządzeniach za pomocą zadania zdalnej instalacji.

W celu przełączenia zarządzanych urządzeń, aby były zarządzane przez Kaspersky Security Center Linux poprzez zainstalowanie Agenta sieciowego:

1. Usuń Agenta sieciowego na importowanych zarządzanych urządzeniach, które zostaną przełączone pod zarządzanie Kaspersky Security Center Linux.
2. Przełącz się na Serwer administracyjny Kaspersky Security Center Windows.
3. Przejdź do opcji **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**, a następnie otwórz właściwości istniejącego pakietu instalacyjnego Agenta sieciowego.

   Jeżeli na liście pakietów nie ma pakietu instalacyjnego Agenta sieciowego, pobierz nowy.

   Można także utworzyć autonomiczny pakiet instalacyjny i używać go do lokalnej instalacji Agenta sieciowego.
4. Na karcie **Ustawienia** wybierz sekcję **Połączenie**. Określ ustawienia połączenia Serwera administracyjnego Kaspersky Security Center Linux.
5. Utwórz zadanie zdalnej instalacji dla zaimportowanych zarządzanych urządzeń, a następnie określ ponownie skonfigurowany pakiet instalacyjny Agenta sieciowego.

   Możesz zainstalować Agenta sieciowego za pośrednictwem Serwera administracyjnego Kaspersky Security Center Windows lub urządzenia z systemem Windows, które działa jako punkt dystrybucji. Jeśli korzystasz z Serwera administracyjnego, włącz opcję **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**. Jeśli korzystasz z punktu dystrybucji, włącz opcję **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**.
6. Uruchom zadanie zdalnej instalacji.

Po pomyślnym zakończeniu zadania zdalnej instalacji przejdź do Serwera administracyjnego Kaspersky Security Center Linux i upewnij się, że zarządzane urządzenia są widoczne w sieci oraz że Agent sieciowy jest na nich zainstalowany i uruchomiony (wartość *Tak* w kolumnach **Widoczny**, **Agent sieciowy jest zainstalowany** oraz **Agent sieciowy jest uruchomiony**).

Logowanie do Kaspersky Security Center Web Console i wylogowywanie

Możesz zalogować się do Kaspersky Security Center Web Console po zainstalowaniu Serwera administracyjnego i serwera Web Console Server. Musisz znać adres internetowy Serwera administracyjnego oraz numer portu określony podczas instalacji (domyślnie jest to port o numerze 8080). W swojej przeglądarce włącz JavaScript.

Możesz zalogować się do Kaspersky Security Center Web Console przy użyciu następujących metod:

- Za pomocą uwierzytelniania domeny

  Jeśli wybierzesz tę metodę, upewnij się, że przeszukiwanie kontrolera domeny zostało aktywowane, a użytkownicy domeny zostali dodani do Serwera administracyjnego.

- Określając nazwę i hasło użytkownika domeny
- Określając nazwę użytkownika i hasło administratora

Konto użytkownika, za pomocą którego chcesz zalogować się do Kaspersky Security Center Web Console musi mieć przypisaną rolę. Przed zalogowaniem upewnij się, że domena lub konto użytkownika wewnętrznego mają przypisaną rolę. W przeciwnym razie wystąpi błąd logowania.

Logowanie przy użyciu uwierzytelniania domeny

W celu zalogowania się do Kaspersky Security Center Web Console przy użyciu uwierzytelniania domeny:

1. W przeglądarce przejdź do https://<adres Kaspersky Security Center Web Console>:<numer portu>

   Zostanie wyświetlona strona logowania.

2. Jeśli dodałeś kilka zaufanych serwerów, na liście Serwerów administracyjnych wybierz Serwer administracyjny, z którym chcesz nawiązać połączenie.

   Jeśli dodano tylko jeden Serwer administracyjny, lista Serwery administracyjne nie jest wyświetlana.

3. Wykonaj jedną z poniższych czynności:

   - Kliknij przycisk **Użyj uwierzytelniania domeny**.
   - Jeżeli jeden lub więcej wirtualnych Serwerów administracyjnych jest utworzonych na Serwerze i chcesz zalogować się do Serwera wirtualnego przy użyciu uwierzytelniania domeny:

     a. Kliknij **Pokaż opcje serwera wirtualnego**.

     b. Wpisz nazwę wirtualnego Serwera administracyjnego określoną podczas tworzenia wirtualnego Serwera.

     c. Kliknij przycisk **Użyj uwierzytelniania domeny**.

4. Jeśli na Twoim koncie włączona jest weryfikacja dwuetapowa, podaj kod bezpieczeństwa wygenerowany przez aplikację uwierzytelniającą na urządzeniu mobilnym.

   Jeśli to konieczne, możesz powrócić do strony logowania.

Po zalogowaniu zostanie wyświetlony pulpit nawigacyjny zawierający język i motyw, których ostatnio używano. Możesz poruszać się po konsoli Kaspersky Security Center Web Console i użyć jej do pracy z Kaspersky Security Center.

Logowanie poprzez podanie nazwy użytkownika i hasła administratora

W celu zalogowania się do Kaspersky Security Center Web Console poprzez podanie nazwy użytkownika i hasła administratora:

1. W przeglądarce przejdź do https://`<adres Kaspersky Security Center Web Console>:<numer portu>`

   Zostanie wyświetlona strona logowania.

2. Jeśli dodałeś kilka zaufanych serwerów, na liście Serwerów administracyjnych wybierz Serwer administracyjny, z którym chcesz nawiązać połączenie.

   Jeśli dodano tylko jeden Serwer administracyjny, lista Serwery administracyjne nie jest wyświetlana.

3. Wykonaj jedną z poniższych czynności:

   - Aby zalogować się do Serwera administracyjnego przy użyciu konta użytkownika domeny:

     a. Poprzez określenie nazwy użytkownika i hasła użytkownika domeny.

     Nazwę użytkownika domeny możesz wprowadzić w jednym z następujących formatów:

     - `Nazwa użytkownika @ dns.domena`
     - `NTDOMAIN\Nazwa użytkownika`

     b. Kliknij przycisk **Zaloguj się**.

     Zanim zalogujesz się na konto użytkownika domeny, przeszukaj kontroler domeny, aby uzyskać listę użytkowników domeny.

   - W celu zalogowania się do Serwera administracyjnego:

     a. Wpisz nazwę użytkownika i hasła lokalnego administratora.

     b. Kliknij przycisk **Zaloguj się**.

   - Jeżeli jeden lub więcej wirtualnych Serwerów administracyjnych jest utworzonych na Serwerze i chcesz zalogować się do Serwera wirtualnego:

     a. Kliknij **Pokaż opcje serwera wirtualnego**.

     b. Wpisz nazwę wirtualnego Serwera administracyjnego określoną podczas tworzenia wirtualnego Serwera.

c. Wprowadź nazwę użytkownika i hasło administratora, który ma uprawnienia na wirtualnym Serwerze administracyjnym.

d. Kliknij przycisk **Zaloguj się**.

4. Jeśli na Twoim koncie włączona jest weryfikacja dwuetapowa, podaj kod bezpieczeństwa wygenerowany przez aplikację uwierzytelniającą na urządzeniu mobilnym.

   Jeśli to konieczne, możesz powrócić do strony logowania.

5. Jeśli dla Twojego konta włączona jest funkcja wymuszonej zmiany hasła lub Twoje hasło wygasło, zostanie wyświetlone okno dialogowe zmiany hasła. Ustaw nowe hasło, aby zalogować się do Kaspersky Security Center Web Console.

Po zalogowaniu zostanie wyświetlony pulpit nawigacyjny zawierający język i motyw, których ostatnio używano. Możesz poruszać się po konsoli Kaspersky Security Center Web Console i użyć jej do pracy z Kaspersky Security Center.

Wylogowanie

W celu wylogowania się z Kaspersky Security Center Web Console:

W menu głównym przejdź do ustawień konta, a następnie wybierz **Wyloguj się**.

Konsola Kaspersky Security Center Web Console zostanie zamknięta i zostanie wyświetlona strona logowania.

Identity and Access Manager w Kaspersky Security Center Web Console

Ta sekcja zawiera informacje o Identity and Access Manager (nazywanym również IAM).

Informacje o Identity and Access Manager

Identity and Access Manager (nazywany również IAM) to komponent Kaspersky Security Center Web Console, który umożliwia korzystanie z logowania jednokrotnego (SSO) między konsolą Kaspersky Security Center Web Console a interfejsem webowym Kaspersky Industrial CyberSecurity for Networks. IAM korzysta z protokołu OAuth 2.0, aby zapewnić autoryzację Kaspersky Industrial CyberSecurity for Networks w Kaspersky Security Center Web Console.

W tym przypadku Kaspersky Industrial CyberSecurity for Networks, do którego uzyskujesz dostęp za pośrednictwem konsoli Kaspersky Security Center Web Console, jest określany jako *serwer zasobów*, a konsola Kaspersky Security Center Web Console i interfejs webowy Kaspersky Industrial CyberSecurity for Networks są określane jako klienty *OAuth 2.0*. Serwer zasobów to program, który współpracuje z wieloma użytkownikami i wymaga autoryzacji. Klient używa *tokena* do autoryzacji na serwerze zasobów. Token to unikatowa sekwencja bajtów. Po wygaśnięciu tokena jest on automatycznie ponownie wystawiany. IAM działa jako jeden serwer autoryzacji dla wielu klientów OAuth 2.0.

Możesz zainstalować IAM podczas instalacji Kaspersky Security Center Web Console. Możesz włączyć ją później w dowolnym momencie w ustawieniach Kaspersky Security Center Web Console. Jeśli Kaspersky Industrial CyberSecurity Server lub interfejs webowy Kaspersky Industrial CyberSecurity jest zainstalowany na urządzeniu, który jest zarządzany przez ten sam Serwer administracyjny, IAM wykryje ten program i wyświetli powiadomienie w konsoli Kaspersky Security Center Web Console informujące o tym fakcie. Możesz zarejestrować Kaspersky Industrial CyberSecurity for Networks, a później używać SSO zarówno dla konsoli Kaspersky Security Center Web Console, jak i interfejsu webowego Kaspersky Industrial CyberSecurity for Networks.

Jeśli wylogujesz się z konsoli Kaspersky Security Center Web Console, Twoja sesja w interfejsie webowym Kaspersky Industrial CyberSecurity for Networks zostanie zakończona i będziesz musiał ponownie zalogować się do Kaspersky Security Center Web Console.

Włączanie Identity and Access Manager: scenariusz

Wymagania wstępne

Przed rozpoczęciem upewnij się, że masz dostęp do Kaspersky Industrial CyberSecurity for Networks w wersji 3.1 lub nowszej.

Etapy

Włączenie Identity and Access Manager (zwanego również IAM) przebiega etapami:

1. **Sprawdzanie niezbędnych portów**

   Upewnij się, że porty 3333, 4004 i 4444 są otwarte na urządzeniu, na którym zainstalowano Kaspersky Security Center Web Console. Te porty są potrzebne do korzystania z protokołu OAuth 2.0. Jeśli chcesz, możesz zmienić domyślne numery portów w oknie ustawień Kaspersky Security Center Web Console.

   Oprócz portów 3333, 4004 i 4444, Kaspersky Security Center Web Console używa również portów 4445, 2444 i 2445 do różnych celów.

2. **Instalowanie Identity and Access Manager**

   Podczas instalacji konsoli Kaspersky Security Center Web Console określ, że chcesz zainstalować Identity and Access Manager. Jeśli tego nie zrobiono, uruchom ponownie kreatora instalacji Kaspersky Security Center Web Console.

3. **Konfigurowanie Identity and Access Manager**

   W oknie ustawień Kaspersky Security Center Web Console upewnij się, że przycisk przełącznika **Zarządzanie tożsamością i dostępem (IAM)** jest włączony. Określ również nazwę DNS urządzenia, na którym zainstalowano Kaspersky Security Center Web Console: aplikacje klienckie nawiążą połączenie z tym urządzeniem.

4. **Określanie ustawień tokena**

   W oknie ustawień Kaspersky Security Center Web Console określ czas życia tokenów i limit czasu autoryzacji, które będą używane przez Identity and Access Manager. Możesz użyć wartości domyślnych lub możesz określić własne wartości zgodnie z własnymi potrzebami.

5. **Przyznawanie certyfikatów**

   Jeśli wolisz korzystać z certyfikatów generowanych przez Serwer administracyjny, to w oknie ustawień Kaspersky Security Center Web Console pobierz certyfikaty główne dla portów używanych przez IAM i roześlij je na stacje robocze użytkowników Kaspersky Security Center Web Console. W przeciwnym razie przeglądarki użytkowników będą wyświetlać komunikaty o błędach podczas próby nawiązania połączenia z konsolą Kaspersky Security Center Web Console.

6. **Rejestrowanie interfejsów webowych Kaspersky Industrial CyberSecurity for Networks Servers i Kaspersky Industrial CyberSecurity for Networks**

   Po zainstalowaniu IAM, konsola Kaspersky Security Center Web Console wyświetla komunikat informujący, że serwer Industrial CyberSecurity for Networks Server (lub kilka serwerów) oraz jeden lub więcej interfejsów webowych Kaspersky Industrial CyberSecurity for Networks czekają na rejestrację. Kliknij tę wiadomość, aby zarejestrować Kaspersky Industrial CyberSecurity for Networks Server (lub kilka serwerów) oraz interfejs webowy (lub kilka interfejsów webowych).

Wyniki

Po zakończeniu tego scenariusza będzie można użyć logowania jednokrotnego i IAM dla Kaspersky Industrial CyberSecurity for Networks i Kaspersky Security Center Web Console.

Konfigurowanie Identity and Access Manager w Kaspersky Security Center Web Console

W celu skonfigurowania Identity and Access Manager zgodnie z własnymi potrzebami:

1. W menu głównym przejdź do **Ustawienia** → **Zarządzanie tożsamością i dostępem**.
2. W sekcji **Zarządzanie tożsamością i dostępem** upewnij się, że Identity and Access Manager jest włączony.
3. Kliknij odnośnik **Ustawienia**, dostępny w wierszu **Nazwa sieciowa urządzenia Zarządzania tożsamością i dostępem**.
4. Podaj nazwę DNS urządzenia, na którym zainstalowałeś Identity and Access Manager. Aplikacje klienckie będą nawiązywać połączenie z tym urządzeniem.
5. Jeśli chcesz, zmień domyślne ustawienia tokena, ustawienia certyfikatu oraz numery portów, klikając odnośnik **Ustawienia** w odpowiedniej grupie ustawień.

Identity and Access Manager jest włączony i działa zgodnie z Twoimi potrzebami.

Rejestrowanie interfejsu aplikacji Kaspersky Industrial CyberSecurity for Networks w Kaspersky Security Center Web Console

Aby rozpocząć pracę z aplikacją Kaspersky Industrial CyberSecurity for Networks za pośrednictwem konsoli Kaspersky Security Center Web Console, musisz najpierw zarejestrować ją w konsoli Kaspersky Security Center Web Console.

W celu zarejestrowania aplikacji Kaspersky Industrial CyberSecurity for Networks:

1. Upewnij się, że wykonano następujące czynności:

   - Pobrano i zainstalowano wtyczkę webową Kaspersky Industrial CyberSecurity for Networks.

     Możesz to jednak zrobić później, czekając na synchronizację Kaspersky Industrial CyberSecurity for Networks Server z Serwerem administracyjnym.

   - Ukończyłeś scenariusz przygotowania do użycia technologii jednokrotnego logowania (SSO).

   - Niezbędne ustawienia w interfejsie webowym Kaspersky Industrial CyberSecurity for Networks są określone na stronie Kaspersky Security Center. Aby uzyskać szczegółowe informacje, zapoznaj się z pomocą online do Kaspersky Industrial CyberSecurity for Networks.

   - Jesteś zalogowany(-a) w Kaspersky Security Center Web Console na koncie administratora.

   - IAM został skonfigurowany.

2. Przenieś urządzenie, na którym zainstalowano Kaspersky Industrial CyberSecurity for Networks Server, z grupy Urządzenia nieprzypisane do grupy Zarządzane urządzenia:

   a. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Urządzenia nieprzypisane**.

   b. Zaznacz pole wyboru obok urządzenia, na którym jest zainstalowany Kaspersky Industrial CyberSecurity for Networks Server.

   c. Kliknij przycisk **Przenieś do grupy**.

   d. W hierarchii grup administracyjnych zaznacz pole wyboru obok grupy Zarządzane urządzenia.

   e. Kliknij przycisk **Przenieś**.

3. Przejdź do właściwości urządzenia, na którym jest zainstalowany Kaspersky Industrial CyberSecurity for Networks Server.

4. Na stronie właściwości urządzenia, w sekcji **Ogólne** wybierz opcję **Nie odłączaj od Serwera administracyjnego**, a następnie kliknij przycisk **Zapisz**.

5. W oknie właściwości urządzenia wybierz sekcję **Aplikacje**.

6. W sekcji **Aplikacje** wybierz Kaspersky Network Agent.

7. Jeśli aktualny stan aplikacji to *Zatrzymana*, poczekaj, aż zmieni się na *Uruchomiona*.

   Ten proces trwa do 15 minut. Jeśli nie zainstalowałeś jeszcze wtyczki internetowej Kaspersky Industrial CyberSecurity for Networks, możesz to zrobić teraz, podczas oczekiwania.

8. W menu głównym przejdź do **Ustawienia → Zarządzanie tożsamością i dostępem**.

   W polu **Prośby o rejestrację** zostanie wyświetlone jedno oczekujące żądanie.

9. Kliknij odnośnik **Ustawienia** link polem **Prośby o rejestrację**.

10. Na otwartej liście zarejestrowanych klientów zaznacz pole obok nazwy serwera Kaspersky Industrial CyberSecurity for Networks, który ma stan *Oczekuje*, a następnie kliknij przycisk **Zatwierdź**.

    Jeśli nie chcesz rejestrować Kaspersky Industrial CyberSecurity for Networks Server, możesz kliknąć przycisk Odrzuć i wrócić do tej listy później.

    Po kliknięciu przycisku **Zatwierdź**, stan zmieni się na *Zatwierdzony*, a następnie na *Gotowy*. Jeśli stan się nie zmieni, możesz kliknąć przycisk Odśwież.

11. Zamknij listę zarejestrowanych klientów i upewnij się, że wartość w polu **Zarejestrowani klienci** wzrosła.

12. W celu dodania widżetu Kaspersky Industrial CyberSecurity for Networks na pulpicie nawigacyjnym:

    a. W menu głównym przejdź do **Monitorowanie i raportowanie → Pulpit nawigacyjny**.

    b. Na pulpicie nawigacyjnym kliknij przycisk **Dodaj lub przywróć widżet sieciowy**.

    c. W otwartym menu widżetu wybierz **Inne**.

    d. Wybierz widżet Kaspersky Industrial CyberSecurity for Networks.

    Możesz teraz przejść do interfejsu webowego Kaspersky Industrial CyberSecurity for Networks, korzystając z odnośnika w widżecie.

Po zakończeniu procedury rejestracji, nowy przycisk, **Kaspersky Security Center**, pojawia się na stronie logowania interfejsu webowego Kaspersky Industrial CyberSecurity for Networks. Możesz kliknąć ten przycisk, aby zalogować się do interfejsu webowego Kaspersky Industrial CyberSecurity for Networks przy użyciu danych uwierzytelniających Kaspersky Security Center.

Czas życia tokenów i limit czasu autoryzacji dla Identity and Access Manager

Podczas konfigurowania Identity and Access Manager (zwany również IAM) należy określić ustawienia okresu istnienia tokena i limitu czasu autoryzacji. Ustawienia domyślne mają odzwierciedlać zarówno standardy bezpieczeństwa, jak i obciążenie serwera. Jednakże możesz zmienić te ustawienia zgodnie z zasadami Twojej organizacji.

IAM automatycznie ponownie wystawiają token, gdy zbliża się jego ważność.

Poniższa tabela zawiera domyślne ustawienia okresu istnienia tokena.

Ustawienia czasu życia tokena

Token	Domyślna żywotność (w sekundach)	Opis
Token tożsamości (id_token)	86400	Token tożsamości używany przez klienta OAuth 2.0 (czyli Kaspersky Security Center Web Console lub Kaspersky Industrial CyberSecurity Console). IAM wysyła token identyfikatora zawierający informacje o użytkowniku (czyli profil użytkownika) do klienta.
Token dostępu (access_token)	86400	Token dostępu używany przez klienta OAuth 2.0 do uzyskiwania dostępu do serwera zasobów w imieniu właściciela zasobu zidentyfikowanego przez IAM.
Token odświeżania (refresh_token)	172800	Klient OAuth 2.0 używa tego tokena do ponownego wystawiania tokena tożsamości i tokena dostępu.

Poniższa tabela zawiera listę limitów czasu dla auth_code i login_consent_request.

Ustawienia limitu czasu autoryzacji

Ustawienie	Domyślny limit czasu (w sekundach)	Opis
Kod autoryzacji (auth_code)	3600	Limit czasu wymiany kodu na token. Klient OAuth 2.0 wysyła ten kod do serwera zasobów i otrzymuje w zamian token dostępu.
Przekroczono limit czasu żądania zgody na logowanie (login_consent_request)	3600	Limit czasu na delegowanie uprawnień użytkownika do klienta OAuth 2.0.

Aby uzyskać więcej informacji o tokenach, zajrzyj na stronę internetową OAuth.

Aby skonfigurować limit czasu dla klientów, u których nie wykryto żadnej aktywności myszy lub klawiatury:

1. W folderze instalacyjnym Kaspersky Security Center Web Console znajdź i otwórz plik config.json. Plik zawiera parametry umożliwiające konfigurację limitu czasu dla bezczynnych klientów.

2. Użyj parametru `clientIdleTimeout`, aby określić czas (w ms), po którym na nieaktywnym kliencie wyświetli się okno ostrzegawcze.

3. Użyj parametru `clientLogoutTimeout`, aby określić czas (w ms), po którym autoryzacja IAM dla nieaktywnego klienta zostanie zakończona. Odliczanie `clientLogoutTimeout` jest sekwencyjne po odliczaniu `clientIdleTimeout`.

Pobieranie i dystrybucja certyfikatów IAM

Domyślnie, Identity and Access Manager używa certyfikatów wygenerowanych przez Serwer administracyjny w celu przyznania przeglądarkom dostępu do Kaspersky Security Center Web Console. Jeśli jednak chcesz, możesz użyć niestandardowych certyfikatów. Niezależnie od używanego certyfikatu, upewnij się, że wszystkie stacje robocze, z których użytkownicy Kaspersky Security Center Web Console uzyskują dostęp do Kaspersky Security Center Web Console, ufają temu certyfikatowi.

W celu pobrania i rozpowszechniania certyfikatów:

1. W menu głównym przejdź do **Ustawienia** → **Zarządzanie tożsamością i dostępem**.
2. Dla każdego certyfikatu kliknij odnośnik **Ustawienia** w odpowiedniej grupie ustawień, a następnie wykonaj jedną z następujących czynności:
   - Jeśli chcesz użyć certyfikatu wygenerowanego przez serwer administracyjny podczas instalacji Kaspersky Security Center Web Console:
     1. Wybierz **Certyfikat wygenerowany przez Serwer administracyjny** w otwartym oknie właściwości certyfikatu.
     2. Kliknij przycisk **Pobierz**, aby pobrać certyfikat.
     3. Roześlij pobrany certyfikat na wszystkie stacje robocze, z których użytkownicy Kaspersky Security Center Web Console uzyskują dostęp do Kaspersky Security Center Web Console.
   - Jeśli masz certyfikat, którego chcesz użyć:
     1. Wybierz **Niestandardowy certyfikat TLS** w otwartym oknie właściwości certyfikatu.
     2. Wybierz plik certyfikatu i klucz prywatny.
     3. Kliknij przycisk **OK**.
     4. Roześlij certyfikat do wszystkich stacji roboczych, z których użytkownicy uzyskują dostęp do Kaspersky Security Center Web Console lub Kaspersky Industrial CyberSecurity Console.

Certyfikaty zapewniają użytkownikom dostęp do Kaspersky Security Center Web Console i Kaspersky Industrial CyberSecurity Console.

Musisz ponownie opublikować wszystkie certyfikaty na czas. Certyfikaty wygenerowane przez Serwer administracyjny muszą zostać ponownie wygenerowane ręcznie. Certyfikaty wygenerowane przez instalator Kaspersky Security Center Web Console muszą zostać ponownie wygenerowane przy użyciu instalatora.

Wyłączanie Identity and Access Manager

Jeśli chcesz, możesz wyłączyć Identity and Access Manager (zwany rónież IAM).

W celu wyłączenia IAM:

1. W menu głównym przejdź do sekcji **Ustawienia** → **Integracja**.
2. W sekcji **Zarządzanie tożsamością i dostępem** ustaw przycisk przełączający **Zarządzanie tożsamością i dostępem** w pozycji wyłączonej.

IAM możesz włączyć w dowolnym momencie później.

Jeżeli aktualizujesz Kaspersky Security Center Web Console za pomocą instalatora i określisz, że nie chcesz instalować IAM, wówczas Kaspersky Security Center Web Console zostanie zaktualizowany, a usługa IAM nie zostanie zainstalowana. Wszystkie informacje dotyczące integracji z Kaspersky Industrial CyberSecurity for Networks zostaną usunięte z urządzenia, a także pliki konfiguracyjne IAM i pliki dziennika.

Konfigurowanie uwierzytelniania domeny przy użyciu protokołów NTLM i Kerberos

Kaspersky Security Center 15.1 umożliwia korzystanie z uwierzytelniania domeny w OpenAPI przy użyciu protokołów NTLM i Kerberos. Użycie uwierzytelniania domeny umożliwia użytkownikowi systemu Windows włączenie bezpiecznego uwierzytelniania w konsoli Kaspersky Security Center Web Console bez konieczności ponownego wprowadzania hasła w sieci firmowej (technologia pojedynczego logowania).

Uwierzytelnianie domeny w OpenAPI przez protokół Kerberos ma następujące ograniczenia:

- Użytkownik Kaspersky Security Center Web Console musi zostać uwierzytelniony w Active Directory przy użyciu protokołu Kerberos. Użytkownik musi mieć ważny bilet uprawniający do przyznania biletu Kerberos (nazywany również TGT). TGT jest wystawiany automatycznie podczas uwierzytelniania w domenie.
- Musisz skonfigurować uwierzytelnianie Kerberos w przeglądarce. Aby uzyskać szczegółowe informacje, zapoznaj się z dokumentacją używanej przeglądarki.

Jeśli chcesz korzystać z uwierzytelniania domeny przy użyciu protokołów Kerberos, Twoja sieć musi spełniać następujące warunki:

- Serwer administracyjny musi być uruchamiany pod nazwą konta domeny.
- Kaspersky Security Center Web Console Server musi być zainstalowany na tym samym urządzeniu, na którym jest zainstalowany Serwer administracyjny.
- Musisz określić następujące nazwy główne usługi (SPN) dla konta Serwera administracyjnego:
  - "http/<server.fqnd.name>"
  - "http/<server>"

  <serwer> to nazwa sieciowa urządzenia z Serwerem administracyjnym, a <serwer.fqnd.nazwa> to nazwa FQDN urządzenia z Serwerem administracyjnym.

- Podczas nawiązywania połączenia z Konsolą administracyjną lub konsolą Kaspersky Security Center Web Console, adres Serwera administracyjnego musi być dokładnie taki sam, jak adres, dla którego zarejestrowana jest nazwa główna usługi (SPN). Możesz określić <server.fqnd.name> lub <server>.

- Aby zalogować się bez hasła, proces przeglądarki, w którym konsola Kaspersky Security Center Web Console jest otwarta jako przeglądarka, musi działać na koncie domeny.

Protokoły Kerberos i NTLM są obsługiwane tylko w interfejsie OpenAPI dla Kaspersky Security Center 15.1. Nie są obsługiwane w OpenAPI dla Kaspersky Security Center Linux.

Konfigurowanie Serwera administracyjnego

W tej sekcji opisano proces konfiguracji i właściwości Serwera administracyjnego.

Konfigurowanie połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym

W celu określenia portów połączenia Serwera administracyjnego:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Porty połączenia**.

   Aplikacja wyświetli główne ustawienia połączenia wybranego serwera.

Kaspersky Security Center Web Console jest połączona z Serwerem administracyjnym poprzez port SSL TCP 13299. Ten sam port może być używany przez obiekty automatyzacji klakaut.

Port TCP o numerze 14000 może być używany do podłączania Kaspersky Security Center Web Console, punktów dystrybucji, podrzędnych Serwerów administracyjnych i obiektów narzędzia klakaut, a także do pobierania danych z urządzeń klienckich.

Zazwyczaj port TCP o numerze 13000 dla protokołu SSL może być używany tylko przez Agenta sieciowego, podrzędny Serwer administracyjny i główny Serwer administracyjny w DMZ. W niektórych przypadkach konieczne może być podłączenie Kaspersky Security Center Web Console za pośrednictwem portu SSL o numerze 13000:

- Jeśli pojedynczy port SSL będzie używany dla Kaspersky Security Center Web Console i do innych działań (pobierania danych z urządzeń klienckich, podłączania punktów dystrybucji lub podłączania podrzędnych Serwerów administracyjnych).

- Jeśli obiekt narzędzia klakaut nie jest podłączany bezpośrednio do Serwera administracyjnego, ale za pośrednictwem punktu dystrybucji w DMZ.

Konfigurowanie rejestrowania zdarzeń połączenia serwera administracyjnego

Historia połączeń i prób nawiązania połączenia z Serwerem administracyjnym podczas jego działania może zostać zapisana w pliku raportu. Informacje w pliku umożliwiają śledzenie nie tylko połączeń w obrębie infrastruktury sieci, ale także nieautoryzowanych prób uzyskania dostępu do serwera.

W celu zapisania zdarzeń nawiązania połączenia z Serwerem administracyjnym:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Porty połączenia**.

3. Włącz opcję **Zapisuj zdarzenia połączenia z Serwerem administracyjnym**.

   Wszystkie dalsze zdarzenia przychodzących połączeń z Serwerem administracyjnym, wyniki autoryzacji i błędy SSL zostaną zapisane do pliku %ProgramData%\KasperskyLab\adminkit\logs\SC.syslog.

Konfigurowanie ustawień dostępu do Internetu dla Serwera administracyjnego

Należy skonfigurować dostęp do Internetu w taki sposób, aby korzystać z Kaspersky Security Network i pobierać aktualizacje antywirusowych baz danych dla Kaspersky Security Center i zarządzanych aplikacji Kaspersky.

Aby określić ustawienia dostępu do Internetu dla Serwera administracyjnego:

1. W menu aplikacji kliknij ikonę ustawień ( ) obok nazwy Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Konfiguracja dostępu do internetu**.

3. Włącz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest włączona, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

   - **Adres**

     Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

   - **Numer portu**

     Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

   - **Pomiń serwer proxy dla adresów lokalnych**

     Żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

- **Uwierzytelnianie na serwerze proxy**

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

- **Nazwa użytkownika**

  Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

- **Hasło**

  Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

  Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

Dostęp do Internetu można również skonfigurować za pomocą kreatora wstępnej konfiguracji.

Określanie maksymalnej liczby zdarzeń w repozytorium zdarzeń

W sekcji **Repozytorium zdarzeń** okna właściwości Serwera administracyjnego możesz zmodyfikować ustawienia przechowywania zdarzeń w bazie danych Serwera administracyjnego, ograniczając liczbę wpisów zdarzeń i czas przechowywania wpisów. Jeśli określisz maksymalną liczbę zdarzeń, aplikacja oblicza przybliżoną ilość miejsca przechowywania, wymaganą dla określonej liczby. Możesz użyć tego przybliżonego obliczenia do oszacowania wystarczającej ilości wolnego miejsca na dysku, aby uniknąć przepełnienia bazy danych. Domyślna pojemność bazy danych Serwera administracyjnego wynosi 400 000 zdarzeń. Maksymalną dozwoloną pojemnością bazy danych jest 45 milionów zdarzeń.

Aplikacja sprawdza bazę danych co 10 minut. Jeśli liczba zdarzeń osiągnie określoną maksymalną wartość plus 10 000, aplikacja usunie najstarsze zdarzenia, tak aby pozostała tylko określona maksymalna liczba zdarzeń.

Jeśli Serwer administracyjny usuwa starsze zdarzenia, nie może zapisywać nowych zdarzeń do bazy danych. W tym czasie informacje o odrzuconych zdarzeniach są zapisywane w dzienniku zdarzeń aplikacji Kaspersky. Nowe zdarzenia zostają zakolejkowane, a następnie zapisane do bazy danych po zakończeniu operacji usuwania.

Aby ograniczyć liczbę zdarzeń, które mogą być przechowywane w repozytorium zdarzeń na Serwerze administracyjnym:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Repozytorium zdarzeń**. Określ maksymalną liczbę zdarzeń przechowywanych w bazie danych.

3. Kliknij przycisk **Zapisz**.

Dodatkowo możesz wykonać następujące czynności:

- Zmienić ustawienia dowolnego zadania, aby zapisywać zdarzenia związane z postępem zadania lub zapisywać tylko wyniki wykonania zadania.

- Skrócić lub wyłączyć okres przechowywania zdarzeń Serwera administracyjnego, Agenta sieciowego i aplikacji Kaspersky zainstalowanych na zarządzanych urządzeniach.

Postępując w ten sposób, zmniejszysz liczbę zdarzeń w bazie danych, zwiększysz prędkość wykonywania scenariuszy skojarzonych z analizą tabeli zdarzeń w bazie danych, a także zmniejszysz ryzyko nadpisania krytycznych zdarzeń przez dużą liczbę zdarzeń.

Ustawienia połączenia urządzeń chronionych UEFI

Urządzenie chronione UEFI to urządzenia z programem lub aplikacją Kaspersky dla UEFI zintegrowanymi na poziomie BIOS-u. Zintegrowana ochrona zapewnia bezpieczeństwo urządzenia od momentu uruchomienia systemu, natomiast ochrona na urządzeniach bez zintegrowanego oprogramowania zaczyna działać dopiero po uruchomieniu aplikacji zabezpieczającej. Kaspersky Security Center obsługuje zarządzanie tymi urządzeniami.

W celu zmodyfikowania ustawień połączenia urządzeń chronionych UEFI:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Porty dodatkowe**.

3. Zmodyfikuj odpowiednie ustawienia:

   - **Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS**

     Urządzenia chronione UEFI mogą nawiązywać połączenie z Serwerem administracyjnym.

   - **Port dla urządzeń chronionych UEFI i urządzeń KasperskyOS**

     Możesz zmienić numer portu, jeśli opcja **Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS** jest włączona. Domyślny numer portu to 13294.

4. Kliknij przycisk **Zapisz**.

Urządzenia chronione UEFI mogą teraz nawiązywać połączenie z Serwerem administracyjnym.

Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego Serwera administracyjnego

Dodawanie podrzędnego Serwera administracyjnego (wykonywane na przyszłym głównym Serwerze administracyjnym)

Możesz dodać Serwer administracyjny jako podrzędny Serwer administracyjny, a tym samym utworzyć hierarchię „główny/podrzędny".

W celu dodania podrzędnego Serwera administracyjnego, który jest dostępny do połączenia poprzez Kaspersky Security Center Web Console:

1. Upewnij się, że port 13000 przyszłego głównego Serwera administracyjnego jest dostępny do odbierania połączeń od podrzędnych Serwerów administracyjnych.

2. Na przyszłym głównym Serwerze administracyjnym kliknij ikonę ustawienia ( ).

3. W otwartym oknie właściwości wybierz zakładkę **Serwery administracyjne**.

4. Zaznacz pole obok nazwy grupy administracyjnej, do której chcesz dodać Serwer administracyjny.

5. W wierszu menu kliknij **Połącz podrzędny Serwer administracyjny**.

   Zostanie uruchomiony Kreator dodawania podrzędnego Serwera administracyjnego. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

6. Wypełnij następujące pola:

   - **Połącz główny Serwer administracyjny z podrzędnym Serwerem administracyjnym w DMZ**

     Wybierz tę opcję, jeśli podrzędny Serwer administracyjny znajduje się w strefie zdemilitaryzowanej (DMZ).

     Jeśli ta opcja jest zaznaczona, należy określić parametr **Adres serwera podrzędnego**.

     Jeżeli ta opcja jest zaznaczona, główny Serwer administracyjny inicjuje połączenie z podrzędnym Serwerem administracyjnym. W przeciwnym razie podrzędny Serwer administracyjny inicjuje połączenie z głównym Serwerem administracyjnym.

   - **Wyświetlana nazwa podrzędnego Serwera administracyjnego**

     Nazwa, pod którą podrzędny Serwer administracyjny będzie wyświetlany w hierarchii. Jeśli chcesz, możesz wprowadzić adres IP jako nazwę lub możesz użyć nazwy, na przykład „Serwer podrzędny dla grupy 1".

   - **Adres podrzędnego Serwera administracyjnego (opcjonalnie)**

     Określ adres IP lub nazwę domeny podrzędnego Serwera administracyjnego.

     Ten parametr jest wymagany, jeśli włączona jest opcja **Połącz główny Serwer administracyjny z podrzędnym Serwerem administracyjnym w DMZ**.

   - **Port SSL Serwera administracyjnego**

     Określ numer portu SSL, który ma być używany do komunikacji między głównym a podrzędnym Serwerem administracyjnym po utworzeniu hierarchii. Domyślny numer portu to 13000.

   - **Port API Serwera administracyjnego**

     Numer portu, którego Web Console będzie używać do odbierania połączeń od podrzędnego Serwera administracyjnego za pośrednictwem OpenAPI. Domyślny numer portu to 13299.

     Podczas tworzenia hierarchii Web Console łączy się z przyszłym podrzędnym Serwerem administracyjnym, żąda poświadczeń, pobiera certyfikat publiczny i przeprowadza konfigurację początkową.

     Po utworzeniu hierarchii Serwerów administracyjnych port 13299 nie będzie już używany. Serwery administracyjne będą komunikować się przez port 13000.

7. Określ certyfikat dla podrzędnego Serwera administracyjnego. Jeżeli określiłeś parametr **Adres serwera podrzędnego**, możesz kliknąć przycisk **Pobierz z podrzędnego Serwera administracyjnego,** aby uzyskać certyfikat. W przeciwnym razie kliknij przycisk **Przeglądaj w poszukiwaniu pliku certyfikatu** i zlokalizuj plik certyfikatu.

8. Określ ustawienia połączenia:

   - Wprowadź adres przyszłego głównego Serwera administracyjnego.

   - Jeśli przyszły podrzędny Serwer administracyjny będzie korzystał z serwera proxy, wprowadź adres serwera proxy i poświadczenia użytkownika, aby połączyć się z serwerem proxy.

9. Wprowadź poświadczenia użytkownika, który ma prawa dostępu na przyszłym podrzędnym Serwerze administracyjnym.

10. Jeśli weryfikacja dwuetapowa jest włączona i skonfigurowana, określ kod zabezpieczający wygenerowany przez aplikację uwierzytelniającą.

    Jeśli dla tego konta włączona jest weryfikacja dwuetapowa, ale nieskonfigurowana, utwórz hierarchię tylko z przyszłego serwera podrzędnego (zobacz instrukcje poniżej).

Jeśli ustawienia połączenia są prawidłowe, nawiązywane jest połączenie z przyszłym serwerem pomocniczym i budowana jest hierarchia „primary/secondary". Jeśli połączenie nie powiodło się, sprawdź ustawienia połączenia lub ręcznie określ certyfikat przyszłego Serwera pomocniczego.

Połączenie między głównym i pomocniczym Serwerem administracyjnym jest nawiązywane przez port 13000. Zostaną pobrane i zastosowane zadania i zasady z głównego Serwera administracyjnego. Podrzędny Serwer administracyjny jest wyświetlany na głównym Serwerze administracyjnym w grupie administracyjnej, do której został dodany.

Dodawanie podrzędnego Serwera administracyjnego (wykonywane na przyszłym podrzędnym Serwerze administracyjnym)

Jeśli nie udało się nawiązać połączenia z przyszłym podrzędnym Serwerem administracyjnym (na przykład był tymczasowo odłączony lub niedostępny), wciąż możesz dodać podrzędny Serwer administracyjny.

W celu dodania podrzędnego Serwera administracyjnego, który nie jest dostępny do połączenia poprzez Kaspersky Security Center Web Console:

1. Wyślij plik certyfikatu przyszłego głównego Serwera administracyjnego do administratora systemu biura, w którym znajduje się przyszły podrzędny Serwer administracyjny (możesz, na przykład, zapisać plik na urządzeniu zewnętrznym, takim jak dysk flash, lub wysłać go przez pocztę e-mail).

   Plik certyfikatu znajduje się na przyszłym głównym Serwerze administracyjnym w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

2. Poproś administratora systemu zarządzającego przyszłym podrzędnym Serwerem administracyjnym o wykonanie następujących czynności:

   a. Kliknij ikonę ustawienia ( ).

   b. W otwartym oknie właściwości przejdź do sekcji **Hierarchia Serwerów administracyjnych** zakładki **Ogólne**.

   c. Wybierz opcję **Ten Serwer administracyjny jest podrzędnym w hierarchii**.

   d. W polu **Adres głównego Serwera administracyjnego** wprowadź nazwę sieci przyszłego głównego Serwera administracyjnego.

   e. Wybierz wcześniej zapisany plik z certyfikatem przyszłego głównego Serwera administracyjnego, klikając **Przeglądaj**.

   f. Jeśli to konieczne, zaznacz pole **Połącz główny Serwer administracyjny z podrzędnym Serwerem administracyjnym w DMZ**.

g. Jeśli połączenie z przyszłym podrzędnym Serwerem administracyjnym odbywa się poprzez serwer proxy, wybierz opcję **Użyj serwera proxy** i określ ustawienia połączenia.

h. Kliknij **Zapisz**.

Zostanie utworzona hierarchia „główny/podrzędny". Główny Serwer administracyjny rozpocznie odbieranie połączenia od podrzędnego Serwera administracyjnego za pośrednictwem portu 13000. Zostaną pobrane i zastosowane zadania i zasady z głównego Serwera administracyjnego. Podrzędny Serwer administracyjny jest wyświetlany na głównym Serwerze administracyjnym w grupie administracyjnej, do której został dodany.

Przeglądanie listy podrzędnych Serwerów administracyjnych

W celu przejrzenia listy podrzędnych (w tym wirtualnych) Serwerów administracyjnych:

W oknie głównym aplikacji kliknij nazwę Serwera administracyjnego, która znajduje się obok ikony ustawienia ( ).

Zostanie wyświetlona lista rozwijana podrzędnych (w tym wirtualnych) Serwerów administracyjnych.

Możesz przejść do dowolnego z tych Serwerów administracyjnych, klikając jego nazwę.

Grupy administracyjne są także wyświetlane, ale są wyszarzone i nie są dostępne do zarządzania w tym menu.

Jeżeli jesteś połączony(-a) z głównym Serwerem administracyjnym w Kaspersky Security Center Web Console i nie możesz połączyć się z wirtualnym Serwerem administracyjnym zarządzanym przez podrzędny Serwer administracyjny, możesz skorzystać z jednego z następujących sposobów:

- **Zmodyfikuj istniejącą instalację Kaspersky Security Center Web Console, aby dodać serwer pomocniczy do listy zaufanych Serwerów administracyjnych**. Następnie będzie można połączyć się z wirtualnym Serwerem administracyjnym w Kaspersky Security Center Web Console.

  1. Na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console Server, uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe z poziomu konta z uprawnieniami administracyjnymi.

     Uruchomi się Kreator instalacji. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

  2. Wybierz opcję **Aktualizuj**.

  3. W kroku **Typ modyfikacji** wybierz opcję **Edycja ustawień połączenia**.

  4. W kroku **Zaufane Serwery administracyjne** dodaj wymagany podrzędny Serwer administracyjny.

  5. W ostatnim kroku kliknij opcję **Modyfikuj**, aby zastosować nowe ustawienia.

  6. Po pomyślnym zakończeniu ponownej konfiguracji aplikacji, kliknij przycisk **Zakończ**.

- Użyj Kaspersky Security Center Web Console, aby połączyć się bezpośrednio z podrzędnym serwerem administracyjnym, na którym utworzono wirtualny serwer. Następnie będzie można przełączyć się na wirtualny Serwer administracyjny w Kaspersky Security Center Web Console.

- Użyj konsoli administracyjnej opartej na programie MMC, aby połączyć się bezpośrednio z serwerem wirtualnym.

Usuwanie hierarchii Serwerów administracyjnych

Jeśli nie chcesz mieć hierarchii Serwerów administracyjnych, możesz odłączyć je od tej hierarchii.

W celu usunięcia hierarchii Serwerów administracyjnych:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy głównego Serwera administracyjnego.
2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.
3. W grupie administracyjnej, z której chcesz usunąć podrzędny Serwer administracyjny, wybierz podrzędny Serwer administracyjny.
4. W wierszu menu kliknij **Usuń**.
5. W otwartym oknie kliknij **OK**, aby potwierdzić chęć usunięcia podrzędnego Serwera administracyjnego.

Poprzedni główny Serwer administracyjny i poprzedni podrzędny Serwer administracyjny są teraz od siebie niezależne. Hierarchia już nie istnieje.

Konserwacja Serwera administracyjnego

Konserwacja Serwera administracyjnego umożliwia zwolnienie miejsca w folderze Serwera administracyjnego i zmniejszenie objętości bazy danych poprzez usunięcie obiektów, które nie są już potrzebne. Pomaga to poprawić wydajność i niezawodność działania aplikacji. Zalecamy przeprowadzanie konserwacji Serwera administracyjnego przynajmniej raz w tygodniu.

Konserwacja Serwera administracyjnego jest wykonywana przy pomocy dedykowanego zadania. Podczas konserwacji Serwera administracyjnego aplikacja wykonuje następujące działania:

- Usuwa niepotrzebne foldery i pliki z folderu przechowywania.
- Usuwa niepotrzebne rekordy z tabel (znane również jako „dangling pointers" (zwisające wskaźniki)).
- Czyści pamięć podręczną.
- Przeprowadza konserwację bazy danych (jeśli używasz SQL Server lub PostgreSQL jako DBMS):
  - Sprawdza bazę danych pod kątem błędów (funkcja dostępna tylko w przypadku SQL Server).
  - Reorganizuje indeksy w bazie danych.
  - Aktualizuje statystyki bazy danych.
  - Zmniejsza bazę danych (jeśli to konieczne).

Zadanie Konserwacja Serwera administracyjnego jest tworzone automatycznie podczas instalacji Kaspersky Security Center. Jeżeli zadanie Konserwacja Serwera administracyjnego zostało usunięte, możesz je utworzyć ręcznie.

W celu utworzenia zadania Konserwacja Serwera administracyjnego:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W oknie **Ustawienia nowych zadań** wybierz **Konserwacja Serwera administracyjnego** jako typ zadania i kliknij przycisk **Dalej**.
4. Wykonaj pozostałe instrukcje kreatora.

Nowo utworzone zadanie będzie wyświetlane na liście zadań. Dla jednego Serwera administracyjnego można uruchomić tylko jedno zadanie Konserwacja Serwera administracyjnego. Jeśli zadanie Konserwacja Serwera administracyjnego zostało już utworzone dla Serwera administracyjnego, nie będzie można utworzyć nowego zadania Konserwacja Serwera administracyjnego.

Konfigurowanie interfejsu

Możesz skonfigurować interfejs konsoli Kaspersky Security Center Web Console, aby wyświetlał i ukrywał sekcje i elementy interfejsu, w zależności od używanych funkcji.

W celu skonfigurowania interfejsu Kaspersky Security Center Web Console zgodnie z aktualnie używanym zestawem funkcji:

1. W menu głównym przejdź do ustawień konta i wybierz **Opcje interfejsu**.
2. W otwartym oknie **Opcje interfejsu** włącz lub wyłącz wymagane opcje.
3. Kliknij **Zapisz**.

Następnie konsola wyświetla sekcje w menu głównym zgodnie z włączonymi opcjami. Na przykład jeśli włączysz opcję **Pokaż alerty EDR**, w menu głównym pojawi się sekcja **Monitorowanie i raportowanie** → **Alerty**.

Zarządzanie wirtualnymi Serwerami administracyjnymi

W tej sekcji opisano następujące czynności zarządzania wirtualnymi Serwerami administracyjnymi:

- Utwórz wirtualne Serwery administracyjne
- Włącz i wyłącz wirtualny Serwer administracyjny
- Przypisz administratora wirtualnego Serwera administracyjnego
- Zmień Serwer administracyjny dla urządzeń klienckich
- Usuń wirtualne Serwery administracyjne

Tworzenie wirtualnego Serwera administracyjnego

Możesz utworzyć wirtualne Serwery administracyjne i dodać je do grup administracyjnych.

Podczas tworzenia wirtualnego Serwera administracyjnego dziedziczy on listę użytkowników i wszystkie uprawnienia użytkownika głównego Serwera administracyjnego. Jeśli użytkownik ma prawa dostępu do Serwera podstawowego, ten użytkownik ma również prawa dostępu do Serwera wirtualnego. Po utworzeniu samodzielnie konfigurujesz prawa dostępu do Serwerów.

W celu utworzenia i dodania wirtualnego Serwera administracyjnego:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.
2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.
3. Wybierz grupę administracyjną, do której chcesz dodać wirtualny Serwer administracyjny.
   Wirtualny serwer administracyjny będzie zarządzać urządzeniami z wybranej grupy (łącznie z podgrupami).
4. W wierszu menu kliknij **Nowy wirtualny Serwer administracyjny**.
5. W otwartym oknie zdefiniuj właściwości nowego wirtualnego Serwera administracyjnego:
   - **Nazwa wirtualnego Serwera administracyjnego**.
   - **Adres połączenia z Serwerem administracyjnym**

     Możesz określić nazwę lub adres IP serwera administracyjnego.
6. Z listy użytkowników wybierz administratora wirtualnego serwera administracyjnego. Jeśli chcesz, możesz edytować jedno z istniejących kont przed przypisaniem do niego roli administratora lub utworzyć nowe konto użytkownika.
7. Kliknij **Zapisz**.

Nowy wirtualny Serwer administracyjny zostanie utworzony, dodany do grupy administracyjnej i wyświetlony na zakładce **Serwery administracyjne**.

Jeżeli jesteś połączony(-a) z głównym Serwerem administracyjnym w Kaspersky Security Center Web Console i nie możesz połączyć się z wirtualnym Serwerem administracyjnym zarządzanym przez podrzędny Serwer administracyjny, możesz skorzystać z jednego z następujących sposobów:

- **Zmodyfikuj istniejącą instalację Kaspersky Security Center Web Console, aby dodać serwer pomocniczy do listy zaufanych Serwerów administracyjnych**. Następnie będzie można połączyć się z wirtualnym Serwerem administracyjnym w Kaspersky Security Center Web Console.

  1. Na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console Server, uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe z poziomu konta z uprawnieniami administracyjnymi.

     Uruchomi się Kreator instalacji. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.
  2. Wybierz opcję **Aktualizuj**.
  3. W kroku **Typ modyfikacji** wybierz opcję **Edycja ustawień połączenia**.

4. W kroku **Zaufane Serwery administracyjne** dodaj wymagany podrzędny Serwer administracyjny.

5. W ostatnim kroku kliknij opcję **Modyfikuj**, aby zastosować nowe ustawienia.

6. Po pomyślnym zakończeniu ponownej konfiguracji aplikacji, kliknij przycisk **Zakończ**.

- Użyj Kaspersky Security Center Web Console, aby połączyć się bezpośrednio z podrzędnym serwerem administracyjnym, na którym utworzono wirtualny serwer. Następnie będzie można przełączyć się na wirtualny Serwer administracyjny w Kaspersky Security Center Web Console.

- Użyj konsoli administracyjnej opartej na programie MMC, aby połączyć się bezpośrednio z serwerem wirtualnym.

Włączanie i wyłączanie wirtualnego Serwera administracyjnego

Jeśli tworzysz nowy wirtualny Serwer administracyjny, jest on domyślnie włączony. Możesz go wyłączyć lub ponownie włączyć w dowolnym momencie. Wyłączenie lub włączenie wirtualnego Serwera administracyjnego jest równoznaczne z wyłączeniem lub włączeniem fizycznego Serwera administracyjnego.

W celu włączenia lub wyłączenia wirtualnego Serwera administracyjnego:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.

3. Wybierz wirtualny Serwer administracyjny, który chcesz włączyć lub wyłączyć.

4. W wierszu menu kliknij przycisk **Włącz / wyłącz wirtualny Serwer administracyjny**.

   Stan wirtualnego Serwera administracyjnego jest zmieniany na włączony lub wyłączony, w zależności od jego poprzedniego stanu. Zaktualizowany stan jest wyświetlany obok nazwy Serwera administracyjnego.

Przypisywanie administratora do wirtualnego Serwera administracyjnego

Gdy używasz wirtualnych Serwerów administracyjnych w swojej organizacji, możesz chcieć przypisać dedykowanego administratora dla każdego wirtualnego Serwera administracyjnego. Na przykład, może to być przydatne podczas tworzenia wirtualnych Serwerów administracyjnych do zarządzania oddzielnymi biurami lub działami Twojej organizacji lub jeśli jesteś dostawcą MSP i zarządzasz swoimi dzierżawcami za pośrednictwem wirtualnych Serwerów administracyjnych.

Podczas tworzenia wirtualnego Serwera administracyjnego dziedziczy on listę użytkowników i wszystkie uprawnienia użytkownika głównego Serwera administracyjnego. Jeśli użytkownik ma prawa dostępu do Serwera podstawowego, ten użytkownik ma również prawa dostępu do Serwera wirtualnego. Po utworzeniu samodzielnie konfigurujesz prawa dostępu do Serwerów. Jeśli chcesz przypisać administratora tylko do wirtualnego Serwera administracyjnego, upewnij się, że administrator nie ma praw dostępu na głównym Serwerze administracyjnym.

Administratora wirtualnego Serwera administracyjnego przypisujesz poprzez nadanie praw dostępu administratora do wirtualnego Serwera administracyjnego. Możesz nadać wymagane prawa dostępu na jeden z następujących sposobów:

- Skonfiguruj ręcznie prawa dostępu administratora
- Przypisz jedną lub więcej ról użytkownika dla administratora

Aby zalogować się do Kaspersky Security Center Web Console, administrator wirtualnego Serwera administracyjnego określa nazwę wirtualnego Serwera administracyjnego, nazwę użytkownika i hasło. Kaspersky Security Center Web Console uwierzytelnia administratora i otwiera wirtualny Serwer administracyjny, do którego administrator ma prawa dostępu. Administrator nie może przełączać się między Serwerami administracyjnymi.

Wymagania wstępne

Przed rozpoczęciem upewnij się, że spełnione są następujące warunki:

- Tworzony jest wirtualny Serwer administracyjny.
- Na głównym Serwerze administracyjnym utworzono konto dla administratora, którego chcesz przypisać do wirtualnego Serwera administracyjnego.
- Masz uprawnienia **Modyfikacja list ACL obiektu** w obszarze funkcjonalnym **Funkcje ogólne** → **Uprawnienia użytkownika**.

Ręczne konfigurowanie praw dostępu

Przypisywanie administratora wirtualnego Serwera administracyjnego:

1. W menu głównym przejdź do wymaganego wirtualnego Serwera administracyjnego:
   a. Kliknij ikonę jodełki ( ) po prawej stronie bieżącej nazwy Serwera administracyjnego.
   b. Wybierz wymagany Serwer administracyjny.
2. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy Serwera administracyjnego.
   Zostanie otwarte okno właściwości Serwera administracyjnego.
3. Na zakładce **Prawa dostępu** kliknij przycisk **Dodaj**.
   Zostanie otwarta ujednolicona lista użytkowników głównego Serwera administracyjnego i bieżącego wirtualnego Serwera administracyjnego.
4. Z listy użytkowników wybierz konto administratora, którego chcesz przypisać do wirtualnego Serwera administracyjnego, a następnie kliknij przycisk **OK**.
   Aplikacja dodaje wybranego użytkownika do listy użytkowników na zakładce **Prawa dostępu**.
5. Zaznacz pole wyboru obok dodanego konta, a następnie kliknij przycisk **Prawa dostępu**.
6. Skonfiguruj uprawnienia, jakie będzie miał administrator na wirtualnym Serwerze administracyjnym.

W celu pomyślnego uwierzytelnienia administrator musi mieć co najmniej następujące uprawnienia:

- **Odczyt** bezpośrednio w obszarze funkcjonalnym **Funkcje ogólne** → **Podstawowa funkcjonalność**
- **Odczyt** bezpośrednio w obszarze funkcjonalnym **Funkcje ogólne** → **Wirtualne Serwery administracyjne**

Aplikacja zapisuje zmodyfikowane uprawnienia użytkownika na koncie administratora.

Konfigurowanie praw dostępu poprzez przypisywanie ról użytkownikom

Alternatywnie możesz przyznać prawa dostępu administratorowi wirtualnego Serwera administracyjnego poprzez role użytkownika. Na przykład, może to być przydatne, jeśli chcesz przypisać kilku administratorów do tego samego wirtualnego Serwera administracyjnego. W takim przypadku można przypisać kontom administratorów identyczne role użytkownika (jedną lub więcej) zamiast konfigurować te same uprawnienia użytkownika w odniesieniu do kilku administratorów.

W celu przypisania administratora wirtualnego Serwera administracyjnego poprzez przypisanie ról użytkownika:

1. Na głównym Serwerze administracyjnym utwórz nową rolę użytkownika, a następnie określ wszystkie wymagane prawa dostępu, które musi posiadać administrator na wirtualnym Serwerze administracyjnym. Możesz utworzyć kilka ról, na przykład jeśli chcesz oddzielić dostęp do różnych obszarów funkcjonalnych.
2. W menu głównym przejdź do wymaganego wirtualnego Serwera administracyjnego:
   a. Kliknij ikonę jodełki (›) po prawej stronie bieżącej nazwy Serwera administracyjnego.
   b. Wybierz wymagany Serwer administracyjny.
3. Przypisz nową rolę lub kilka ról do konta administratora.

Aplikacja przypisuje role do konta administratora.

Konfigurowanie praw dostępu na poziomie obiektu

Oprócz przypisywania praw dostępu na poziomie obszaru funkcjonalnego, możesz skonfigurować dostęp do określonych obiektów na wirtualnym Serwerze administracyjnym, na przykład do określonej grupy administracyjnej lub zadania. W tym celu przełącz się na wirtualny Serwer administracyjny, a następnie skonfiguruj prawa dostępu we właściwościach obiektu.

Zmienianie Serwera administracyjnego dla urządzeń klienckich

Można zmienić Serwer administracyjny zarządzający urządzeniami klienckimi na inny, używając zadania *Zmiana Serwera administracyjnego*. Po zakończeniu zadania wybrane urządzenia klienckie zostaną objęte zarządzaniem przez określony Serwer administracyjny.

Nie możesz użyć zadania *Zmiana Serwera administracyjnego* w przypadku urządzeń klienckich podłączonych do Serwera administracyjnego poprzez bramy połączeń. W przypadku takich urządzeń należy albo ponownie skonfigurować Agenta sieciowego, albo ponownie zainstalować Agenta sieciowego i określić bramę połączenia.

W celu zmiany Serwera administracyjnego zarządzającego urządzeniami klienckimi na inny Serwer:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. W kroku **Ustawienia nowych zadań** kreatora określ następujące ustawienia:

   a. Z listy rozwijanej **Aplikacja** wybierz **Kaspersky Security Center**.

   b. W polu **Typ zadania** wybierz opcję **Zmiana Serwera administracyjnego**.

   c. W oknie **Nazwa zadania** określ nazwę dla zadania, które tworzysz.

      Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

   d. Wybierz urządzenia, do których zadanie zostanie przypisane:

      - **Przypisz zadanie do grupy administracyjnej**

        Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

        Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

        Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

      - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

        Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

        Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

      - **Przypisz zadanie do wyboru urządzeń**

        Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

        Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

4. W kroku **Zakres zadania** kreatora określ grupę administracyjną, urządzenia o określonych adresach lub wybór urządzeń.

5. W tym kroku kreatora potwierdź, że akceptujesz warunki zmiany Serwera administracyjnego dla urządzeń klienckich.

6. W tym kroku kreatora wybierz Serwer administracyjny, którego chcesz używać do zarządzania wybranymi urządzeniami:

   - **Zmień na inny główny Serwer administracyjny**

     Aby przenieść urządzenia klienckie na inny główny Serwer administracyjny, należy określić następujące ustawienia połączenia z Serwerem administracyjnym:

     1. W polu **Adres Serwera administracyjnego** należy podać adres nowego głównego Serwera administracyjnego.

     2. W polu **Numer portu** należy określić numer portu, za pomocą którego ma zostać nawiązane połączenie z Serwerem administracyjnym.

        Domyślny numer portu to 14000.

     3. W polu **Port SSL** określ numer portu SSL na głównym Serwerze administracyjnym.

        Domyślny numer portu to 13000.

     4. W razie potrzeby włącz opcję **Użyj serwera proxy**.

        Jeżeli ta opcja jest wyłączona, do połączenia urządzenia z Serwerem administracyjnym wykorzystywane jest połączenie bezpośrednie.

        Jeżeli ta opcja jest włączona, określ parametry serwera proxy:

        - **Adres serwera proxy**

        - **Port serwera proxy**

        Jeżeli Twój serwer proxy wymaga uwierzytelnienia, w polach **Nazwa użytkownika** i **Hasło**, określ poświadczenia konta, w ramach którego nawiązywane jest połączenie z serwerem proxy. Zalecamy określenie poświadczeń konta, które ma minimalne uprawnienia wymagane tylko do uwierzytelnienia serwera proxy.

     5. W razie potrzeby prześlij nowy certyfikat Serwera administracyjnego.

   - **Zmień na inny wirtualny Serwer na głównym Serwerze**

     Wybierz tę opcję, aby przenieść urządzenia klienckie na wirtualny Serwer administracyjny na bieżącym głównym Serwerze administracyjnym. Aby to zrobić, z listy rozwijanej **Nazwa wirtualnego Serwera administracyjnego** wybierz żądany wirtualny Serwer administracyjny.

7. W kroku **Wybieranie konta do uruchomienia zadania** kreatora określ ustawienia konta:

   - **Konto domyślne**

     Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

     Domyślnie opcja ta jest zaznaczona.

   - **Określ konto**

     Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

     - **Konto**

       Konto, z poziomu którego zadanie jest uruchamiane.

- **Hasło**

  Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

8. Jeśli chcesz zmienić domyślne ustawienia zadania, w kroku **Zakończ tworzenie zadania** kreatora zaznacz opcję **Otwórz szczegóły zadania po jego utworzeniu**.

   Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

9. Kliknij przycisk **Zakończ**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

10. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

11. Jeśli chcesz zmienić domyślne ustawienia zadania, w oknie właściwości zadania określ ogólne ustawienia zadania według swoich potrzeb.

12. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

13. Uruchom utworzone zadanie.

Po zakończeniu wykonywania zadania, urządzenia klienckie, dla których zostało ono utworzone, zostaną przekazane Serwerowi administracyjnemu określonemu w ustawieniach zadania.

Usuwanie wirtualnego Serwera administracyjnego

Jeśli usuniesz wirtualny Serwer administracyjny, wszystkie obiekty utworzone na Serwerze administracyjnym, w tym zasady i zadania, również zostaną usunięte. Zarządzane urządzenia z grup administracyjnych, którymi zarządzał wirtualny Serwer administracyjny, zostaną usunięte z grup administracyjnych. Aby przywrócić urządzenia zarządzane przez Kaspersky Security Center, uruchom przeszukiwanie sieci, a następnie przenieś wykryte urządzenia z grupy Urządzenia nieprzypisane do grup administracyjnych.

W celu usunięcia wirtualnego Serwera administracyjnego:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy Serwera administracyjnego.

2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.

3. Wybierz wirtualny Serwer administracyjny, który chcesz usunąć.

4. W wierszu menu kliknij **Usuń**.

Wirtualny Serwer administracyjny zostanie usunięty.

Włączanie ochrony konta przed nieautoryzowaną modyfikacją

Możesz włączyć dodatkową opcję ochrony konta użytkownika przed nieautoryzowaną modyfikacją. Jeżeli opcja jest włączona, modyfikowanie ustawień konta użytkownika wymaga autoryzacji przez użytkownika z uprawnieniami do modyfikacji.

W celu włączenia lub wyłączenia ochrony konta przed nieautoryzowaną modyfikacją:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Kliknij nazwę wewnętrznego konta użytkownika, dla którego chcesz określić ochronę konta przed nieautoryzowaną modyfikacją.
3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Ochrona konta**.
4. Na zakładce **Ochrona konta** wybierz opcję **Poproś o uwierzytelnienie, aby sprawdzić uprawnienia do modyfikowania kont użytkowników**, jeśli chcesz żądać poświadczeń za każdym razem, gdy ustawienia konta są zmieniane lub modyfikowane. W przeciwnym razie wybierz opcję **Zezwalaj użytkownikom na modyfikowanie tego konta bez dodatkowego uwierzytelniania**.
5. Kliknij przycisk **Zapisz**.

Ochrona konta przed nieautoryzowaną modyfikacją jest włączona dla konta użytkownika.

Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego

Tworzenie kopii zapasowej danych umożliwia przeniesienie Serwera administracyjnego z jednego urządzenia na inne, bez utraty danych. Dzięki kopii zapasowej możesz przywrócić dane podczas przenoszenia bazy danych Serwera administracyjnego na inne urządzenie lub podczas aktualizacji do nowszej wersji Kaspersky Security Center. Możesz również wykorzystać Kopię zapasową danych do przeniesienia danych Serwera administracyjnego z Kaspersky Security Center Windows zarządzanego przez Kaspersky Security Center Linux (przenoszenie danych z Kaspersky Security Center Linux do Kaspersky Security Center Windows nie jest obsługiwane).

Nie są tworzone kopie zapasowe zainstalowanych wtyczek zarządzających. Po przywróceniu danych Serwera administracyjnego z kopii zapasowej należy pobrać i ponownie zainstalować wtyczki dla zarządzanych aplikacji.

Zanim utworzysz kopię zapasową danych Serwera administracyjnego, sprawdź, czy do grupy administracyjnej został dodany wirtualny Serwer administracyjny. Jeśli dodany jest wirtualny Serwer administracyjny, przed utworzeniem kopii zapasowej upewnij się, że do tego wirtualnego Serwera administracyjnego został przypisany administrator. Po utworzeniu kopii zapasowej nie możesz nadać administratorowi praw dostępu do wirtualnego Serwera administracyjnego. Należy pamiętać, że w przypadku utraty poświadczeń konta administratora nie będzie można przypisać nowego administratora do wirtualnego Serwera administratora.

Aby utworzyć kopię zapasową lub przywrócić klaster pracy awaryjnej Kaspersky Security Center, należy zatrzymać cały klaster w celu przeprowadzenia konserwacji, a następnie ponownie go uruchomić po zakończeniu tworzenia kopii zapasowej lub przywracania.

Możesz utworzyć kopię zapasową danych Serwera administracyjnego w jeden z następujących sposobów:

- Tworząc i uruchamiając zadanie wykonywania kopii zapasowej danych poprzez Konsolę administracyjną.
- Uruchamiając narzędzie klbackup na urządzeniu, na którym jest zainstalowany Serwer administracyjny. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center. Po zainstalowaniu Serwera administracyjnego, narzędzie jest umieszczane w katalogu głównym folderu docelowego, określonego podczas instalacji aplikacji.

W kopii zapasowej Serwera administracyjnego zapisywane są następujące dane:

- Baza danych Serwera administracyjnego (zasady, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym).
- Informacje o konfiguracji struktury grup administracyjnych i urządzeń klienckich.
- Repozytorium pakietów dystrybucyjnych aplikacji przeznaczonych do zdalnego zainstalowania.
- Certyfikat Serwera administracyjnego.
- Zawartość folderu *Aktualizacje*.

  Domyślna ścieżka do folderu to C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

Odzyskanie danych Serwera administracyjnego jest możliwe tylko przy użyciu narzędzia klbackup. Należy wykonać przywracanie kopii zapasowej na działającej instancji Serwera administracyjnego, który został właśnie zainstalowany i posiada tę samą wersję (lub nowszą), dla której kopia zapasowa została utworzona.

Tworzenie zadania wykonywania kopii zapasowej

Zadania kopii zapasowej są zadaniami Serwera administracyjnego i są tworzone podczas działania kreatora wstępnej konfiguracji. Jeśli zadanie kopii zapasowej utworzone przez Kreator wstępnej konfiguracji zostało usunięte, możesz je utworzyć ręcznie.

W celu utworzenia zadania kopii zapasowej danych Serwera administracyjnego:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W oknie **Ustawienia nowych zadań** wybierz typ zadania **Kopia zapasowa danych Serwera administracyjnego**
4. Wykonaj pozostałe instrukcje kreatora.

Zadanie **Kopia zapasowa danych Serwera administracyjnego** może zostać utworzone tylko w jednej kopii. Jeśli dla Serwera administracyjnego już utworzono zadanie tworzenia kopii zapasowych danych Serwera administracyjnego, nie będzie wyświetlane w oknie wyboru typu zadania kreatora tworzenia zadania kopii zapasowej Serwera administracyjnego.

Aby skonfigurować zadanie Kopia zapasowa danych Serwera administracyjnego:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**, a następnie wybierz zadanie **Kopia zapasowa danych Serwera administracyjnego**.
2. Kliknij zadanie **Kopia zapasowa danych Serwera administracyjnego**.

   Zostanie otwarte okno właściwości zadania.
3. W razie potrzeby określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.
4. W sekcji **Ustawienia aplikacji** określ ścieżkę do folderu przechowywania kopii zapasowych danych Serwera administracyjnego, ustaw hasło ochrony kopii zapasowej oraz, jeśli to konieczne, liczbę kopii zapasowych.
5. Kliknij **Zapisz**, aby zastosować zmiany.

Zadanie *Kopia zapasowa danych Serwera administracyjnego* zostało skonfigurowane.

Przenoszenie Serwera administracyjnego na inne urządzenie

Jeśli chcesz użyć Serwera administracyjnego na nowym urządzeniu, możesz je przenieść w jeden z następujących sposobów:

- Przenieś Serwer administracyjny i serwer bazy danych na nowe urządzenie (serwer bazy danych może być zainstalowany na nowym urządzeniu wraz Serwerem administracyjnym, lub na innym urządzeniu).
- Zachowaj serwer bazy danych na poprzednim urządzeniu i przenieś tylko Serwer administracyjny na nowe urządzenie.

W celu przeniesienia Serwera administracyjnego i serwera bazy danych na nowe urządzenie:

1. Na poprzednim urządzeniu utwórz kopię zapasową danych Serwera administracyjnego.

   W tym celu możesz uruchomić zadanie tworzenia kopii zapasowej danych poprzez Kaspersky Security Center Web Console lub uruchomić narzędzie klbackup.

   > Jeśli używasz SQL Server jako DBMS dla Serwera administracyjnego, możesz migrować dane z SQL Server do MySQL lub MariaDB DBMS. Aby to zrobić, uruchom narzędzie klbackup w trybie interaktywnym, aby utworzyć kopię zapasową danych. Włącz opcję **Wykonaj migrację do formatu MySQL/MariaDB** w oknie **Ustawienia kopii zapasowej** kopii zapasowej Kreatora kopii zapasowych i przywracania. Kaspersky Security Center utworzy kopię zapasową kompatybilną z MySQL i MariaDB. Następnie możesz przywrócić dane z kopii zapasowej do MySQL lub MariaDB.

   > Możesz również włączyć opcję **Wykonaj migrację do formatu Azure** jeśli chcesz migrować dane z SQL Server do Azure SQL DBMS.
2. Na poprzednim urządzeniu odłącz Serwer administracyjny od sieci.
3. Wybierz nowe urządzenie, na którym chcesz zainstalować Serwer administracyjny. Upewnij się, że sprzęt i oprogramowanie na wybranym urządzeniu spełniają wymagania Serwera administracyjnego, Kaspersky Security Center Web Console oraz Agenta sieciowego. Sprawdź również, czy dostępne są porty używane na Serwerze administracyjnym.

4. Przypisz ten sam adres do nowego urządzenia.

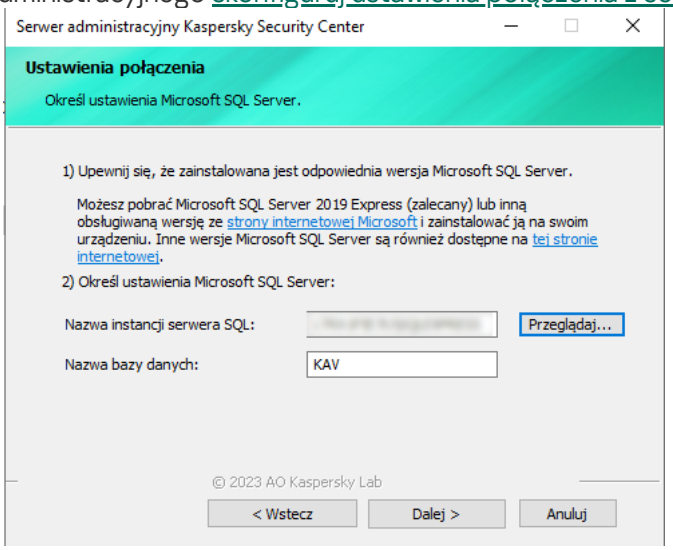
   Nowy Serwer administracyjny może mieć przypisaną nazwę NetBIOS, FQDN i statyczny adres IP. Zależy to od tego, który adres Serwera administracyjnego został ustawiony w pakiecie instalacyjnym Agenta sieciowe w momencie instalacji Agenta sieciowego. Alternatywnie można użyć adresu połączenia, który określa Serwer administracyjny, z którym łączy się Agent sieciowy (możesz uzyskać ten adres na zarządzanych urządzeniach korzystając z narzędzia klnagchk).

5. W razie konieczności, na innym urządzeniu, zainstaluj system zarządzania bazą danych (DBMS), którego będzie używał Serwer administracyjny.

   Bazę danych można zainstalować na nowym urządzeniu razem z Serwerem administracyjnym lub na innym urządzeniu. Upewnij się, że urządzenia spełnia wymagania sprzętowe i programowe. Kiedy wybierasz DBMS, weź pod uwagę liczbę urządzeń obsługiwanych przez Serwer administracyjny.

6. Uruchom instalację Serwera administracyjnego na nowym urządzeniu.

7. Podczas instalacji Serwera administracyjnego skonfiguruj ustawienia połączenia z serwerem bazy danych.



Przykład okna Ustawienia połączenia dla Microsoft SQL Server

W zależności od tego, gdzie chcesz zlokalizować serwer bazy danych, wykonaj jedną z następujących czynności:

- **Zachowaj serwer bazy danych na poprzednim urządzeniu**

  1. Kliknij przycisk **Przeglądaj** obok pola **Nazwa instancji serwera SQL**, a następnie wybierz poprzednią nazwę urządzenia z wyświetlonej listy.

     Pamiętaj, że poprzednie urządzenie musi być dostępne do połączenia z nowym Serwerem administracyjnym.

  2. Wprowadź poprzednią nazwę bazy danych w polu **Nazwa bazy danych**.

- **Przenieś bazę danych na inne urządzenie**

  1. Kliknij przycisk **Przeglądaj** obok pola **Nazwa instancji serwera SQL**, a następnie wybierz nazwę urządzenia z wyświetlonej listy.

  2. Wprowadź nową nazwę bazy danych w polu **Nazwa bazy danych**.

     Należy pamiętać, że nazwa nowej bazy danych musi być zgodna z nazwą bazy danych z poprzedniego urządzenia. Nazwy baz danych muszą być identyczne, abyś mógł korzystać z kopii zapasowej Serwera administracyjnego. Domyślna nazwa bazy danych to *KAV*.

8. Po zakończeniu instalacji odzyskaj dane Serwera administracyjnego na nowym urządzeniu za pomocą narzędzia klbackup.

   Jeśli używasz programu SQL Server jako DBMS na poprzednich i nowych urządzeniach, pamiętaj, że wersja programu SQL Server zainstalowana na nowym urządzeniu musi być taka sama lub nowsza niż wersja programu SQL Server zainstalowana na poprzednim urządzeniu. W przeciwnym razie nie będzie możliwe odzyskanie danych Serwera administracyjnego na nowym urządzeniu.

9. Otwórz Kaspersky Security Center Web Console i połącz się z Serwerem administracyjnym.

10. Sprawdź, czy wszystkie zarządzane urządzenia są podłączone do Serwera administracyjnego.

11. Odinstaluj Serwer administracyjny i serwer bazy danych z poprzedniego urządzenia.

Możesz także użyć Konsoli administracyjnej do przeniesienia Serwera administracyjnego i serwera bazy danych na inne urządzenie.

Sprawdzanie integralności modułów za pomocą narzędzi klscmodchk i integrity_checker

Kaspersky Security Center zawiera wiele modułów binarnych w formie bibliotek dołączanych dynamicznie, plików wykonywalnych, plików konfiguracyjnych i plików interfejsu. Intruzi mogą wymienić jeden lub więcej modułów wykonywalnych lub plików aplikacyjnych na inne pliki zawierające szkodliwy kod. Aby nie dopuścić do zamiany modułów i plików, Kaspersky Security Center zapewnia kontrolę integralności komponentów za pomocą narzędzi klscmodchk i integrity_checker. Te narzędzia sprawdzają moduły i pliki pod kątem nieautoryzowanych zmian lub uszkodzeń. Jeżeli moduł lub plik aplikacji ma nieprawidłową sumę kontrolną, jest uznawany za uszkodzony.

Narzędzie klscmodchk wykonuje kontrolę integralności dla następujących komponentów Kaspersky Security Center:

- Serwer administracyjny
- Agent sieciowy
- Wtyczki zarządzające dla Konsoli administracyjnej z plikami manifestu

Narzędzie integrity_checker wykonuje kontrolę integralności dla następujących komponentów Kaspersky Security Center:

- Serwer administracyjny
- Agent sieciowy
- Kaspersky Security Center Web Console

Oba narzędzia sprawdzają integralność modułów w oparciu o plik manifestu kl_file_integrity_manifest.xml, który jest częścią kompilacji Kaspersky Security Center i znajduje się w folderze instalacyjnym. Plik manifestu komponentu zawiera pliki, których integralność jest ważna z punktu widzenia prawidłowego działania komponentu Kaspersky Security Center. Integralność samego pliku manifestu jest również sprawdzana.

Zdecydowanie nie zalecamy modyfikacji pliku manifestu kl_file_integrity_manifest.xml, gdyż spowoduje to unieważnienie podpisu cyfrowego i nieudaną kontrolę integralności.

Aby sprawdzić integralność komponentu Kaspersky Security Center, uruchomić jedno z poniższych poleceń:

- `$ klscmodchk [ parametry ]`

  Narzędzie klscmodchk uruchamia narzędzie integrity_checker z parametrem `--verbose` i sprawdza integralność modułów.

  Parametry dla narzędzia klscmodchk:

  - `-logfile <log_file_path>`—Określa ścieżkę do pliku na dysku do logowania. Domyślnie informacja jest wyświetlana na konsoli.
  - `-chkplugins`—Sprawdza integralność zainstalowanych modułów wtyczek zarządzających dla Konsoli administracyjnej, która zawiera pliki manifestu. Domyślnie wtyczki zarządzające nie są sprawdzane.
  - `-verbose`—Wyświetla rozszerzone informacje w trakcie sprawdzania integralności.

- `$ integrity_checker [ parametry ] <ścieżka_do_pliku_manifestu>`

  Parametry dla narzędznia integrity_checker:

  - `--help`—Wyświetla pomoc narzędzia integrity_checker.
  - `--version`—Wyświetla wersję narzędzia integrity_checker.
  - `--verbose`—Wyświetla informacje o działaniu narzędzia. Wykonując kontrolę integralności, wystarczy użyć tego parametru w wierszu poleceń.

Wyniki sprawdzenia każdego pliku manifestu są wyświetlane obok nazwy pliku manifestu w następującym formacie:

- SUCCEEDED—Integralność pliku potwierdzona (kod zwrotny 0).
- FAILED—Integralność pliku nie została potwierdzona (niezerowy kod powrotny).

Można również skonfigurować automatyczne uruchamianie sprawdzania integralności podczas uruchamiania aplikacji. Domyślnie automatyczne sprawdzanie integralności jest wyłączone.

Aby włączyć automatyczne sprawdzanie integralności:

1. Na urządzeniu z zainstalowanym Serwerem Administracyjnym, w wierszu poleceń systemu Windows wprowadź następujące polecenie:

   ```
   klscflag.exe -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Uruchom urządzenie ponownie.

Automatyczne sprawdzanie integralności jest włączone.

Przy kolejnym uruchomieniu Kaspersky Security Center narzędzie klscmodchk zostanie uruchomione wraz z Serwerem Administracyjnym i rozpocznie sprawdzanie integralności modułów. Wyniki kontroli integralności są zapisywane do Dziennika zdarzeń aplikacji Kaspersky.

Początkowa konfiguracja Kaspersky Security Center Web Console

Ta sekcja opisuje kroki, jakie należy podjąć po zainstalowaniu Kaspersky Security Center Web Console, aby przeprowadzić wstępną konfigurację.

Kreator wstępnej konfiguracji (Kaspersky Security Center Web Console)

Ta sekcja zawiera informacje o działaniu kreatora wstępnej konfiguracji Serwera administracyjnego.

kreator wymaga dostępu do Internetu. Jeżeli Twój Serwer administracyjny nie ma dostępu do Internetu, zalecamy ręczne wykonanie wszystkich kroków kreatora poprzez interfejs konsoli Kaspersky Security Center Web Console.

Kaspersky Security Center umożliwia dostosowanie minimalnego zestawu ustawień niezbędnych do stworzenia systemu scentralizowanego zarządzania ochroną sieci przed zagrożeniami bezpieczeństwa. Taka konfiguracja jest przeprowadzana przez Kreator wstępnej konfiguracji. Przy pierwszym uruchomieniu kreatora możesz wprowadzić w aplikacji następujące zmiany:

- Dodaj pliki klucza lub wprowadź kody aktywacyjne, które mogą być automatycznie przesyłane do urządzeń w grupach administracyjnych.
- Skonfigurować interakcję z Kaspersky Security Network (KSN). Jeśli zezwolono na używanie KSN, kreator uruchomi usługę serwera proxy KSN, która zapewnia połączenie pomiędzy KSN a urządzeniami.
- Skonfigurować dostarczanie powiadomień informujących o zdarzeniach występujących podczas działania Serwera administracyjnego i zarządzanych aplikacji (w celu zapewnienia poprawnego działania opcji dostarczania powiadomień, na Serwerze administracyjnym i wszystkich urządzeniach, na które mają być wysyłane powiadomienia, powinna być włączona usługa Posłaniec).
- Utworzyć zasadę ochrony dla stacji roboczych i serwerów, a także zadania skanowania w poszukiwaniu złośliwego oprogramowania, zadania pobierania aktualizacji i zadania tworzenia kopii zapasowej danych dla najwyższego poziomu hierarchii zarządzanych urządzeń.

  Kreator wstępnej konfiguracji tworzy zasady tylko dla tych aplikacji, dla których folder **Zarządzane urządzenia** nie zawiera żadnych zasad. Kreator wstępnej konfiguracji nie tworzy zadań, jeśli zadania o tych samych nazwach zostały już utworzone dla najwyższego poziomu hierarchii zarządzanych urządzeń.

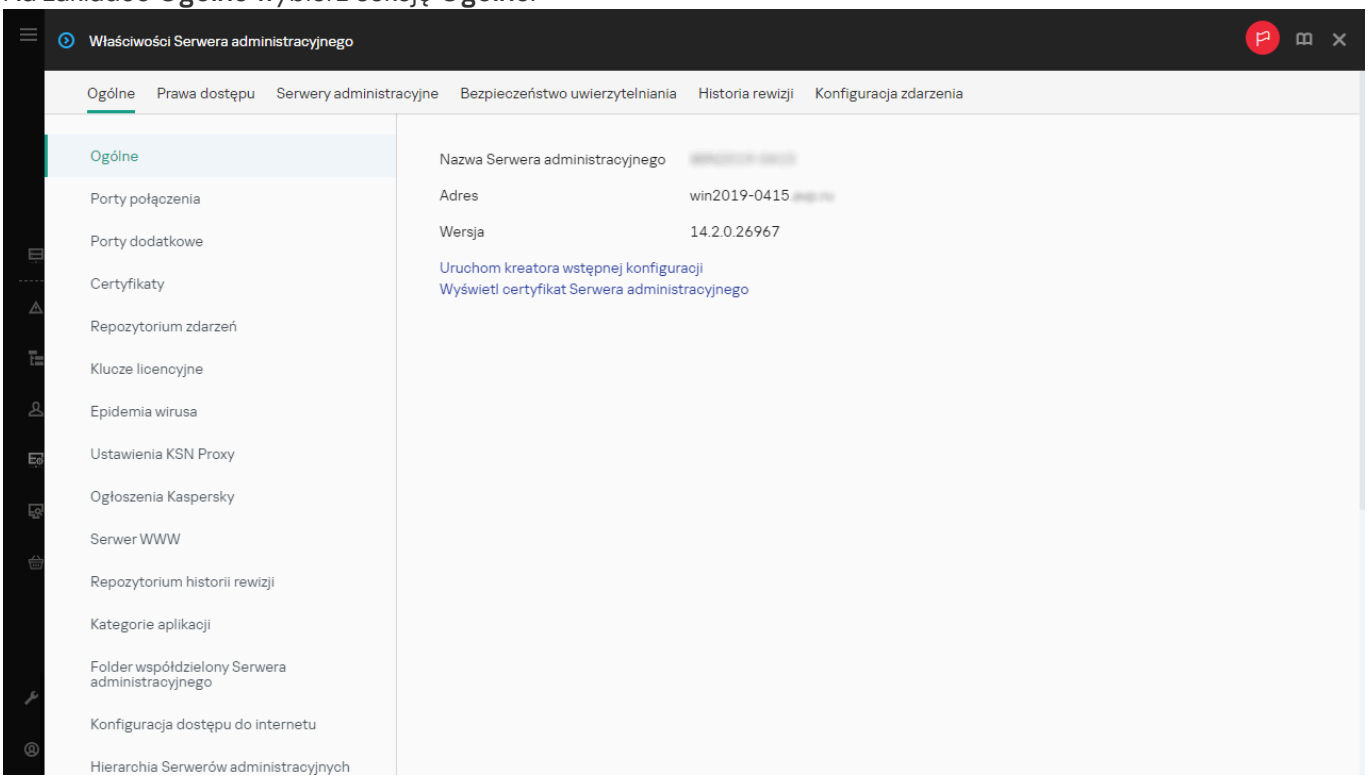
Po zainstalowaniu Serwera administracyjnego, przy pierwszym nawiązaniu połączenia z nim, aplikacja automatycznie wyświetli pytanie dotyczące uruchomienia kreatora wstępnej konfiguracji. Kreator wstępnej konfiguracji można również uruchomić ręcznie w dowolnym momencie.

W celu ręcznego uruchomienia kreatora wstępnej konfiguracji:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ogólne**.



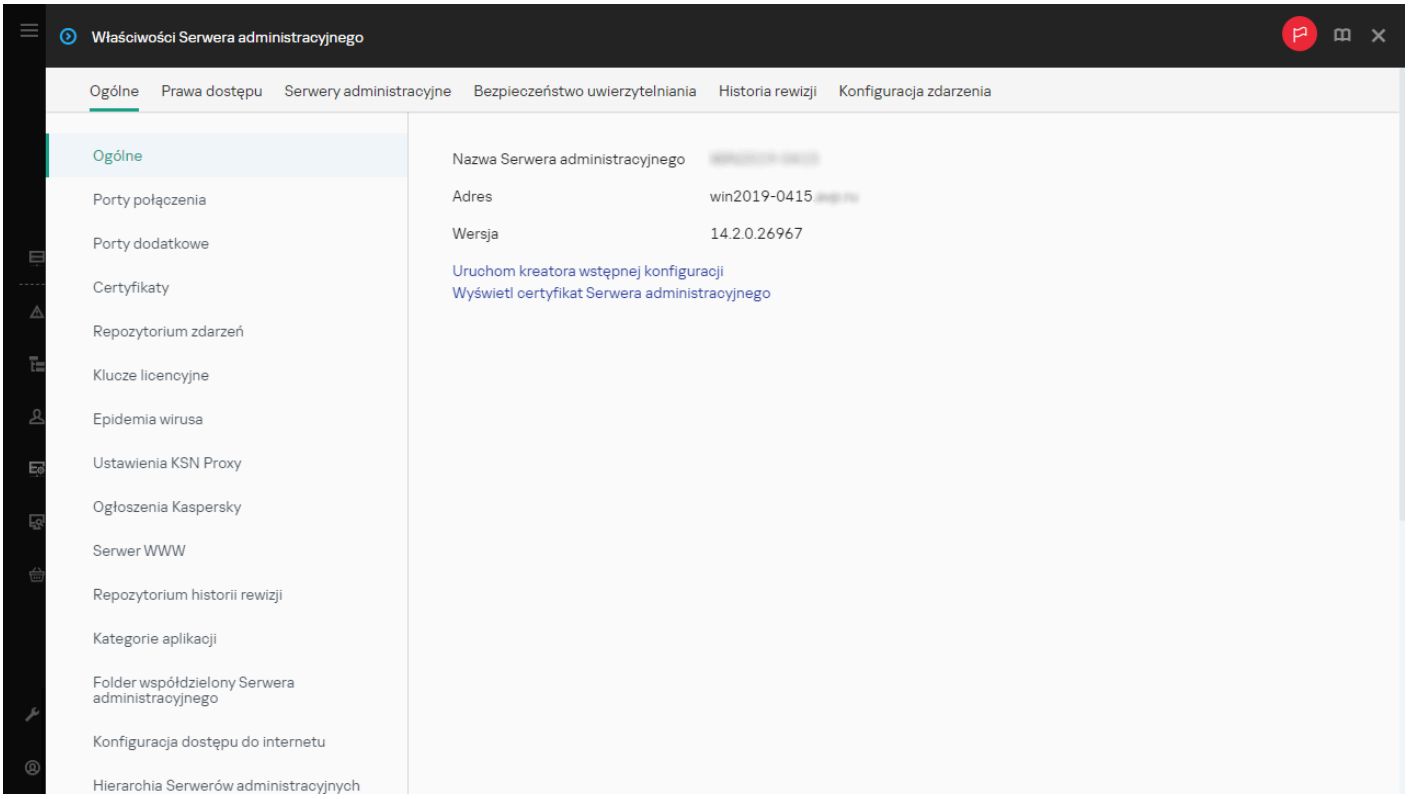
Okno właściwości Serwera administracyjnego

3. Kliknij **Uruchom kreatora wstępnej konfiguracji**.

kreator wyświetli pytanie o przeprowadzenie wstępnej konfiguracji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

Krok 1. Określenie ustawień połączenia internetowego

Określ ustawienia dostępu do Internetu dla Serwera administracyjnego. Należy skonfigurować dostęp do Internetu w taki sposób, aby korzystać z Kaspersky Security Network i pobierać aktualizacje antywirusowych baz danych dla Kaspersky Security Center i zarządzanych aplikacji Kaspersky.



Ustawienia połączenia z internetem

Włącz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest włączona, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

- **Adres**

  Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

- **Numer portu**

  Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

- **Pomiń serwer proxy dla adresów lokalnych**

  Żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

- **Uwierzytelnianie na serwerze proxy**

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

- **Nazwa użytkownika**

  Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

- **Hasło**

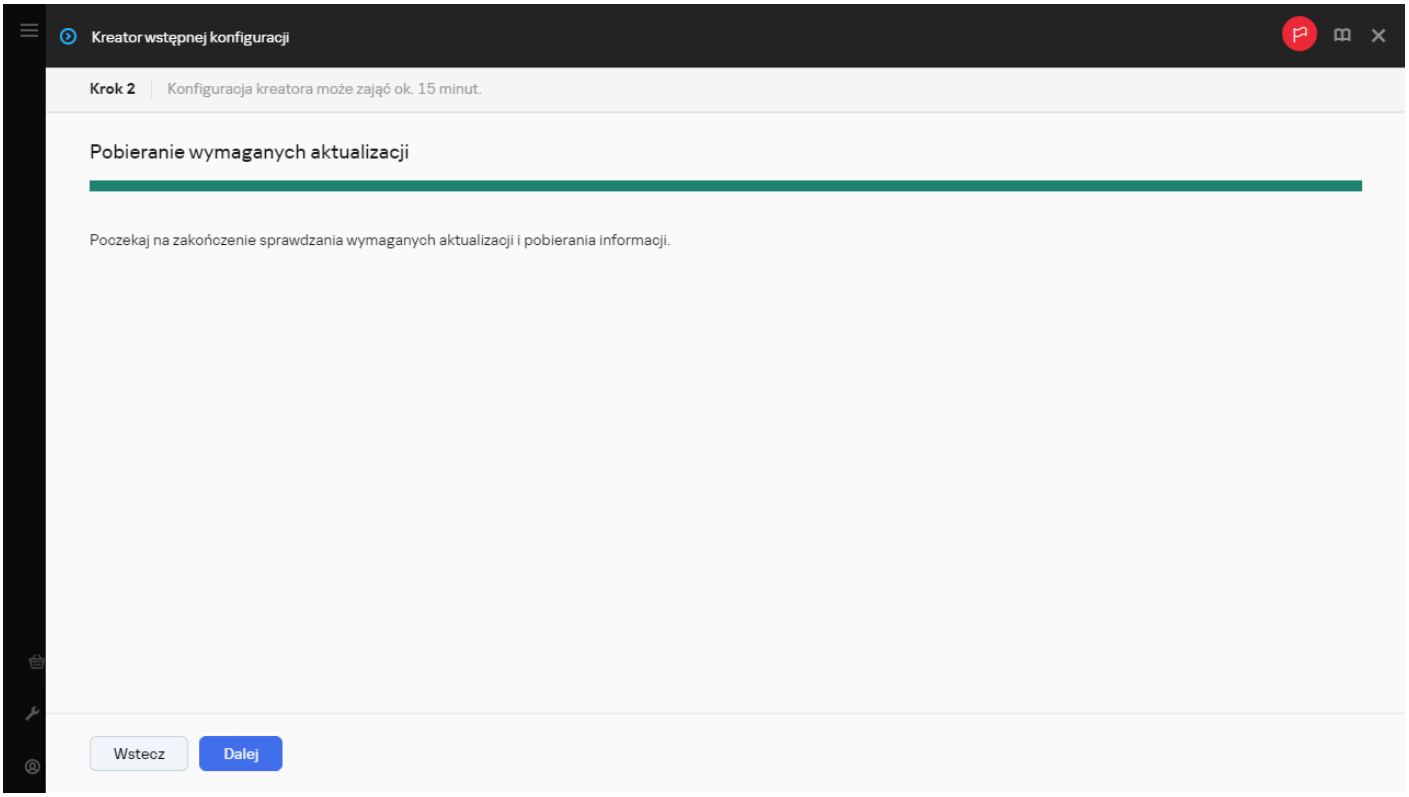
  Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

  Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

Możesz skonfigurować dostęp do Internetu później, niezależnie od kreatora wstępnej konfiguracji.

Krok 2. Pobieranie żądanych uaktualnień

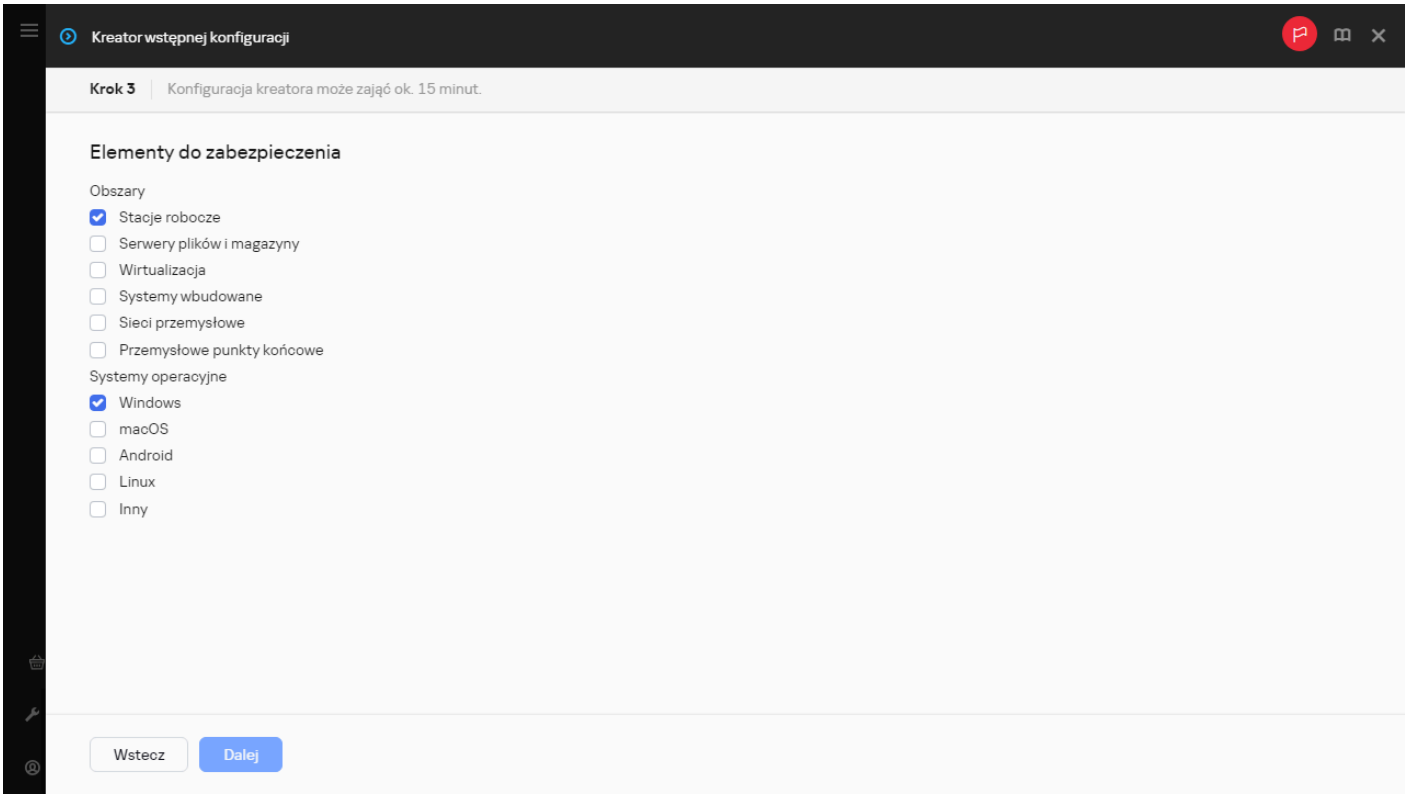
Wymagane aktualizacje są automatycznie pobierane z serwerów Kaspersky.



Pobieranie żądanych uaktualnień

Krok 3. Wybór elementów do zabezpieczenia

Wybierz obszary ochrony i systemy operacyjne używane w Twojej sieci. Jeśli wybierzesz te opcje, określ filtry dla wtyczek zarządzających aplikacjami i pakietami dystrybucyjnymi na serwerach Kaspersky, które możesz pobrać do zainstalowania na urządzeniach klienckich w Twojej sieci.



Wybór elementów do zabezpieczenia

Wybierz opcje:

- **Obszary**

  Możesz wybrać następujące obszary ochrony:

  - **Stacje robocze**. Wybierz tę opcję, jeśli chcesz chronić stacje robocze w swojej sieci. Domyślnie zaznaczona jest opcja Stacja robocza.
  - **Serwery plików i magazyny**. Wybierz tę opcję, jeśli chcesz chronić serwery plików w swojej sieci.
  - **Urządzenia mobilne**. Wybierz tę opcję, jeśli chcesz chronić urządzenia mobilne należące do firmy lub pracowników firmy. Jeśli wybierzesz tę opcję, ale nie dostarczyłeś licencji z funkcją Zarządzanie urządzeniami mobilnymi, zostanie wyświetlona wiadomość informująca o konieczności dostarczenia licencji z funkcją Zarządzanie urządzeniami mobilnymi. Jeśli nie dostarczysz licencji, nie możesz korzystać z funkcji Urządzenia mobilne.
  - **Wirtualizacja**. Wybierz tę opcję, jeśli chcesz chronić maszyny wirtualne w swojej sieci.
  - **Kaspersky Anti-Spam**. Wybierz tę opcję, jeśli chcesz chronić serwery pocztowe w swojej organizacji przed spamem, szkodliwymi programami i oszukańczymi wiadomościami.
  - **Systemy wbudowane**. Wybierz tę opcję, jeśli chcesz chronić wbudowane systemy Windows, takie jak bankomat.

- **Sieci przemysłowe**. Wybierz tę opcję, jeśli chcesz monitorować dane bezpieczeństwa w sieci przemysłowej oraz z punktów końcowych sieci, które są chronione przez aplikacje firmy Kaspersky.
- **Przemysłowe punkty końcowe**. Wybierz tę opcję, jeśli chcesz chronić pojedyncze węzły w sieci przemysłowej.

- **Systemy operacyjne**

  Możesz wybrać następujące platformy:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Inne

  Aby uzyskać informacje na temat obsługiwanych systemów operacyjnych, zobacz Wymagania sprzętowe i programowe dla Kaspersky Security Center Web Console.

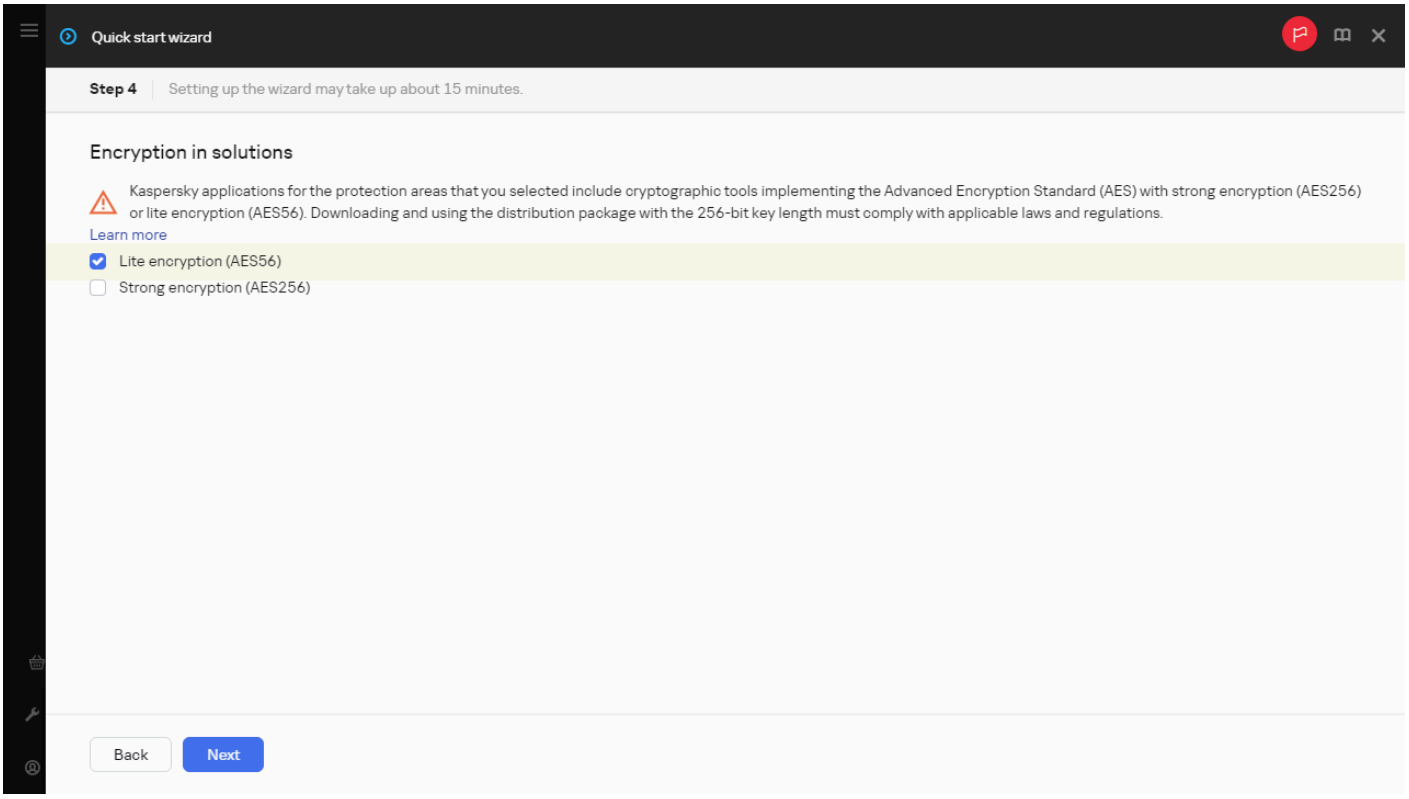
Możesz wybrać pakiety aplikacji Kaspersky z listy dostępnych pakietów później, niezależnie od kreatora wstępnej konfiguracji. Aby uprościć wyszukiwanie potrzebnych pakietów, możesz filtrować listę dostępnych pakietów według różnych kryteriów.

Krok 4. Wybieranie szyfrowania w rozwiązaniach

Okno **Szyfrowanie w rozwiązaniach** jest wyświetlane tylko wtedy, gdy wybrano **Stacje robocze** jako obszar ochrony.

Kaspersky Endpoint Security for Windows zawiera narzędzia do szyfrowania informacji przechowywanych na urządzeniach klienckich z systemem Windows. Te narzędzia szyfrujące mają zaimplementowany standard Advanced Encryption Standard (AES) z kluczem o długości 256-bitowej lub 56-bitowej.

Pobieranie i korzystanie z pakietu dystrybucyjnego z kluczem o długości 256 bitów musi odbywać się zgodnie z obowiązującymi przepisami i regulacjami. Aby pobrać pakiet dystrybucyjny Kaspersky Endpoint Security for Windows potrzebny w Twojej organizacji, miej na uwadze ustawodawstwo kraju, w którym znajdują się urządzenia klienckie Twojej organizacji.



Wybieranie szyfrowania w rozwiązaniach

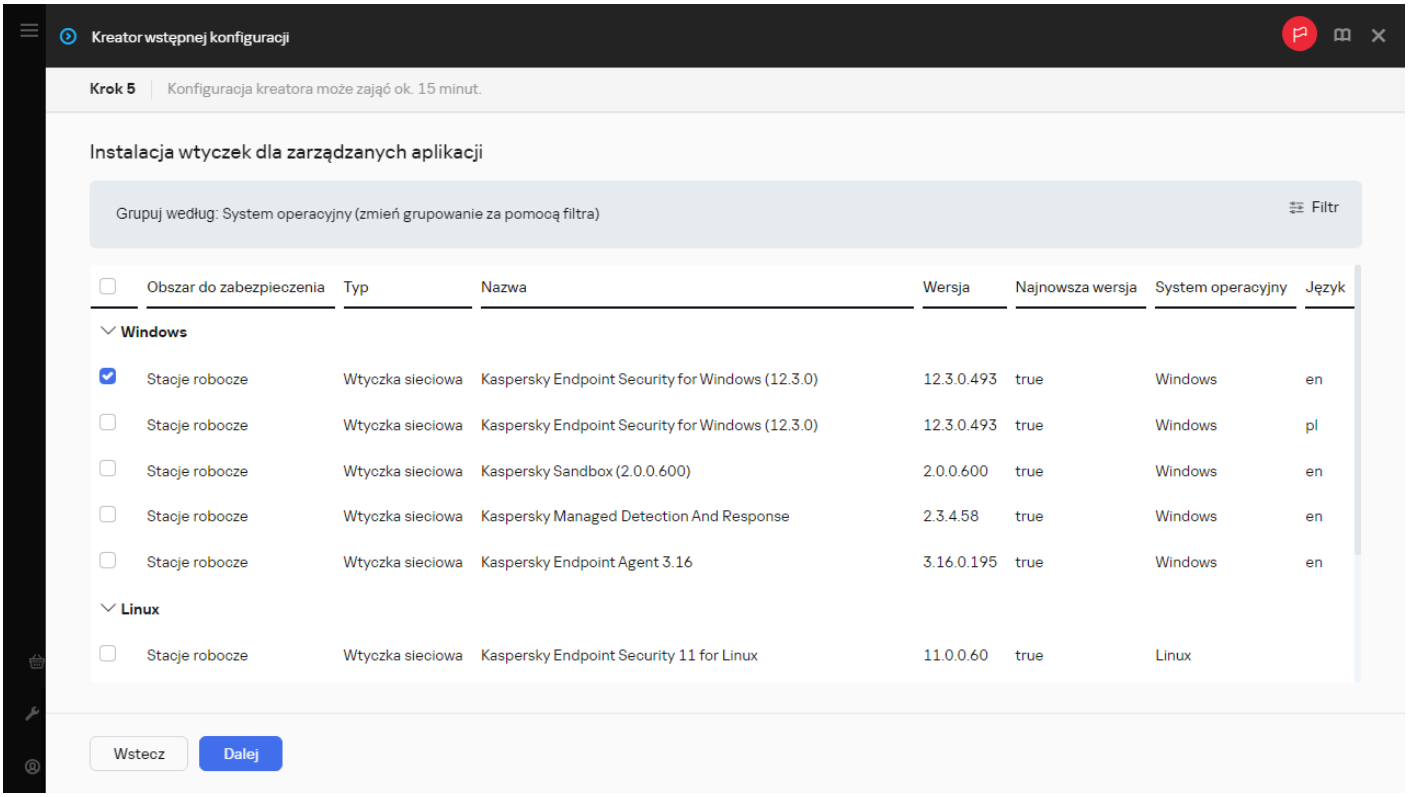
W oknie **Szyfrowanie w rozwiązaniach** wybierz jeden z następujących typów szyfrowania:

- Lite encryption (Szyfrowanie podstawowe). Ten typ szyfrowania używa klucza o długości 56 bitów.
- Strong encryption (Silne szyfrowanie). Ten typ szyfrowania używa klucza o długości 256 bitów.

Możesz wybrać pakiet dystrybucyjny dla Kaspersky Endpoint Security for Windows z wymaganym typem szyfrowania później, niezależnie od kreatora wstępnej konfiguracji.

Krok 5. Konfigurowanie instalacji wtyczek dla zarządzanych aplikacji

Wybierz wtyczki dla zarządzanych aplikacji, które mają zostać zainstalowane. Zostanie wyświetlona lista wtyczek znajdujących się na serwerach Kaspersky. Lista jest filtrowana zgodnie z opcjami wybranymi w poprzednim kroku kreatora. Domyślnie, pełna lista zawiera wtyczki we wszystkich językach. Aby wyświetlić tylko wtyczkę w określonym języku, użyj filtru.



Instalacja wtyczek dla zarządzanych aplikacji

Lista wtyczek zawiera następujące kolumny:

- **Obszar do zabezpieczenia**

  W tej kolumnie wyświetlane są wybrane obszary do zabezpieczenia.

- **Typ**

  W tej kolumnie wyświetlane są typy wtyczek.

- **Nazwa**

  Zostały wybrane wtyczki zależne od obszarów ochrony i platform, które wybrano w poprzednim kroku.

- **Wersja**

  Lista zawiera wtyczki we wszystkich wersjach umieszczone na serwerach Kaspersky. Domyślnie zostaną wybrane wtyczki w najnowszych wersjach.

- **Najnowsza wersja**

  Ta kolumna wskazuje, czy wersja wtyczki jest najnowsza. Jeśli wyświetlana jest wartość **true**, odpowiednia wtyczka posiada najnowszą wersję. Jeśli wyświetlana jest wartość **false**, odpowiednia wtyczka posiada starszą wersję.

- **System operacyjny**

  W tej kolumnie wyświetlane są systemy operacyjne wtyczek.

- **Język**

  Domyślnie wersja językowa wtyczki jest definiowana przez wersję językową Kaspersky Security Center, którą wybrałeś w momencie instalacji. Możesz określić inne wersje językowe na liście rozwijalnej **Wskaż język dla Konsoli administracyjnej lub**.

Po wybraniu wtyczek kliknij przycisk **Dalej**, aby rozpocząć instalację.

Wtyczki administracyjne dla aplikacji Kaspersky można zainstalować ręcznie, niezależnie od kreatora wstępnej konfiguracji.

Kreator wstępnej konfiguracji automatycznie instaluje wybrane wtyczki. Aby zainstalować niektóre wtyczki, należy zaakceptować warunki Umowy licencyjnej użytkownika końcowego. Zapoznaj się z treścią wyświetlonej Umowy licencyjnej użytkownika końcowego, zaznacz pole **Zgadzam się na korzystanie z Kaspersky Security Network** i kliknij przycisk **Zainstaluj**. Jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego, wtyczka nie zostanie zainstalowana.

Po zainstalowaniu wszystkich wybranych wtyczek Kreator wstępnej konfiguracji automatycznie przeniesie Cię do następnego kroku.

Krok 6. Instalowanie wybranych wtyczek

Kreator wstępnej konfiguracji automatycznie instaluje wtyczki wybrane w poprzednim kroku. Aby zainstalować niektóre wtyczki, należy zaakceptować warunki Umowy licencyjnej użytkownika końcowego. Zapoznaj się z treścią wyświetlonej Umowy licencyjnej użytkownika końcowego, zaznacz pole **Zgadzam się na korzystanie z Kaspersky Security Network** i kliknij przycisk **Zainstaluj**. Jeśli nie akceptujesz warunków Umowy licencyjnej użytkownika końcowego, wtyczka nie zostanie zainstalowana.

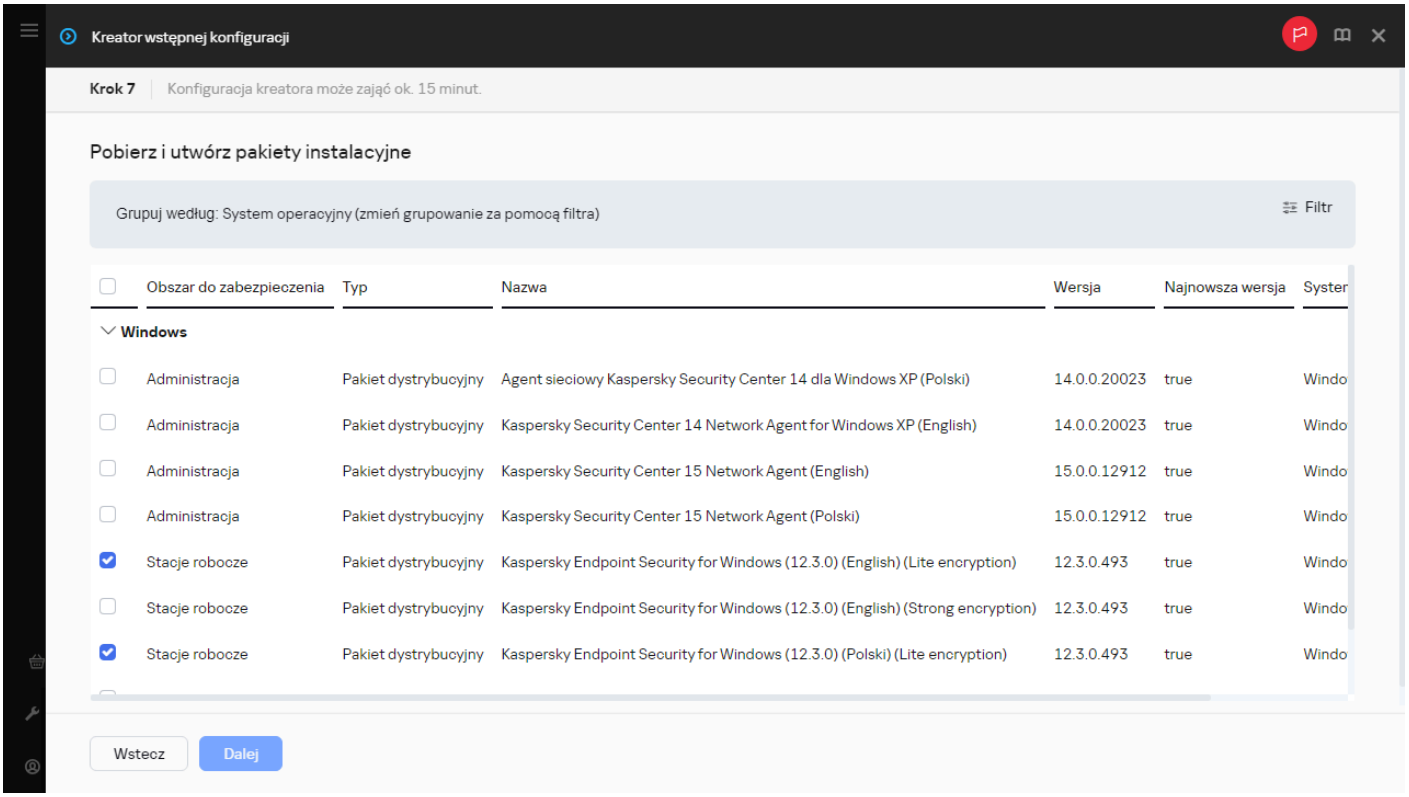
Po zainstalowaniu wszystkich wybranych wtyczek Kreator wstępnej konfiguracji automatycznie przeniesie Cię do następnego kroku.

Krok 7. Pobieranie pakietów dystrybucyjnych i tworzenie pakietów instalacyjnych

Wybierz pakiety dystrybucyjne do pobrania.

Dystrybutory zarządzanych aplikacji mogą wymagać zainstalowania określonej minimalnej wersji Kaspersky Security Center.

Po wybraniu typu szyfrowania dla Kaspersky Endpoint Security for Windows, zostanie wyświetlona lista pakietów dystrybucyjnych obu typów szyfrowania. Pakiet dystrybucyjny z wybranym typem szyfrowania zostanie wybrany z listy. Możesz wybrać pakiety dystrybucyjne dowolnego typu szyfrowania. Język pakietu dystrybucyjnego odpowiada językowi Kaspersky Security Center. Jeśli wersja językowa pakietu dystrybucyjnego Kaspersky Endpoint Security for Windows dla Kaspersky Security Center nie istnieje, zostanie wybrana angielska wersja językowa pakietu dystrybucyjnego.



Pobieranie pakietów dystrybucyjnych i tworzenie pakietów instalacyjnych

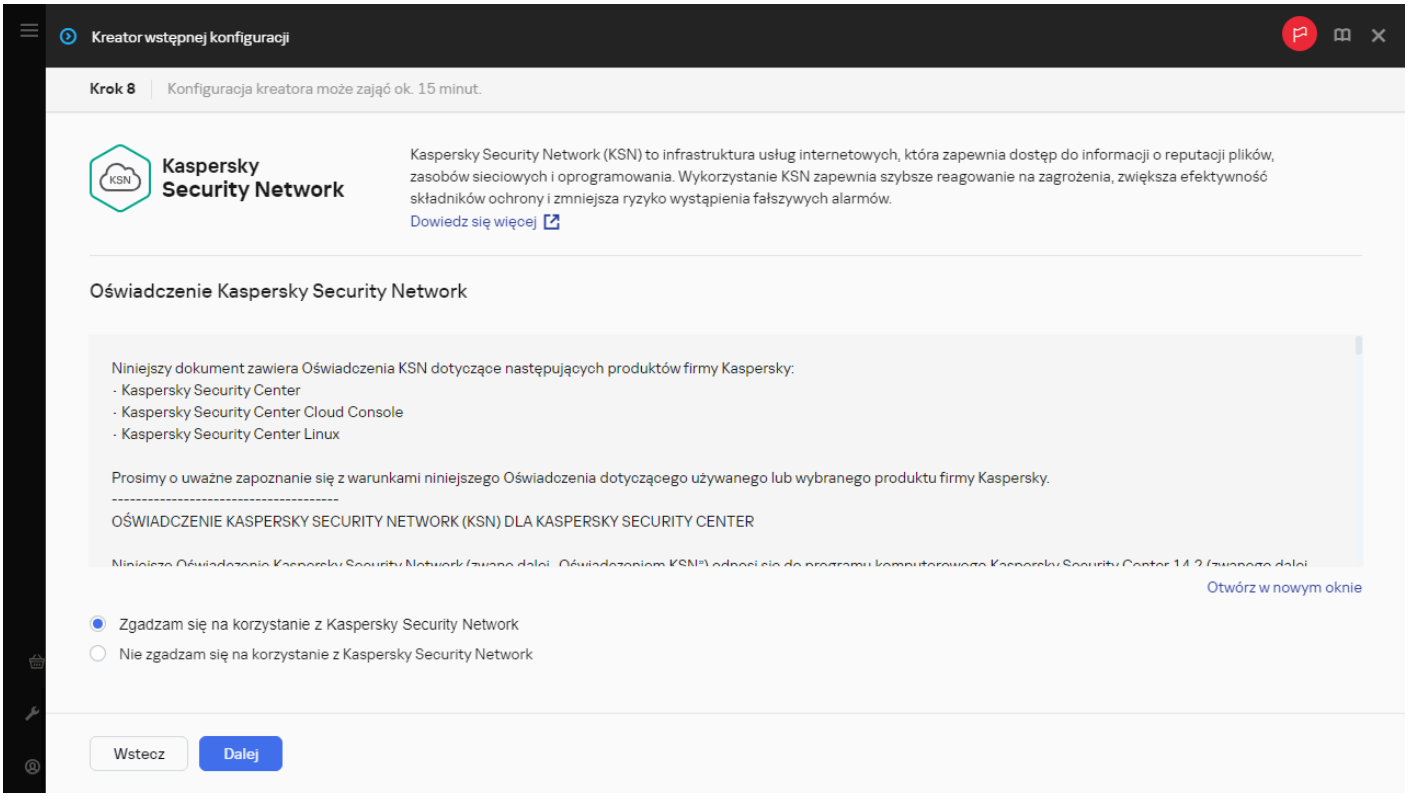
Aby zakończyć pobieranie niektórych pakietów dystrybucyjnych, należy zaakceptować Umowę licencyjną użytkownika końcowego. Jeśli klikniesz przycisk **Zaakceptuj**, zostanie wyświetlona treść Umowy licencyjnej użytkownika końcowego. Aby przejść do kolejnego kroku kreatora, należy zaakceptować warunki i postanowienia Umowy licencyjnej użytkownika końcowego oraz warunki i postanowienia Polityki prywatności Kaspersky. Jeśli nie akceptujesz warunków i postanowień, pobieranie pakietu zostanie anulowane.

Po zaakceptowaniu warunków i postanowień Umowy licencyjnej użytkownika końcowego oraz warunków i postanowień Polityki prywatności Kaspersky, pobieranie pakietów dystrybucyjnych będzie kontynuowane. W późniejszym czasie możesz wykorzystać pakiety instalacyjne do wdrożenia aplikacji Kaspersky na urządzeniach klienckich.

Możesz pobrać pakiety dystrybucyjne i utworzyć pakiety instalacyjne później, niezależnie od kreatora wstępnej konfiguracji.

Krok 8. Konfigurowanie Kaspersky Security Network

Określ ustawienia przekazywania informacji o działaniach Kaspersky Security Center do bazy wiedzy Kaspersky Security Network.



Konfigurowanie Kaspersky Security Network

Wybierz jedną z następujących opcji:

- **Zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje zainstalowane na urządzeniach klienckich automatycznie prześlą szczegóły swoich działań do Kaspersky Security Network. Uczestnictwo w Kaspersky Security Network umożliwia szybsze aktualizowanie baz danych zawierających informacje o wirusach i innych zagrożeniach, co zapewnia szybszą reakcję na pojawiające się zagrożenia bezpieczeństwa.

- **Nie zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje nie dostarczą informacji do Kaspersky Security Network.

  Jeśli wybierzesz tę opcję, korzystanie z Kaspersky Security Network zostanie wyłączone.

Możesz skonfigurować dostęp do Kaspersky Security Network (KSN) później, niezależnie od kreatora wstępnej konfiguracji.

Krok 9. Wybieranie metody aktywacji aplikacji

Wybierz jedną z poniższych opcji aktywacji Kaspersky Security Center:

- **Wprowadzając kod aktywacyjny**

  Kod aktywacyjny to unikatowa sekwencja 20 znaków alfanumerycznych. Możesz wprowadzić kod aktywacyjny w celu dodania klucza aktywującego Kaspersky Security Center. Możesz otrzymać kod aktywacyjny na adres e-mail, który określiłeś po zakupieniu Kaspersky Security Center.

  Aby aktywować aplikację za pomocą kodu aktywacyjnego, potrzebny jest dostęp do internetu w celu nawiązania połączenia z serwerami aktywacji Kaspersky.

  Jeśli wybrano tę opcję aktywacji, możesz włączyć opcję **Automatycznie roześlij klucz licencyjny do zarządzanych urządzeń**.

  Jeśli ta opcja jest włączona, klucz licencyjny zostanie automatycznie zainstalowany na zarządzanych urządzeniach.

  Jeśli ta opcja jest wyłączona, możesz wdrożyć klucz licencyjny na zarządzanych urządzeniach później, w węźle **Licencje Kaspersky** drzewa Konsoli administracyjnej.

- **Określając plik klucza**

  Plik klucza to plik z rozszerzeniem .key, dostarczony przez firmę Kaspersky. Plik klucza jest przeznaczony do dodania klucza aktywującego aplikację.

  Metody uzyskiwania pliku klucza opisano w poniższej sekcji: O pliku klucza.

  Aby aktywować aplikację przy pomocy pliku klucza, nie musisz łączyć się z serwerami aktywacji Kaspersky.

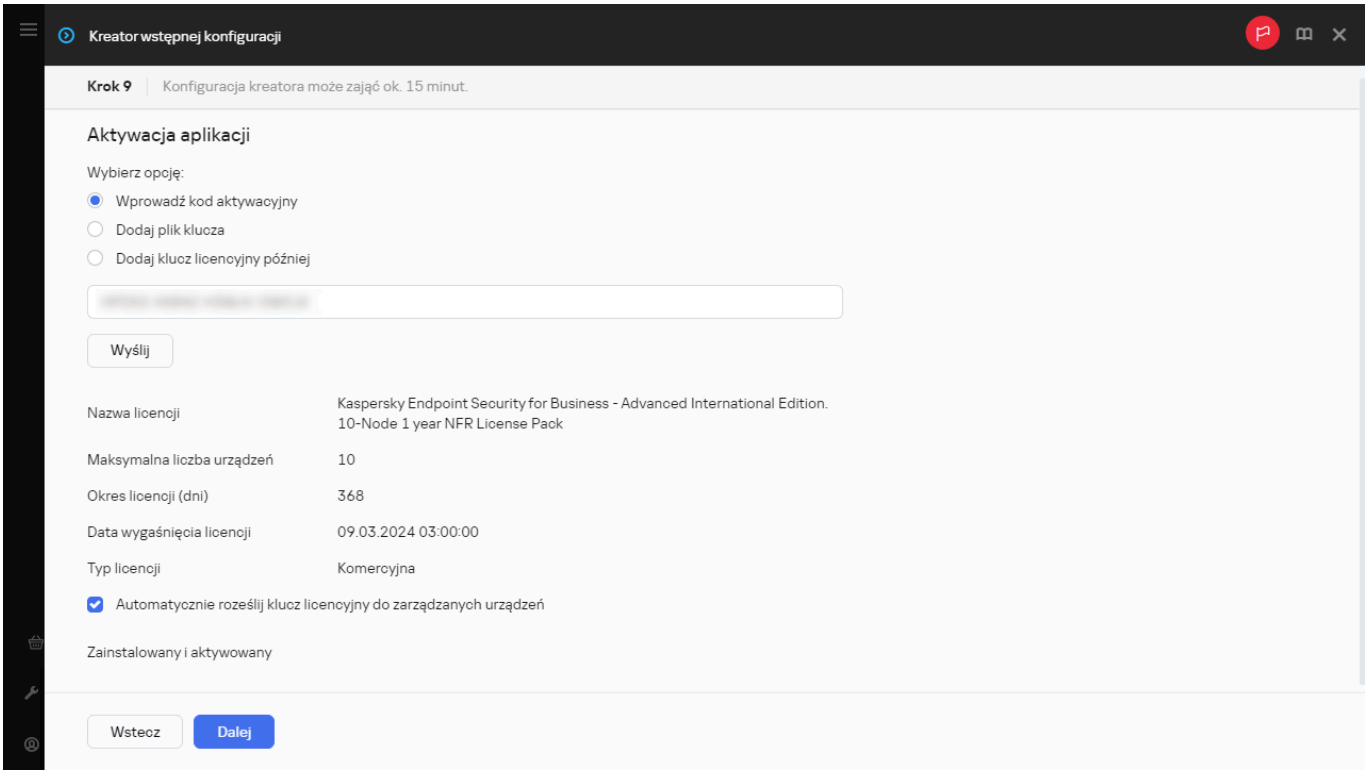
  Jeśli wybrano tę opcję aktywacji, możesz włączyć opcję **Automatycznie roześlij klucz licencyjny do zarządzanych urządzeń**.

  Jeśli ta opcja jest włączona, klucz licencyjny zostanie automatycznie zainstalowany na zarządzanych urządzeniach.

  Jeśli ta opcja jest wyłączona, możesz wdrożyć klucz licencyjny na zarządzanych urządzeniach później, w węźle **Licencje Kaspersky** drzewa Konsoli administracyjnej.

- **Odraczając aktywację aplikacji**

  Aplikacja będzie działała z podstawową funkcjonalnością, bez Zarządzania urządzeniami mobilnymi oraz bez Zarządzania systemami.



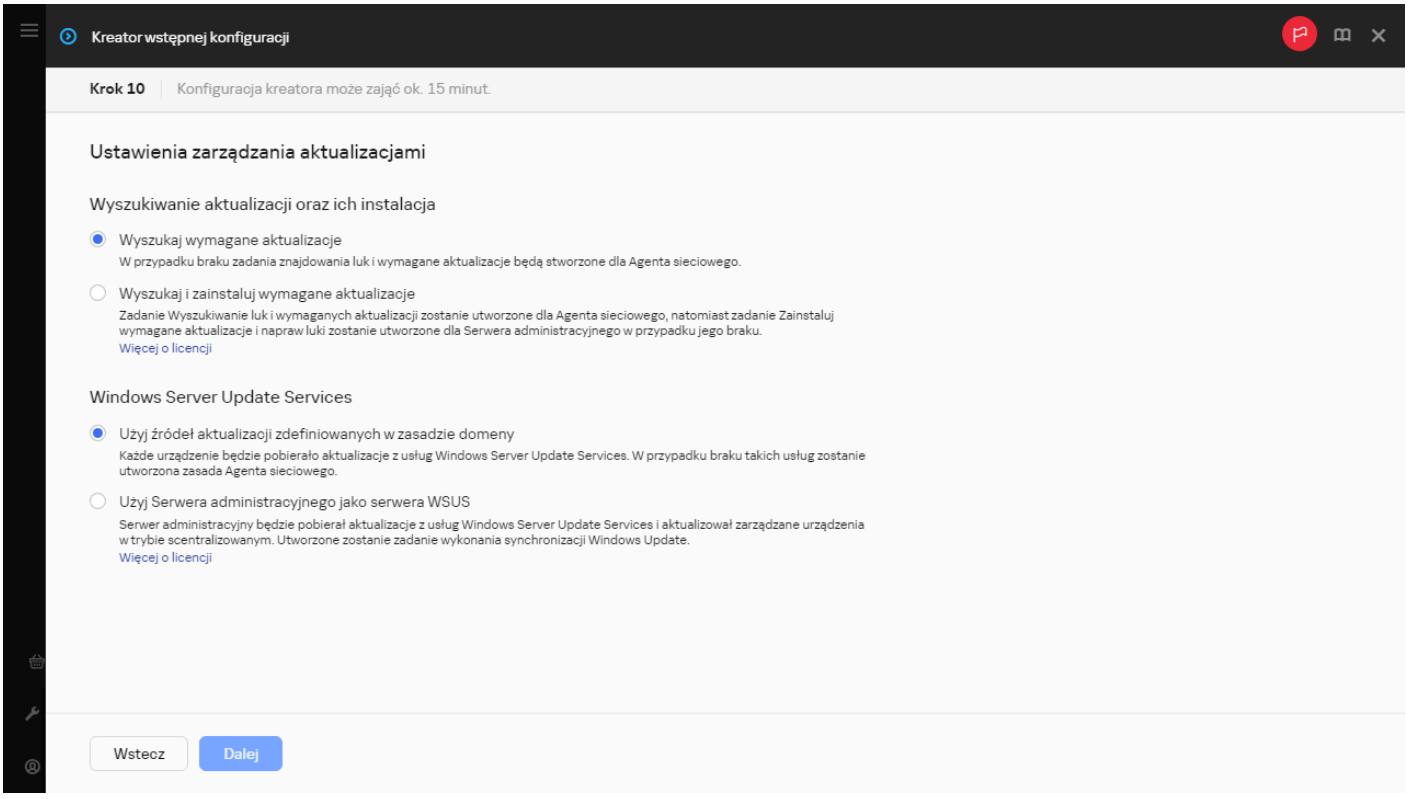
Wybieranie metody aktywacji aplikacji

Jeśli wybierzesz opcję odroczenia aktywacji aplikacji, będziesz mógł dodać klucz licencyjny w późniejszym czasie, wybierając **Operacje** → **Licencjonowanie**.

Podczas pracy z Kaspersky Security Center wdrożonym z płatnego obrazu AMI lub dla Usage-based monthly billed SKU nie można określić pliku klucza ani wprowadzić kodu.

Krok 10. Określanie ustawień zarządzania aktualizacjami firm trzecich

Ten krok nie jest wyświetlany, jeśli nie posiadasz licencji Zarządzanie lukami i poprawkami, a zadanie *Wyszukiwanie luk i wymaganych aktualizacji* już istnieje.



Ustawienia zarządzania aktualizacjami firm trzecich

Dla aktualizacji oprogramowania innych firm wybierz jedną z następujących opcji:

- **Wyszukaj wymagane aktualizacje**

  Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie, jeśli ich nie ma.

  Opcja ta jest wybrana domyślnie.

- **Wyszukaj i zainstaluj wymagane aktualizacje**

  Zadania *Wyszukiwanie luk i wymaganych aktualizacji* i *Zainstaluj wymagane aktualizacje i napraw luki* są tworzone automatycznie, jeśli ich nie ma.

  Ta opcja jest dostępna tylko w ramach licencji na Zarządzanie lukami i poprawkami.

Dla aktualizacji Windows Update wybierz jedną z następujących opcji:

- **Użyj źródeł aktualizacji zdefiniowanych w zasadzie domeny**

  Urządzenia klienckie pobiorą aktualizacje Windows Update zgodnie z ustawieniami zasad domeny. Zasada Agenta sieciowego jest tworzona automatycznie, jeśli jeszcze jej nie masz.

- **Użyj Serwera administracyjnego jako serwera WSUS**

  Urządzenia klienckie pobiorą aktualizacje Windows Update z Serwera administracyjnego. Zadanie *Wykonaj synchronizację Windows Update* i zasada Agenta sieciowego są tworzone automatycznie, jeśli jeszcze ich nie masz.

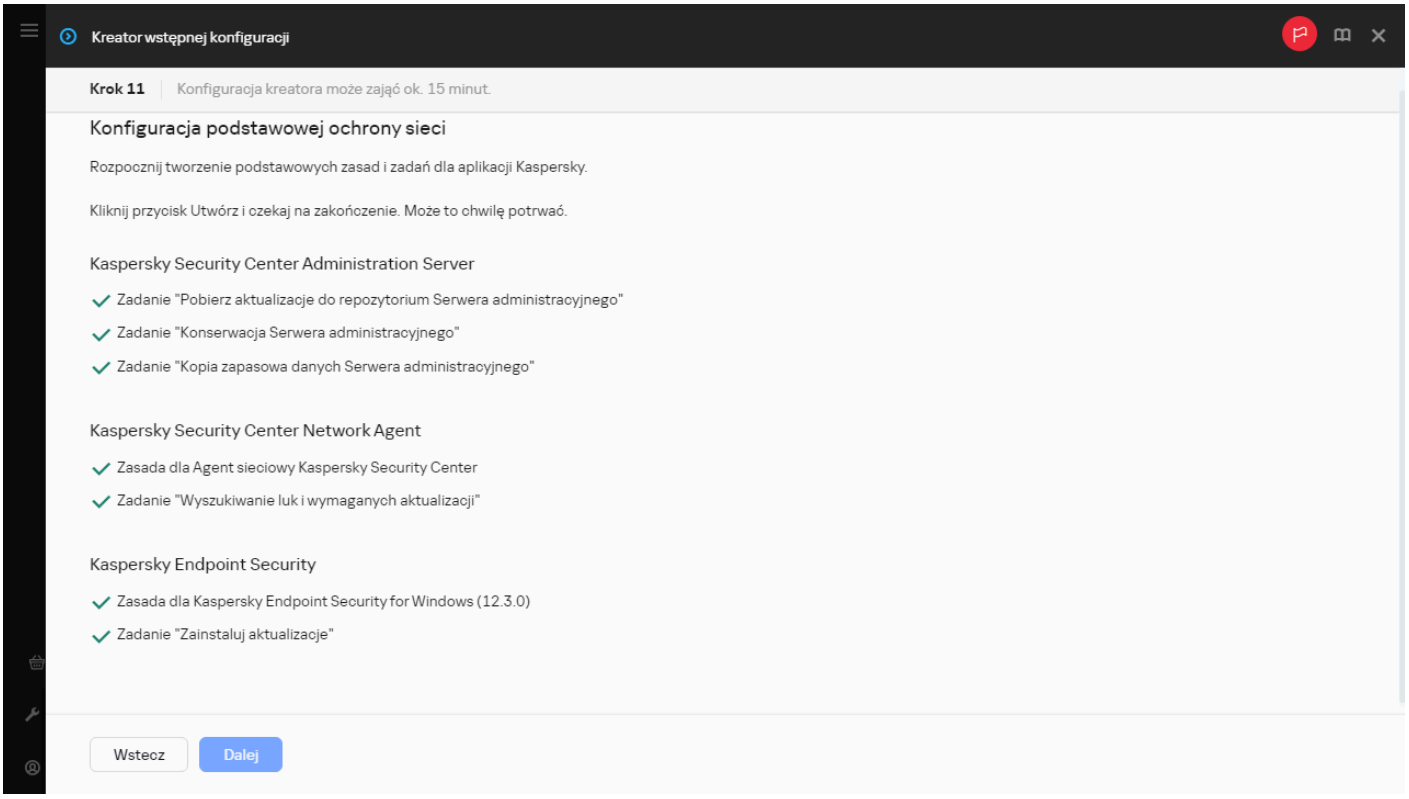
  Ta opcja jest dostępna tylko w ramach licencji na Zarządzanie lukami i poprawkami.

Zadania *Wyszukiwanie luk i wymaganych aktualizacji* oraz *Zainstaluj wymagane aktualizacje i napraw luki* możesz utworzyć niezależnie od kreatora wstępnej konfiguracji. Aby użyć Serwera administracyjnego jako serwera WSUS, utwórz zadanie *Wykonaj synchronizację Windows Update* i wybierz opcję **Użyj Serwera administracyjnego jako serwera WSUS** w zasadzie Agenta sieciowego.

Krok 11. Tworzenie podstawowej konfiguracji ochrony sieci

Możesz sprawdzić listę utworzonych zasad i zadań.

Przed przystąpieniem do następnego kroku kreatora poczekaj na zakończenie tworzenia zasad i zadań.

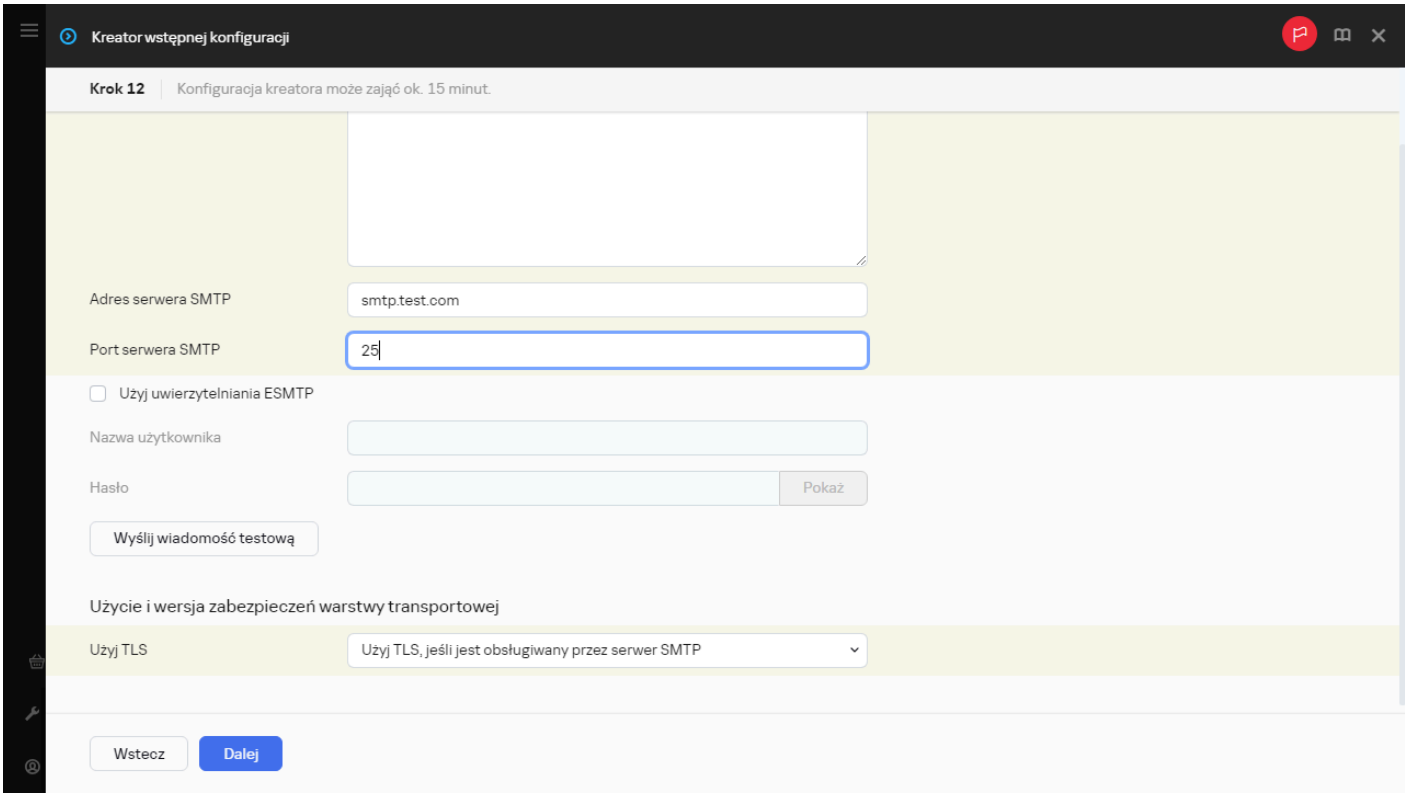


Tworzenie podstawowej konfiguracji ochrony sieci

Możesz utworzyć wymagane zadania i zasady później, niezależnie od kreatora wstępnej konfiguracji.

Krok 12. Konfigurowanie powiadomień e-mail

Skonfiguruj dostarczanie powiadomień o zdarzeniach zarejestrowanych podczas działania aplikacji firmy Kaspersky na urządzeniach klienckich. Ustawienia te będą używane jako ustawienia domyślne dla zasad aplikacji.



Konfigurowanie powiadomień e-mail

W celu skonfigurowania dostarczania powiadomień o zdarzeniach występujących w aplikacjach firmy Kaspersky użyj następujących ustawień:

- **Adresaci (adresy e-mail)**

  Adresy e-mail użytkowników, którym aplikacja będzie wysyłała powiadomienia. Możesz wprowadzić jeden lub więcej adresów; jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami.

- **Adres serwera SMTP**

  Adres lub adresy serwerów pocztowych Twojej organizacji.

  Jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami. Możesz użyć następujących wartości:

  - Adres IPv4 lub IPv6
  - Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
  - Nazwa DNS serwera SMTP

- **Port serwera SMTP**

  Numer portu komunikacji serwera SMTP. Jeśli korzystasz z kilku serwerów SMTP, połączenie z nimi jest nawiązywane przez określony port komunikacyjny. Domyślny numer portu to 25.

- **Użyj uwierzytelniania ESMTP**

  Włącza obsługę autoryzacji ESMTP. Po zaznaczeniu opcji, w polach **Nazwa użytkownika** i **Hasło** możesz określić ustawienia autoryzacji ESMTP. Domyślnie pole to nie jest zaznaczone.

- **Użyj TLS**

  Możesz określić ustawienia TLS połączenia z serwerem SMTP:

  - **Nie używaj TLS**

    Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.

  - **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

    Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.

  - **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**

    Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

    > Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

    Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

  Możesz określić certyfikat dla połączenia TLS, klikając odnośnik **Określ certyfikaty**:

  - Odszukaj plik certyfikatu serwera SMTP:

    Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

  - Odszukaj plik certyfikatu klienta:

    Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

    - Certyfikat X-509:

      Musisz określić plik z certyfikatem oraz plik z kluczem prywatnym. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po załadowaniu obu plików należy określić hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

    - Kontener pkcs12:

      Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

Możesz przetestować nowe ustawienia powiadomień e-mail, klikając przycisk **Wyślij wiadomość testową**.

Możesz skonfigurować powiadomienia o zdarzeniach później, niezależnie od kreatora wstępnej konfiguracji.

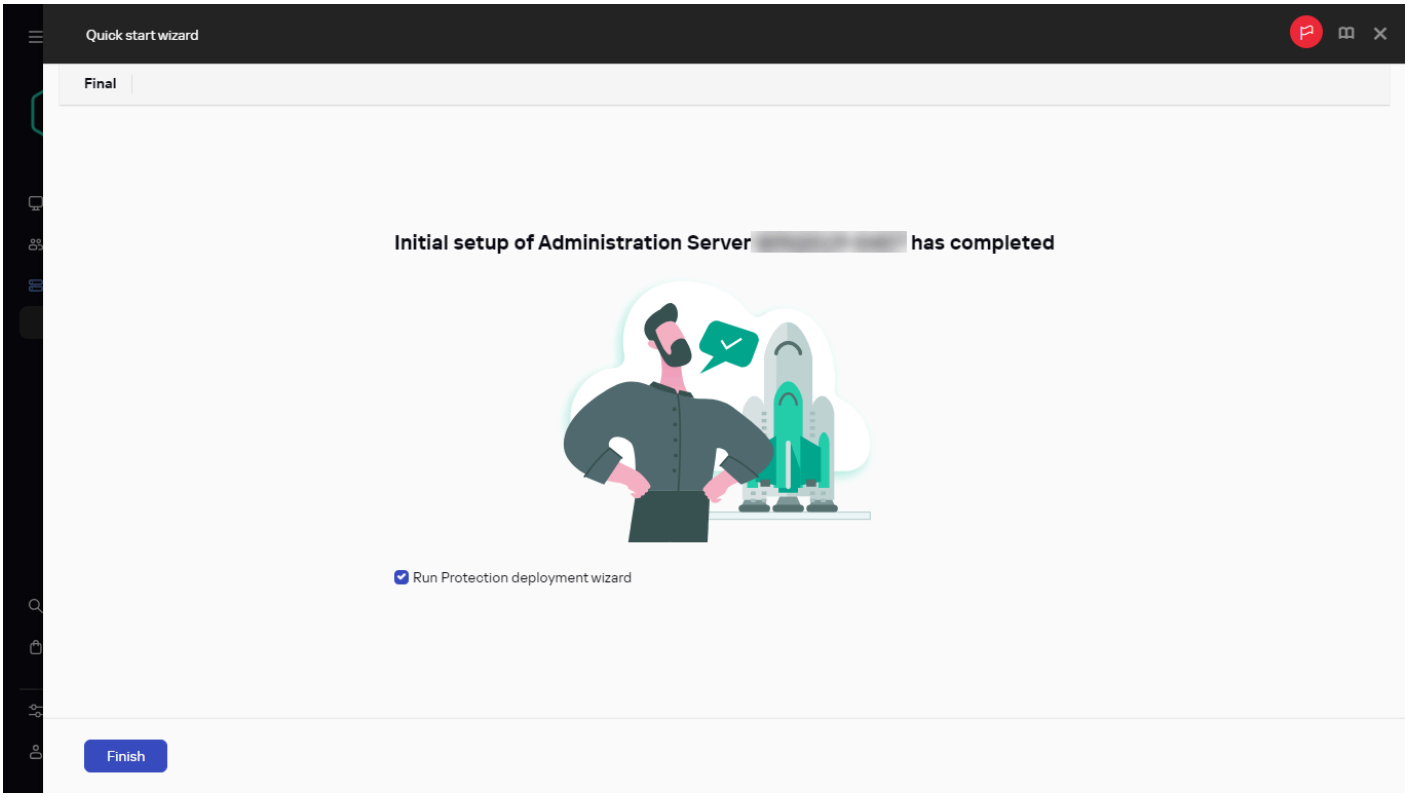
Krok 13. Przeprowadzanie przeszukiwania sieci

Serwer administracyjny przeprowadzi wstępne przeszukiwanie. Podczas przeszukiwania wyświetlany jest pasek postępu. Po zakończeniu przeszukiwania, odnośnik **Wyświetl wykryte urządzenia** stanie się dostępny. Możesz kliknąć ten odnośnik, aby przejrzeć urządzenia w sieci wykryte przez Serwer administracyjny. Aby wrócić do kreatora wstępnej konfiguracji, wciśnij klawisz **Escape**.

Możesz wykonać przeszukiwanie sieci później, niezależnie od kreatora wstępnej konfiguracji. Użyj Kaspersky Security Center Web Console, aby skonfigurować przeszukiwanie kontrolera domen, domen Windows, zakresów IP i sieci IPv6.

Krok 14. Zamykanie kreatora wstępnej konfiguracji

W oknie zakończenia pracy Kreatora wstępnej konfiguracji zaznacz pole **Uruchom Kreatora wdrażania ochrony**, jeśli chcesz uruchomić automatyczną instalację aplikacji antywirusowych lub Agenta sieciowego na urządzeniach w sieci.



Ostatni krok Kreatora wstępnej konfiguracji

Aby zamknąć kreator, kliknij przycisk **Zakończ**.

Podłączanie urządzeń mobilnych

Ta sekcja opisuje sposób podłączania zarządzanych urządzeń mobilnych (czyli zarządzanych urządzeń znajdujących się poza siecią główną) z Serwerem administracyjnym.

Scenariusz: Podłączanie urządzeń mobilnych przez bramę połączenia

W tym scenariuszu opisano sposób podłączania zarządzanych urządzeń znajdujących się poza siecią główną z Serwerem administracyjnym.

Wymagania wstępne

Scenariusz ma następujące wymagania wstępne:

- Strefa zdemilitaryzowana (DMZ) jest zorganizowana w sieci Twojej organizacji.
- Serwer administracyjny Kaspersky Security Center jest zainstalowany w sieci firmowej.

Etapy

Ten scenariusz przebiega etapami:

1. **Wybieranie urządzenia kliencka w DMZ**

   To urządzenie zostanie użyte jako brama połączenia. Urządzenie, które wybrałeś, musi spełniać wymagania dla bram połączenia.

2. **Instalowanie Agenta sieciowego w roli bramy połączenia**

   Do zainstalowania Agenta sieciowego na wybranym urządzeniu zalecane jest używanie instalacji lokalnej.

   Domyślnie plik instalacyjny znajduje się w następującym miejscu: \\<nazwa serwera>\KLSHARE\PkgInst\NetAgent_<numer wersji>

   W oknie **Brama połączenia** kreatora instalacji Agenta sieciowego wybierz **Użyj Agenta sieciowego jako bramy połączenia w DMZ**. Ten tryb jednocześnie aktywuje rolę bramy połączenia i nakazuje Agentowi sieciowemu czekać na połączenia z Serwera administracyjnego zamiast nawiązywać połączenia z Serwerem administracyjnym.

   Alternatywnie możesz zainstalować Agenta sieciowego na urządzeniu z systemem Linux i skonfigurować Agenta sieciowego do pracy jako brama połączenia, ale zwróć uwagę na listę ograniczeń Agenta sieciowego działającego na urządzeniach z systemem Linux.

3. **Zezwalanie na połączenia w zaporach sieciowych w bramie połączenia**

   Aby upewnić się, że Serwer administracyjny może faktycznie połączyć się z bramą połączenia w strefie DMZ, zezwolić na połączenia z portem TCP o numerze 13000 we wszystkich zaporach ogniowych między Serwerem administracyjnym a bramą połączenia.

   Jeśli brama połączenia nie ma rzeczywistego adresu IP w Internecie, ale zamiast tego znajduje się poza NAT (Network Address Translation — translacja adresów sieciowych), skonfiguruj regułę, aby przekazywać połączenia przez NAT.

4. **Tworzenie grupy administracyjnej dla urządzeń zewnętrznych**

   Utwórz nową grupę w grupie **Zarządzane urządzenia**. Ta nowa grupa będzie zawierała zewnętrzne zarządzane urządzenia.

5. **Podłączanie bramy połączenia do Serwera administracyjnego**

   Brama połączenia, którą skonfigurowałeś, oczekuje na połączenie z Serwera administracyjnego. Jednakże Serwer administracyjny nie wyświetla urządzenia z bramą połączenia wśród zarządzanych urządzeń. Dzieje się tak ponieważ brama połączenia nie próbowała nawiązać połączenia z Serwerem administracyjnym. Dlatego też należy przeprowadzić specjalną procedurę w celu zapewnienia, że Serwer administracyjny zainicjuje połączenie z bramą połączenia.

   Wykonaj następujące czynności:

   1. Dodaj bramę połączenia jako punkt dystrybucji.
   2. Przenieś bramę połączenia z grupy **Urządzenia nieprzypisane** do grupy utworzonej dla urządzeń zewnętrznych.

   Brama połączenia została podłączona i skonfigurowana.

6. **Podłączanie zewnętrznych urządzeń stacjonarnych do Serwera administracyjnego**

   Zwykle zewnętrzne komputery stacjonarne nie są przenoszone wewnątrz granic. Dlatego musisz skonfigurować je tak, aby łączyły się z Serwerem administracyjnym przez bramę podczas instalowania Agenta sieciowego.

7. **Konfigurowanie aktualizacji dla zewnętrznych urządzeń stacjonarnych**

   Jeśli aktualizacje aplikacji zabezpieczających są skonfigurowane do pobierania z Serwera administracyjnego, urządzenia zewnętrzne pobierają aktualizacje przez bramę połączenia. Ma to dwie wady:

   - To niepotrzebny ruch, który zajmuje przepustowość kanału komunikacji internetowej firmy.
   - Niekoniecznie jest to najszybszy sposób uzyskiwania aktualizacji. Jest bardzo prawdopodobne, że pobieranie aktualizacji z serwerów aktualizacji Kaspersky byłoby tańsze i szybsze dla urządzeń zewnętrznych.

   Wykonaj następujące czynności:

   1. Przenieś wszystkie urządzenia zewnętrzne do oddzielnej grupy administracyjnej, którą utworzyłeś wcześniej.
   2. Wyklucz grupę z urządzeniami zewnętrznymi z zadania aktualizacji.
   3. Utwórz osobne zadanie aktualizacji dla grupy z urządzeniami zewnętrznymi.

8. **Podłączanie przenośnych laptopów do Serwera administracyjnego**

   Przenośne laptopy są czasami w sieci, a czasami poza nią. W celu efektywnego zarządzania należy połączyć je z Serwerem administracyjnym w różny sposób w zależności od ich lokalizacji. Aby efektywnie wykorzystywać ruch sieciowy, muszą również pobierać uaktualnienia z różnych źródeł w zależności od ich lokalizacji.

   Należy skonfigurować reguły dla użytkowników mobilnych: profile połączeń i opisy lokalizacji sieciowych. Każda reguła definiuje instancję Serwera administracyjnego, z którym muszą łączyć się przenośne laptopy w zależności od ich lokalizacji oraz instancji Serwera administracyjnego, z którego muszą pobierać aktualizacje.

Scenariusz: Połączanie urządzeń spoza biura poprzez podrzędny Serwer administracyjny w strefie DMZ

Jeśli chcesz podłączyć urządzenia zarządzane, które znajdują się poza główną siecią, do Serwera administracyjnego, można to zrobić za pomocą podrzędnego Serwera administracyjnego znajdującego się w strefie zdemilitaryzowanej (DMZ).

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- DMZ jest organizowana w sieci Twojej organizacji.
- Serwer administracyjny Kaspersky Security Center jest zlokalizowany w wewnętrznej sieci organizacji.

Etapy

Ten scenariusz przebiega etapami:

1. **Wybieranie urządzenia kliencka w DMZ**

   W DMZ wybierz urządzenie klienckie, które będzie używane jako podrzędny Serwer administracyjny.

2. **Instalowanie Serwera administracyjnego Kaspersky Security Center**

   Zainstaluj Serwer administracyjny Kaspersky Security Center na tym urządzeniu klienckim.

3. **Tworzenie hierarchii Serwerów administracyjnych**

   W przypadku umieszczenia podrzędnego Serwera administracyjnego w strefie DMZ, podrzędny Serwer administracyjny musi uzyskiwać połączenie z głównego Serwera administracyjnego. W tym celu należy dodać nowy Serwer administracyjny jako serwer podrzędny, tak, aby główny Serwer administracyjny łączył się z podrzędnym Serwerem administracyjnym poprzez port 13000. Podczas łączenia dwóch Serwerów administracyjnych w hierarchię upewnij się, że port 13299 jest dostępny na obu Serwerach administracyjnych. Kaspersky Security Center Web Console nawiązuje połączenie z Serwerem administracyjnym poprzez port 13299.

4. **Połączanie mobilnych urządzeń zarządzanych do podrzędnego Serwera administracyjnego**

   Urządzenia mobilne można połączyć z Serwerem administracyjnym w strefie DMZ w taki sam sposób, w jaki nawiązywane jest połączenie pomiędzy Serwerem administracyjnym i urządzeniami zarządzanymi zlokalizowanymi w sieci głównej. Mobilne urządzenia zarządzane inicjują połączenie poprzez port 13000.

Informacje o podłączaniu urządzeń mobilnych

Niektóre zarządzane urządzenia zawsze znajdują się poza główną siecią (na przykład, urządzenia w oddziałach regionalnych firmy; kioski, bankomaty i terminale zainstalowane w różnych punktach sprzedaży; urządzenia w domowych biurach pracowników). Niektóre urządzenia od czasu do czasu wyjeżdżają poza granicę (na przykład, laptopy użytkowników, którzy odwiedzają oddziały regionalne lub biuro klienta).

Nadal musisz monitorować i zarządzać ochroną urządzeń znajdujących się poza biurem - otrzymywać aktualne informacje o ich stanie ochrony i zapewniać aktualność aplikacji zabezpieczających. Jest to konieczne, ponieważ, na przykład, jeśli do takiego urządzenia ktoś się włamał, gdy znajdowało się poza siecią główną, może stać się platformą do rozprzestrzeniania zagrożeń, gdy tylko połączy się z siecią główną. W celu podłączenia urządzeń mobilnych do Serwera administracyjnego, możesz użyć dwóch metod:

- Brama połączenia w strefie zdemilitaryzowanej (DMZ)

  Zobacz schemat transmisji danych: Serwer administracyjny w sieci LAN, zarządzane urządzenia w internecie, używana brama połączenia

- Serwer administracyjny w strefie DMZ

  Zobacz schemat transmisji danych: Serwer administracyjny w strefie DMZ, zarządzane urządzenia w internecie

Brama połączenia w strefie DMZ

Zalecaną metodą podłączania urządzeń mobilnych do Serwera administracyjnego jest zorganizowanie strefy DMZ w sieci organizacji i zainstalowanie bramy połączenia w strefie DMZ. Urządzenia zewnętrzne nawiążą połączenie z bramą połączenia, a Serwer administracyjny znajdujący się w sieci zainicjuje połączenie z urządzeniami za pośrednictwem bramy połączenia.

W porównaniu z drugą metodą ta jest bezpieczniejsza:

- Nie musisz otwierać dostępu do Serwera administracyjnego spoza sieci.
- Uszkodzona brama połączenia nie stwarza dużego zagrożenia dla bezpieczeństwa urządzeń sieciowych. Brama połączeń w rzeczywistości sama niczym nie zarządza i nie ustanawia żadnych połączeń.

Ponadto brama połączeń nie wymaga wielu zasobów sprzętowych.

Jednakże ta metoda ma bardziej skomplikowany proces konfiguracji:

- Aby urządzenie służyło jako brama połączenia w DMZ, musisz zainstalować Agenta sieciowego i podłączyć go do Serwera administracyjnego w określony sposób.
- Nie będziesz mógł używać tego samego adresu do łączenia się z Serwerem administracyjnym we wszystkich sytuacjach. Poza granicami, będziesz musiał użyć nie tylko innego adresu (adresu bramy połączenia), ale także innego trybu połączenia: przez bramę połączenia.
- Musisz także zdefiniować różne ustawienia połączeń dla laptopów w różnych lokalizacjach.

Aby dodać bramę połączenia do wcześniej skonfigurowanej sieci:

1. Zainstaluj Agenta sieciowego w trybie bramy połączenia.
2. Ponownie zainstaluj Agenta sieciowego na urządzeniach, które chcesz połączyć z nowo dodaną bramą połączenia.

Serwer administracyjny w strefie DMZ

Inną metodą jest zainstalowanie pojedynczego Serwera administracyjnego w strefie DMZ.

Ta konfiguracja jest mniej bezpieczna niż inna metoda. Aby w tym przypadku zarządzać zewnętrznymi laptopami, Serwer administracyjny musi akceptować połączenia z dowolnego adresu w Internecie. Nadal będzie zarządzać wszystkimi urządzeniami w sieci wewnętrznej, ale z DMZ. Dlatego przejęty Serwer może spowodować ogromne szkody, pomimo niskiego prawdopodobieństwa takiego zdarzenia.

Ryzyko jest znacznie niższe, jeśli Serwer administracyjny w DMZ nie zarządza urządzeniami w sieci wewnętrznej. Taka konfiguracja może być wykorzystana, na przykład, przez usługodawcę do zarządzania urządzeniami klientów.

Możesz chcieć użyć tej metody w następujących przypadkach:

- Jeśli jesteś zaznajomiony z instalacją i konfiguracją Serwera administracyjnego i nie chcesz wykonywać innej procedury instalacji i konfiguracji bramy połączenia.
- Jeśli potrzebujesz zarządzać większą liczbą urządzeń. Maksymalna pojemność Serwera administracyjnego to 100 000 urządzeń, podczas gdy brama połączenia może obsługiwać do 10 000 urządzeń.

To rozwiązanie ma również możliwe trudności:

- Serwer administracyjny wymaga większej ilości zasobów sprzętowych i jeszcze jednej bazy danych.
- Informacje o urządzeniach będą przechowywane w dwóch niepowiązanych bazach danych (dla Serwera administracyjnego w sieci i jednej w DMZ), co komplikuje monitorowanie.
- Aby zarządzać wszystkimi urządzeniami, Serwer administracyjny musi być połączony w hierarchię, co komplikuje nie tylko monitorowanie, ale także zarządzanie. Instancja podrzędnego Serwera administracyjnego nakłada ograniczenia na możliwe struktury grup administracyjnych. Musisz zdecydować, w jaki sposób i które zadania i zasady mają być dystrybuowane do instancji podrzędnego Serwera administracyjnego.
- Skonfigurowanie urządzeń zewnętrznych do używania Serwera administracyjnego w DMZ z zewnątrz oraz do używania głównego Serwera administracyjnego od wewnątrz nie jest prostsze niż zwykłe skonfigurowanie ich tak, aby używały warunkowego połączenia przez bramę.
- Wysokie zagrożenia bezpieczeństwa. Zagrożona instancja Serwera administracyjnego ułatwia włamanie się do zarządzanych laptopów. Jeśli tak się stanie, hakerzy muszą tylko poczekać, aż jeden z laptopów wróci do sieci firmowej, aby mogli kontynuować atak na sieć lokalną.

Podłączanie zewnętrznych urządzeń stacjonarnych do Serwera administracyjnego

Urządzenia stacjonarne, które zawsze znajdują się poza główną siecią (na przykład, urządzenia w oddziałach regionalnych firmy; kioski, bankomaty i terminale zainstalowane w różnych punktach sprzedaży; urządzenia w domowych biurach pracowników) nie mogą być podłączane bezpośrednio do Serwera administracyjnego. Muszą być podłączeni do Serwera administracyjnego przez bramę połączenia zainstalowaną w strefie zdemilitaryzowanej (DMZ). Ta konfiguracja jest wykonywana podczas instalacji Agenta sieciowego na tych urządzeniach.

W celu podłączenia zewnętrznych urządzeń stacjonarnych do Serwera administracyjnego:

1. Utwórz nowy pakiet instalacyjny dla Agenta sieciowego.
2. Otwórz właściwości utworzonego pakietu instalacyjnego i przejdź do sekcji **Ustawienia** → **Zaawansowane**, a następnie wybierz opcję **Połącz z Serwerem administracyjnym korzystając z bramy połączenia**.

   Ustawienie **Połącz z Serwerem administracyjnym korzystając z bramy połączenia** jest niekompatybilne z ustawieniem **Użyj Agenta sieciowego jako bramy połączenia w DMZ**. Nie możesz włączyć obu tych ustawień jednocześnie.

3. W sekcji **Adres bramy połączenia** określ publiczny adres bramy połączenia.

   Jeśli brama połączenia znajduje się za translacją adresów sieciowych (NAT) i nie ma własnego adresu publicznego, skonfiguruj regułę bramy NAT w celu przekazywania połączeń z adresu publicznego na adres wewnętrzny bramy połączenia.

4. Utwórz autonomiczny pakiet instalacyjny w oparciu o utworzony pakiet instalacyjny.

5. Dostarcz autonomiczny pakiet instalacyjny na docelowe urządzenia, elektronicznie lub na dysku wymiennym.

6. Zainstaluj Agenta sieciowego z pakietu autonomicznego.

Zewnętrzne urządzenia stacjonarne są połączone z Serwerem administracyjnym.

Informacje o profilach połączenia dla użytkowników mobilnych

Mobilni użytkownicy laptopów (zwanych dalej również "urządzeniami") mogą potrzebować zmiany metody łączenia się z Serwerem administracyjnym lub przełączania pomiędzy Serwerami administracyjnymi w zależności od aktualnej lokalizacji urządzenia w sieci firmowej.

Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows i macOS.

Używanie różnych adresów jednego Serwera administracyjnego

Urządzenia z zainstalowanym Agentem sieciowym mogą łączyć się z Serwerem administracyjnym z poziomu wewnętrznej sieci organizacji lub internetu. W tej sytuacji wymagane może być, aby Agent sieciowy używał innych adresów do łączenia się z Serwerem administracyjnym: zewnętrznego adresu Serwera administracyjnego dla połączenia internetowego oraz wewnętrznego adresu Serwera administracyjnego dla wewnętrznego połączenia sieciowego.

W tym celu we właściwościach zasady agenta sieciowego dodaj profil do łączenia się z serwerem administracyjnym (w sekcji **Ustawienia aplikacji → Łączność → Profile połączenia → Profile połączeń Serwera administracyjnego**). W oknie tworzenia profilu wyłącz opcję **Użyj tylko do pobierania aktualizacji** i upewnij się, że opcja **Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu** jest wybrana. Jeśli do łączenia się z Serwerem administracyjnym używasz bramy połączenia (na przykład, w konfiguracji Kaspersky Security Center, opisanej w sekcji Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej), w odpowiednim polu profilu połączenia musisz określić adres bramy połączenia.

Przełączanie pomiędzy Serwerami administracyjnymi w zależności od aktualnej sieci

Jeśli organizacja posiada kilka biur z różnymi Serwerami administracyjnymi, a niektóre urządzenia z zainstalowanym Agentem sieciowym są przenoszone pomiędzy nimi, Agent sieciowy musi łączyć się z Serwerem administracyjnym sieci lokalnej w biurze, w którym znajduje się urządzenie.

W tej sytuacji konieczne jest utworzenie profilu dla połączenia z serwerem administracyjnym we właściwościach zasad agenta sieciowego dla każdego z biur, za wyjątkiem głównego biura, w którym znajduje się oryginalny macierzysty serwer administracyjny. W profilach połączenia należy określić adresy serwerów administracyjnych i włączyć lub wyłączyć opcję **Użyj tylko do pobierania aktualizacji**:

- Wybierz tę opcję, jeśli chcesz, aby Agent sieciowy zsynchronizował się z macierzystym Serwerem administracyjnym, a Serwer lokalny był używany tylko do pobierania uaktualnień.

- Wyłącz tę opcję, jeśli Agent sieciowy ma być całkowicie zarządzany przez lokalny Serwer administracyjny.

Następnie powinieneś ustalić warunki przełączania do nowo utworzonych profili: przynajmniej jeden warunek dla każdego z biur, za wyjątkiem głównego biura. Celem każdego warunku jest wykrycie elementów, które są specyficzne dla środowiska sieciowego w biurze. Jeśli warunek jest prawdziwy, odpowiedni profil zostaje aktywowany. Jeśli żaden z warunków nie jest prawdziwy, Agent sieciowy przełączy się do macierzystego Serwera administracyjnego.

Tworzenie profilu połączenia dla użytkowników mobilnych

Profil połączenia serwera administracyjnego jest dostępny tylko na urządzeniach działających pod kontrolą systemu Windows i macOS.

W celu utworzenia profilu połączenia Agenta sieciowego z Serwerem administracyjnym dla użytkowników mobilnych:

1. Jeżeli chcesz utworzyć profil połączenia dla grupy zarządzanych urządzeń, otwórz zasadę agenta sieciowego tej grupy. W tym celu wykonaj następujące czynności:

   a. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.

   b. Kliknij łącze bieżącej ścieżki.

   c. W oknie, które zostanie otwarte, wybierz żądaną grupę administracyjną.

   Następnie bieżąca ścieżka zostanie zmieniona.

   d. Dodaj zasadę agenta sieciowego dla grupy zarządzanych urządzeń. Jeśli już ją utworzono, kliknij nazwę zasady agenta sieciowego, aby otworzyć właściwości zasady.

2. Jeśli chcesz utworzyć profil połączenia dla konkretnego zarządzanego urządzenia, wykonaj następujące czynności:

   a. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.

   b. Kliknij nazwę zarządzanego urządzenia.

   c. W otwartym oknie właściwości zarządzanego urządzenia kliknij zakładkę **Aplikacje**.

   d. Kliknij nazwę zasady agenta sieciowego, której dotyczy tylko wybrane zarządzane urządzenie.

3. W otwartym oknie właściwości przejdź do **Ustawienia aplikacji** → **Łączność** → **Profile połączenia.**

4. W grupie ustawień **Profile połączeń Serwera administracyjnego** kliknij przycisk **Dodaj**.

   Domyślnie, lista profili połączeń zawiera profile <Tryb offline> i <Macierzysty serwer administracyjny>. Profili nie można modyfikować ani usunąć.

   Profil <Tryb offline> nie określa żadnego Serwera do nawiązania połączenia. Dlatego też, Agent sieciowy, gdy zostaje przełączony do tego profilu, nie próbuje nawiązać połączenia z żadnym Serwerem administracyjnym, gdy aplikacje zainstalowane na urządzeniach klienckich działają pod kontrolą zasad użytkownika mobilnego. Profil <Tryb offline> może być używany, jeśli urządzenia są odłączone od sieci.

   Profil <Macierzysty serwer administracyjny> określa połączenie z serwerem administracyjnym, który został wybrany podczas instalacji agenta sieciowego. Profil <Macierzysty serwer administracyjny> jest stosowany, gdy urządzenie jest ponownie podłączane do macierzystego Serwera administracyjnego po tym, jak przez jakiś czas działało w sieci zewnętrznej.

5. W otwartym oknie **Konfiguruj profil** skonfiguruj profil połączenia:

- **Nazwa profilu**

  W tym polu możesz przejrzeć lub zmienić nazwę profilu połączenia.

- **Adres Serwera administracyjnego**

  Adres Serwera administracyjnego, z którym urządzenie klienckie musi łączyć się podczas aktywacji profilu.

- **Numer portu**

  Numer portu używanego do nawiązywania połączenia.

- **Port SSL**

  Numer portu połączenia podczas używania portu SSL.

- **Użyj połączenia SSL**

  Jeśli ta opcja jest włączona, połączenie jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

  Domyślnie opcja ta jest włączona. Zalecamy, aby nie wyłączać tej opcji, aby Twoje połączenie pozostało bezpieczne.

- Wybierz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest wybrana, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

  - **Adres**

    Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

  - **Numer portu**

    Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

  - **Uwierzytelnianie na serwerze proxy**

    Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  - **Nazwa użytkownika**

    Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

  - **Hasło**

    Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

    Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

- **Adres bramy połączenia**

  Adres bramy, poprzez którą urządzenia klienckie łączą się z Serwerem administracyjnym.

- **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny**

  Zaznacz to pole, aby zezwolić aplikacjom zainstalowanym na urządzeniu klienckim na korzystanie z profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego, za każdym razem, gdy serwer administracyjny nie jest dostępny. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

  Jeżeli ta opcja jest wyłączona, aplikacje będą używać zasad aktywnych.

  Domyślnie pole to nie jest zaznaczone.

- **Użyj tylko do pobierania uaktualnień**

  Jeżeli ta opcja jest włączona, profil będzie używany tylko do pobierania aktualizacji przez aplikacje zainstalowane na urządzeniu klienckim. Dla innych działań połączenie z Serwerem administracyjnym będzie nawiązywane z użyciem wstępnych ustawień określonych podczas instalacji Agenta sieciowego.

  Domyślnie opcja ta jest włączona.

- **Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu**

  Jeśli ta opcja jest włączona, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym przy użyciu ustawień określonych we właściwościach profilu.

  Jeśli ta opcja jest wyłączona, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym przy użyciu oryginalnych ustawień określonych podczas instalacji.

  Ta opcja jest dostępna, jeśli opcja **Użyj tylko do pobierania uaktualnień** jest wyłączona.

  Domyślnie opcja ta jest wyłączona.

Profil połączenia Agenta sieciowego z Serwerem administracyjnym zostanie utworzony dla użytkowników mobilnych. Jeśli agent sieciowy łączy się z serwerem administracyjnym przy użyciu tego profilu, aplikacje zainstalowane na urządzeniu klienckim będą używać zasad dla urządzeń w trybie użytkownika mobilnego lub zasad użytkownika mobilnego.

Informacje o przełączaniu Agenta sieciowego na inne Serwery administracyjne

Kaspersky Security Center oferuje opcję przełączania Agenta sieciowego na urządzeniu klienckim na inne Serwery administracyjne, jeśli następujące ustawienia sieci zostały zmienione:

- **Warunek dla adresu serwera DHCP** — zmiana adresu IP serwera sieciowego (DHCP).
- **Warunek dla adresu domyślnej bramy połączenia** — zmiana adresu głównej bramy sieci.
- **Warunek dla domeny DNS** — zmiana sufiksu DNS podsieci.
- **Warunek dla adresu serwera DNS** — zmiana adresu IP serwera sieciowego DNS.
- **Warunek dla adresu serwera WINS** — zmiana adresu IP sewera sieciowego WINS. To ustawienie jest dostępne tylko dla urządzeń z systemem Windows.
- **Warunek dla rozwiązania nazw** — zmiana nazwy DNS lub NetBIOS urządzenia klienckiego.
- **Warunek dla podsieci** — zmiana adresu i maski podsieci.

- **Warunek dla dostępności domeny Windows** — zmiana stanu domeny systemu Windows, do której podłączone jest urządzenie klienckie. To ustawienie jest dostępne tylko dla urządzeń z systemem Windows.

- **Warunek dla dostępności adresu połączenia SSL** — urządzenie klienckie może lub nie może (w zależności od wybranej opcji) nawiązać połączenie SSL z określonym serwerem (nazwa:port). Musisz użyć dedykowanego serwera z oprogramowaniem zdolnym do obsługi dużego obciążenia i częstych żądań połączenia od Agenta sieciowego. Nie podawaj portu Serwera administracyjnego. Dla każdego serwera możesz dodatkowo określić certyfikat SSL. W takim przypadku Agent sieciowy weryfikuje certyfikat serwera, oprócz sprawdzenia możliwości połączenia SSL. Jeśli certyfikat nie pasuje, połączenie nie powiedzie się.

Ta funkcja jest obsługiwana tylko w przypadku agentów sieciowych zainstalowanych na urządzeniach z systemem Windows lub macOS.

Początkowe ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym są definiowane podczas instalacji Agenta sieciowego. Następnie, jeśli reguły przełączania Agenta sieciowego na inne Serwery administracyjne zostały zmienione, Agent sieciowy odpowiada na zmiany w ustawieniach sieci w następujący sposób:

- Jeśli ustawienia sieci pokrywają się z ustawieniami jednej z utworzonych reguł, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym określonym w tej regule. Aplikacje zainstalowane na urządzeniach klienckich przełączają się do zasady użytkownika mobilnego pod warunkiem, że takie zachowanie jest dozwolone przez regułę.

- Jeśli nie jest stosowana żadna z reguł, Agent sieciowy przywróci ustawienia domyślne połączenia z Serwerem administracyjnym określone podczas instalacji. Aplikacje zainstalowane na urządzeniach klienckich przywracają aktywne zasady.

- Jeśli Serwer administracyjny jest niedostępny, Agent sieciowy używa zasad użytkownika mobilnego.

Agent sieciowy przełącza się do zasady użytkownika mobilnego tylko wtedy, gdy opcja **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny** jest włączona w ustawieniach zasady Agenta sieciowego.

Ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym są zapisywane w profilu połączenia. W profilu połączenia możesz utworzyć reguły przełączania urządzeń klienckich do zasad użytkownika mobilnego, a także skonfigurować profil tak, aby mógł być używany tylko do pobierania uaktualnień.

Tworzenie reguły przełączania Agenta sieciowego według lokalizacji sieciowej

Przełączanie agenta sieciowego według lokalizacji sieciowej jest dostępne tylko na urządzeniach działających pod kontrolą systemu Windows i macOS.

W celu utworzenia reguły przełączania Agenta sieciowego z jednego z Serwera administracyjnego na inny w przypadkui zmiany ustawień sieciowych:

1. Jeśli chcesz utworzyć regułę dla grupy zarządzanych urządzeń, otwórz zasadę agenta sieciowego tej grupy. W tym celu wykonaj następujące czynności:

   a. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.

   b. Kliknij łącze bieżącej ścieżki.

c. W oknie, które zostanie otwarte, wybierz żądaną grupę administracyjną.

Następnie bieżąca ścieżka zostanie zmieniona.

d. Dodaj zasadę agenta sieciowego dla grupy zarządzanych urządzeń. Jeśli już ją utworzono, kliknij nazwę zasady agenta sieciowego, aby otworzyć właściwości zasady.

2. Jeśli chcesz utworzyć regułę dla określonego zarządzanego urządzenia, wykonaj następujące czynności:

a. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.

b. Kliknij nazwę zarządzanego urządzenia.

c. W otwartym oknie właściwości zarządzanego urządzenia kliknij zakładkę **Aplikacje**.

d. Kliknij nazwę zasady agenta sieciowego, której dotyczy tylko wybrane zarządzane urządzenie.

3. W otwartym oknie właściwości przejdź do **Ustawienia aplikacji** → **Łączność** → **Profile połączenia.**

4. W sekcji **Ustawienia lokalizacji sieciowej** kliknij przycisk **Dodaj**.

5. W otwartym oknie właściwości skonfiguruj opis lokalizacji sieciowej i regułę przełączania. Określ następujące ustawienia opisu lokalizacji sieciowej:

- **Opis**

  Nazwa opisu lokalizacji sieciowej nie może być dłuższa niż 255 znaków i nie może zawierać znaków specjalnych, takich jak ("*<>?\/:|).

- **Użyj profilu połączenia**

  Na liście rozwijalnej możesz określić profil połączenia, którego Agent sieciowy używa do nawiązania połączenia z Serwerem administracyjnym. Ten profil będzie używany, jeśli spełnione są warunki opisu lokalizacji sieciowej. Profil połączenia zawiera ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym i definiuje, kiedy urządzenia klienckie muszą przełączyć się do zasad użytkownika mobilnego. Profil jest używany tylko do pobierania uaktualnień.

- **Opis włączony**

  Zaznacz to pole wyboru, aby umożliwić korzystanie z nowego opisu lokalizacji sieciowej.

6. Wybierz warunki reguły przełączania agenta sieciowego:

- **Warunek dla adresu serwera DHCP** — zmiana adresu IP serwera sieciowego (DHCP).
- **Warunek dla adresu domyślnej bramy połączenia** — zmiana adresu głównej bramy sieci.
- **Warunek dla domeny DNS** — zmiana sufiksu DNS podsieci.
- **Warunek dla adresu serwera DNS** — zmiana adresu IP serwera sieciowego DNS.
- **Warunek dla adresu serwera WINS** — zmiana adresu IP sewera sieciowego WINS. To ustawienie jest dostępne tylko dla urządzeń z systemem Windows.
- **Warunek dla rozwiązania nazw** — zmiana nazwy DNS lub NetBIOS urządzenia klienckiego.
- **Warunek dla podsieci** — zmiana adresu i maski podsieci.

- **Warunek dla dostępności domeny Windows** — zmiana stanu domeny systemu Windows, do której podłączone jest urządzenie klienckie. To ustawienie jest dostępne tylko dla urządzeń z systemem Windows.

- **Warunek dla dostępności adresu połączenia SSL** — urządzenie klienckie może lub nie może (w zależności od wybranej opcji) nawiązać połączenie SSL z określonym serwerem (nazwa:port). Dla każdego serwera możesz dodatkowo określić certyfikat SSL. W takim przypadku Agent sieciowy weryfikuje certyfikat Serwera, oprócz sprawdzenia możliwości połączenia SSL. Jeśli certyfikat nie pasuje, połączenie nie powiedzie się.

Warunki w regule są połączone przy użyciu operatora logicznego I. Aby wyzwolić regułę przełączania według opisu lokalizacji sieciowej, muszą być spełnione wszystkie warunki przełączania reguły.

7. W sekcji warunku określ, kiedy agent sieciowy powinien zostać przełączony na inny serwer administracyjny. W tym celu kliknij przycisk **Dodaj**, a następnie ustaw wartość warunku.

   Ponadto opcja **Zgodny z przynajmniej jedną wartością z listy** jest domyślnie włączona. Możesz wyłączyć tę opcję, jeśli chcesz, aby warunek został spełniony ze wszystkimi określonymi wartościami.

8. Zapisz zmiany.

Zostanie utworzona nowa reguła przełączania według opisu lokalizacji sieciowej. Za każdym razem, gdy zostaną spełnione warunki reguły, Agent sieciowy będzie używał profilu połączenia, określonego w regule, do łączenia się z Serwerem administracyjnym.

Kreator wdrażania ochrony

Do zainstalowania aplikacji firmy Kaspersky można użyć kreatora wdrażania ochrony. Kreator wdrażania ochrony umożliwia przeprowadzenie zdalnej instalacji aplikacji przy pomocy specjalnie utworzonych pakietów instalacyjnych lub bezpośrednio z pakietu dystrybucyjnego.

Kreator wdrażania ochrony wykonuje następujące działania:

- Pobiera pakiet instalacyjny potrzebny do zainstalowania aplikacji (jeśli nie został utworzony wcześniej). Pakiet instalacyjny znajduje się w: **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**. Możesz użyć tego pakietu instalacyjnego do przyszłej instalacji aplikacji.

- Tworzy i uruchamia zadanie zdalnej instalacji dla określonych urządzeń lub grupy administracyjnej. Nowo utworzone zadanie zdalnej instalacji jest przechowywane w sekcji **Zadania**. Możesz później uruchomić to zadanie ręcznie. Typ zadania to **Zdalna instalacja aplikacji**.

Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym SUSE Linux Enterprise Server 15, w pierwszej kolejności zainstaluj pakiet insserv-compat, aby skonfigurować Agenta sieciowego.

Krok 1. Uruchamianie kreatora wdrażania ochrony

W celu ręcznego uruchomienia kreatora wdrażania ochrony:

W głównym menu kliknij **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Kreator wdrażania ochrony**.

Zostanie uruchomiony kreatora wdrażania ochrony. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

Krok 2. Wybieranie pakietu instalacyjnego

Wybierz pakiet instalacyjny aplikacji, którą chcesz zainstalować.

Jeśli nie ma pakietu instalacyjnego żądanej aplikacji, kliknij przycisk **Dodaj**, a następnie wybierz aplikację z listy.

Krok 3. Wybieranie metody rozsyłania pliku klucza lub kodu aktywacyjnego

Wybierz metodę rozesłania pliku klucza lub kodu aktywacyjnego:

- **Nie dodawaj klucza licencyjnego do pakietu instalacyjnego**

  Klucz jest automatycznie rozsyłany na wszystkie urządzenia, z którymi jest kompatybilny:
  - Jeśli we właściwościach klucza jest włączona automatyczna dystrybucja.
  - Jeśli utworzono zadanie **Dodaj klucz**.

- **Dodaj klucz licencyjny do pakietu instalacyjnego**

  Klucz jest rozsyłany na urządzenia wraz z pakietem instalacyjnym.

  > Nie zalecamy rozpowszechniania klucza przy użyciu tej metody, ponieważ współdzielone prawa dostępu do odczytu są włączone do repozytorium pakietów instalacyjnych.

Jeśli pakiet instalacyjny już zawiera plik klucza lub kod aktywacyjny, to okno zostanie wyświetlone, ale będzie zawierało tylko informacje dotyczące klucza licencyjnego.

Krok 4. Wybieranie wersji Agenta sieciowego

Jeśli wybrałeś pakiet instalacyjny aplikacji innej niż Agent sieciowy, musisz także zainstalować Agenta sieciowego, który łączy aplikację z Serwerem administracyjnym Kaspersky Security Center.

Wybierz najnowszą wersję Agenta sieciowego.

Krok 5. Wybór urządzeń

Określ listę urządzeń, na których zostanie zainstalowana aplikacja:

- **Zainstaluj na zarządzanych urządzeniach**

  Jeżeli ta opcja jest zaznaczona, zadanie zdalnej instalacji jest tworzone dla grupy urządzeń.

- **Wybierz urządzenia do instalacji**

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

Krok 6. Określanie ustawień zadania zdalnej instalacji

W oknie **Ustawienia zadania zdalnej instalacji** określ ustawienia zdalnej instalacji aplikacji.

W grupie ustawień **Wymuś pobranie pakietu instalacyjnego** określ sposób rozsyłania na urządzenia klienckie plików, które są niezbędne do zainstalowania aplikacji:

- **Przy użyciu Agenta sieciowego**

  Jeśli ta opcja jest włączona, pakiety instalacyjne są dostarczane na urządzenia klienckie przez Agenta sieciowego zainstalowanego na tych urządzeniach klienckich.

  Jeśli ta opcja jest wyłączona, pakiety instalacyjne są dostarczane przy użyciu narzędzi systemu operacyjnego urządzeń klienckich.

  Zalecane jest włączenie tej opcji, jeśli zadanie zostało przypisane do urządzeń z zainstalowanymi Agentami sieciowymi.

  Domyślnie opcja ta jest włączona.

- **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**

  Jeśli ta opcja jest włączona, pakiety instalacyjne są przesyłane na urządzenia klienckie przy użyciu narzędzi systemu operacyjnego za pośrednictwem punktów dystrybucyjnych. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny.

  Jeśli opcja **Przy użyciu Agenta sieciowego** jest włączona, pliki będą dostarczane przy użyciu narzędzi systemu operacyjnego, jeśli narzędzia Agenta sieciowego są niedostępne.

  Domyślnie ta opcja jest włączona dla zadań zdalnej instalacji utworzonych na wirtualnym Serwerze administracyjnym.

  > Jeśli wszystkie punkty dystrybucji przypisane do urządzenia okażą się wadliwe, urządzenie nie będzie otrzymywać aktualizacji (baz wirusów i poprawek) ani pakietów instalacyjnych.

- **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**

  Jeśli ta opcja jest włączona, pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego urządzeń klienckich za pośrednictwem Serwera administracyjnego. Możesz włączyć tę opcję, jeśli na urządzeniu klienckim nie ma zainstalowanego Agenta sieciowego, ale urządzenie klienckie jest w tej samej sieci co Serwer administracyjny.

  Domyślnie opcja ta jest włączona.

Określ ustawienia dodatkowe:

- **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana**

  Jeśli ta opcja jest włączona, wybrana aplikacja nie zostanie ponownie zainstalowana, jeśli już jest zainstalowana na tym urządzeniu klienckim.

  Jeśli ta opcja jest wyłączona, aplikacja zostanie zainstalowana mimo wszystko.

Domyślnie opcja ta jest włączona.

- **Przypisz pakiet instalacyjny do zasad grupy Active Directory**

  Jeśli ta opcja jest włączona, pakiet instalacyjny jest instalowany przy użyciu zasad grupy Active Directory.

  Ta opcja jest dostępna, jeśli wybrany jest pakiet instalacyjny Agenta sieciowego.

  Domyślnie opcja ta jest wyłączona.

Krok 7. Zarządzanie ponownym uruchomieniem

Określ działanie, jakie ma zostać wykonane, jeśli system operacyjny musi być uruchomiony ponownie podczas instalowania aplikacji:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

  - **Uruchom ponownie po (min)**

    Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

    Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

Krok 8. Usuwanie niekompatybilnych aplikacji przed instalacją

Ten krok jest dostępny tylko wtedy, gdy wiadomo, że aplikacja, którą instalujesz, jest niekompatybilna z innymi aplikacjami.

Wybierz opcję, jeśli chcesz, aby program Kaspersky Security Center automatycznie usuwał aplikacje, które są niekompatybilne z instalowaną aplikacją.

Lista niekompatybilnych aplikacji także zostanie wyświetlona.

Jeśli nie wybierzesz tej opcji, aplikacja zostanie zainstalowana tylko na urządzeniach, na których nie ma niekompatybilnych aplikacji.

Krok 9. Przenoszenie urządzeń do grupy Zarządzane urządzenia

Określ, czy urządzenia powinny zostać przeniesione do grupy administracyjnej po zainstalowaniu Agenta sieciowego.

- **Nie przenoś urządzeń**

  Urządzenia pozostają w grupach, w których aktualnie się znajdują. Urządzenia, które zostały umieszczone w dowolnej grupie, pozostaną nieprzypisane.

- **Przenieś nieprzypisane urządzenia do grupy**

  Urządzenia są przenoszone do wybranej grupy administracyjnej.

Opcja **Nie przenoś urządzeń** została wybrana domyślnie. W celach bezpieczeństwa możesz ręcznie przenieść urządzenia.

Krok 10. Wybieranie kont w celu uzyskania dostępu do urządzeń

Jeśli to konieczne, dodaj konta, które będą używane do uruchamiania zadania zdalnej instalacji:

- **Konto nie jest wymagane (Agent sieciowy jest zainstalowany)**

  Jeśli ta opcja jest zaznaczona, nie musisz określić konta, z poziomu którego zostanie uruchomiony instalator aplikacji. Zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

  Jeśli Agent sieciowy nie został zainstalowany na urządzeniach klienckich, ta opcja nie będzie dostępna.

- **Konto wymagane (Agent sieciowy nie jest używany)**

  Wybierz tę opcję, jeśli Agent sieciowy nie jest zainstalowany na urządzeniach, do których przypisano zadanie zdalnej instalacji. W takim przypadku możesz określić konto użytkownika lub certyfikat SSH, aby zainstalować aplikację.

  - **Konto lokalne**. Jeśli ta opcja jest zaznaczona, określ konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji. Kliknij przycisk **Dodaj**, wybierz **Konto lokalne**, a następnie określ poświadczenia konta użytkownika.

    Możesz określić wiele kont użytkowników, jeśli na przykład żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, do których przypisujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

  - **Certyfikat SSH**. Jeśli chcesz zainstalować aplikację na urządzeniu klienckim opartym na systemie Linux, możesz określić certyfikat SSH zamiast konta użytkownika. Kliknij przycisk **Dodaj**, wybierz **Certyfikat SSH**, a następnie określ klucze prywatny i publiczny certyfikatu.

    Aby wygenerować klucz prywatny, możesz użyć narzędzia ssh-keygen. Należy zauważyć, że Kaspersky Security Center obsługuje format PEM kluczy prywatnych, ale narzędzie ssh-keygen domyślnie generuje klucze SSH w formacie OPENSSH. Format OPENSSH nie jest obsługiwany przez Kaspersky Security Center. Aby utworzyć klucz prywatny w obsługiwanym formacie PEM, dodaj opcję -m PEM w poleceniu ssh-keygen. Na przykład:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< adres e-mail użytkownika >"
    ```

Krok 11. Uruchamianie instalacji

Ten krok to ostatni krok kreatora. W tym kroku **Zadanie zdalnej instalacji** zostało pomyślnie utworzone i skonfigurowane.

Domyślnie opcja **Uruchom zadanie po zakończeniu działania kreatora** nie jest zaznaczona. Jeśli wybierzesz tę opcję, **Zadanie zdalnej instalacji** zostanie uruchomione natychmiast po zakończeniu działania kreatora. Jeśli nie wybierzesz tej opcji, **Zadanie zdalnej instalacji** nie zostanie uruchomione. Możesz później uruchomić to zadanie ręcznie.

Kliknij **OK**, aby zakończyć ostatni krok kreatora wdrażania ochrony.

Wdrażanie aplikacji Kaspersky poprzez Kaspersky Security Center Web Console

W tej sekcji opisano sposób wdrażania aplikacji Kaspersky na urządzeniach klienckich w Twojej organizacji przy użyciu Kaspersky Security Center Web Console.

Scenariusz: Wdrażanie aplikacji Kaspersky poprzez Kaspersky Security Center Web Console

Ten scenariusz wyjaśnia sposób wdrażania aplikacji Kaspersky za pośrednictwem Kaspersky Security Center Web Console. Możesz użyć kreatora wstępnej konfiguracji i kreatora wdrażania ochrony lub możesz ręcznie wykonać wszystkie niezbędne kroki.

Do zdalnego wdrożenia przy użyciu Kaspersky Security Center Web Console dostępne są następujące aplikacje:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

Etapy

Wdrożenie aplikacji firmy Kaspersky odbywa się w krokach:

1. **Pobranie wtyczki zarządzającej dla aplikacji**

   Ten krok jest częścią kreatora wstępnej konfiguracji. Jeśli zdecydujesz się nie uruchamiać kreatora, ręcznie pobierz wtyczkę dla Kaspersky Endpoint Security for Windows.

   Jeśli planujesz zarządzać firmowymi urządzeniami mobilnymi, postępuj zgodnie z instrukcjami podanymi w pomocy dla Kaspersky Security for Mobile w celu pobrania i zainstalowania wtyczek zarządzających dla Kaspersky Endpoint Security for Android.

2. **Pobieranie i tworzenie pakietów instalacyjnych**

   Ten krok jest częścią kreatora wstępnej konfiguracji.

   Kreator wstępnej konfiguracji umożliwia pobranie pakietu instalacyjnego z wtyczką zarządzającą. Jeśli nie wybrano tej opcji podczas uruchamiania kreatora lub jeśli w ogóle nie uruchomiono kreatora, musisz ręcznie pobrać pakiet.

   Jeśli nie możesz zainstalować aplikacji firmy Kaspersky przy użyciu Kaspersky Security Center na niektórych urządzeniach, na przykład, na zdalnych urządzeniach pracowników, możesz utworzyć autonomiczne pakiety instalacyjne dla aplikacji. Jeśli używasz autonomicznych pakietów do instalacji aplikacji Kaspersky, nie musisz tworzyć i uruchamiać zadania zdalnej instalacji, ani tworzyć i konfigurować zadań dla Kaspersky Endpoint Security for Windows.

3. **Tworzenie, konfigurowanie i uruchamianie zadania zdalnej instalacji**

Dla Kaspersky Endpoint Security for Windows ten krok jest częścią kreatora wdrażania ochrony, który jest uruchamiany automatycznie po zakończeniu pracy kreatora wstępnej konfiguracji. Jeśli zdecydujesz się nie uruchamiać Kreator wdrażania ochrony, musisz ręcznie utworzyć to zadanie oraz ręcznie je skonfigurować.

Możesz także ręcznie utworzyć kilka zadań zdalnej instalacji dla różnych grup administracyjnych lub różnych wyborów urządzeń. Możesz wdrożyć różne wersje jednej aplikacji w tych zadaniach.

Upewnij się, że wszystkie urządzenia w Twojej sieci zostały wykryte, a następnie uruchom zadanie zdalnej instalacji (lub zadania).

Zainstaluj narzędzie nmap na swoich urządzeniach z systemem Linux. To narzędzie jest wymagane do włączenia funkcji rozpoznawania lokalizacji w sieci (NLA).

Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym SUSE Linux Enterprise Server 15, w pierwszej kolejności zainstaluj pakiet insserv-compat, aby skonfigurować Agenta sieciowego.

Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym RED OS 7.3.4 lub nowszym albo MSVSPHERE 9.2 lub nowszym, zainstaluj pakiet libxcrypt-compat, aby Agent sieciowy działał prawidłowo.

4. **Tworzenie i konfigurowanie zadań dla zarządzanej aplikacji**

   Należy skonfigurować zadanie *Zainstaluj aktualizacje programu* Kaspersky Endpoint Security for Windows.

   Ten krok jest częścią kreatora wstępnej konfiguracji: zadanie jest tworzone i konfigurowane automatycznie z domyślnymi ustawieniami. Jeśli nie uruchomiono kreatora, musisz ręcznie utworzyć to zadanie oraz ręcznie je skonfigurować. Jeśli użyjesz kreatora wstępnej konfiguracji, upewnij się, że terminarz zadania spełnia Twoje wymagania (domyślnie, zaplanowane uruchomienie zadania jest ustawione na **Ręcznie**, ale możesz chcieć wybrać inną opcję).

   Inne aplikacje Kaspersky mogą mieć inne domyślne zadania. Więcej informacji można znaleźć w dokumentacji dla konkretnej aplikacji.

   Upewnij się, że terminarz dla każdego zadania, które tworzysz, spełnia Twoje wymagania.

5. **Instalowanie Kaspersky Security for Mobile (opcjonalnie)**

   Jeśli planujesz zarządzać firmowymi urządzeniami mobilnymi, postępuj zgodnie z instrukcjami podanymi w pomocy dla Kaspersky Security for Mobile, aby uzyskać informacje o wdrożeniu Kaspersky Endpoint Security for Android.

6. **Tworzenie zasad**

   Utwórz zasadę dla każdej aplikacji ręcznie lub (w przypadku Kaspersky Endpoint Security for Windows) poprzez Kreatora wstępnej konfiguracji. Możesz użyć domyślnych ustawień zasady; możesz także zmodyfikować domyślne ustawienia zasady zgodnie ze swoimi potrzebami w dowolnym momencie.

7. **Sprawdzanie wyników**

   Upewnij się, że zdalna instalacja zakończyła się pomyślnie: masz zasady i zadania dla każdej aplikacji, a te aplikacje są instalowane na zarządzanych urządzeniach.

Wyniki

Zakończenie scenariusza powoduje, że:

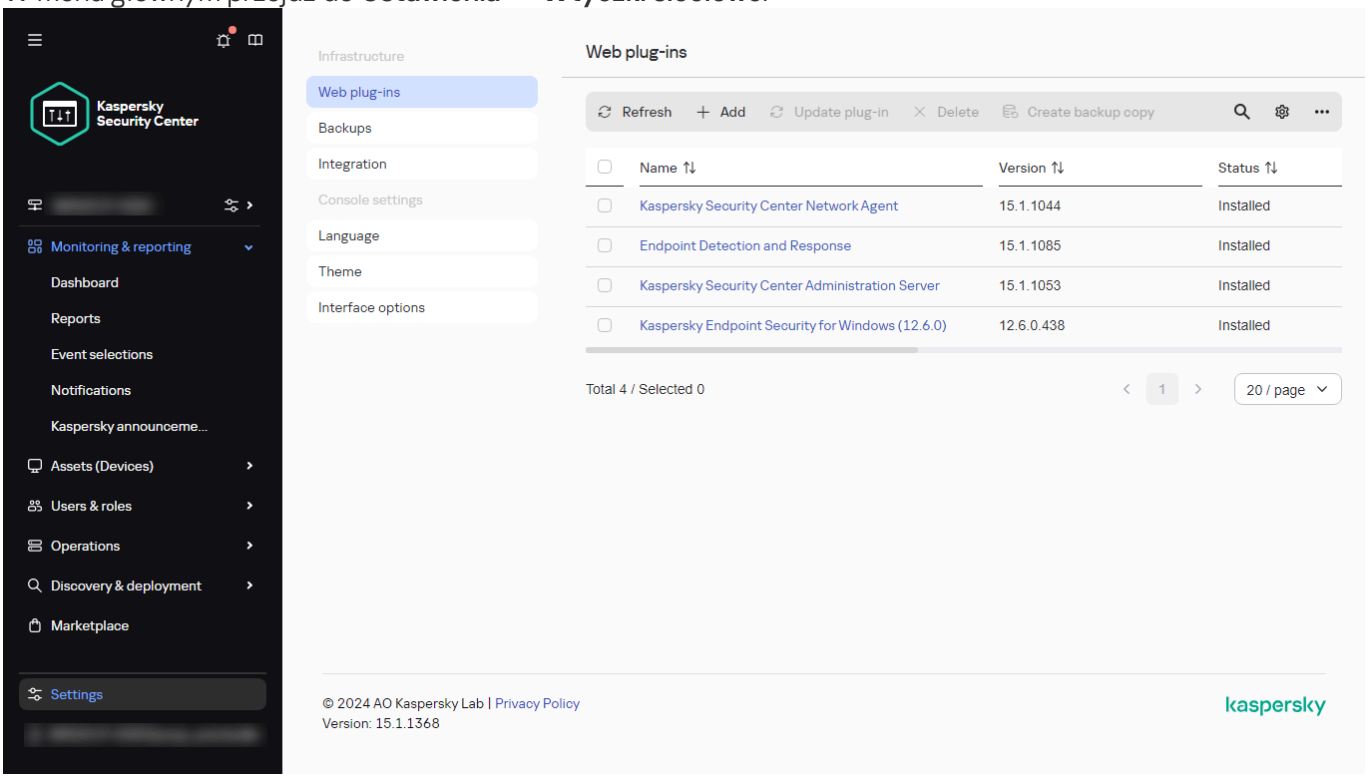
- Zostaną utworzone wszystkie wymagane zasady i zadania dla wybranych aplikacji.
- Terminarze zadań zostaną skonfigurowane według Twoich potrzeb.
- Wybrane aplikacje zostaną zainstalowane lub zostanie zaplanowane ich zainstalowanie na wybranych urządzeniach klienckich.

Uzyskiwanie wtyczek dla aplikacji firmy Kaspersky

Aby zdalnie zainstalować aplikację Kaspersky, taką jak Kaspersky Endpoint Security for Windows, musisz pobrać wtyczkę zarządzającą dla aplikacji.

W celu pobrania wtyczki zarządzającej dla aplikacji Kaspersky:

1. W menu głównym przejdź do **Ustawienia** → **Wtyczki sieciowe**.



Lista zainstalowanych wtyczek webowych

2. W otwartym oknie kliknij przycisk **Dodaj**.

   Zostanie wyświetlona lista dostępnych wtyczek.

3. Na liście dostępnych wtyczek wybierz wtyczkę, którą chcesz pobrać (na przykład, Kaspersky Endpoint Security 11 for Windows), klikając jej nazwę.

   Zostanie wyświetlona strona opisu wtyczki.

4. Na stronie opisu wtyczki kliknij **Zainstaluj wtyczkę**.

5. Po zakończeniu instalacji, kliknij **OK**.

   Wtyczka zarządzająca zostanie pobrana z domyślną konfiguracją i zostanie wyświetlona na liście wtyczek zarządzających.

Możesz dodać wtyczki i zaktualizować pobrane wtyczki z pliku. Możesz pobierać wtyczki do zarządzania i webowe wtyczki do zarządzania ze strony pomocy technicznej Kaspersky.

W celu pobrania lub zaktualizowania wtyczki z pliku:

1. W menu głównym przejdź do **Ustawienia** → **Wtyczki sieciowe**.

2. Wykonaj jedną z poniższych czynności:

   - Kliknij **Dodaj z pliku**, aby pobrać wtyczkę z pliku.

   - Kliknij **Aktualizuj z pliku**, aby pobrać aktualizację wtyczkę z pliku.

3. Określ plik i sygnaturę pliku.

4. Pobierz określone pliki.

   Wtyczka zarządzająca zostanie pobrana z pliku i zostanie wyświetlona na liście wtyczek zarządzających.

Pobieranie i tworzenie pakietów instalacyjnych dla aplikacji Kaspersky

Możesz utworzyć pakiety instalacyjne dla aplikacji firmy Kaspersky z serwerów Kaspersky, jeśli Serwer administracyjny ma dostęp do internetu.

W celu pobrania i utworzenia pakietu instalacyjnego dla aplikacji Kaspersky:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**.

   - W menu głównym przejdź do **Operacje** → **Repozytoria** → **Pakiety instalacyjne**.

   Możesz także przejrzeć powiadomienia o nowych pakietach dla aplikacji firmy Kaspersky na liście powiadomień ekranowych. Jeśli istnieją powiadomienia o nowym pakiecie, możesz kliknąć odnośnik obok powiadomienia i przejść do listy dostępnych pakietów instalacyjnych.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Wybierz opcję **Utwórz pakiet instalacyjny dla aplikacji Kaspersky**.

   Pojawi się lista pakietów instalacyjnych dostępnych na serwerach sieciowych Kaspersky. Lista zawiera pakiety instalacyjne tylko dla tych aplikacji, które są kompatybilne z bieżącą wersją Kaspersky Security Center.

4. Kliknij nazwę pakietu instalacyjnego, na przykład, Kaspersky Endpoint Security for Windows (11.1.0).

   Zostanie otwarte okno z informacjami o pakiecie instalacyjnym.

   > Możesz pobrać i używać pakietu instalacyjnego, który zawiera narzędzia kryptograficzne, które implementują silne szyfrowanie, jeśli jest to zgodne z obowiązującymi przepisami i regulacjami. Aby pobrać pakiet instalacyjny Kaspersky Endpoint Security for Windows potrzebny w Twojej organizacji, miej na uwadze ustawodawstwo kraju, w którym znajdują się urządzenia klienckie Twojej organizacji.

5. Przeczytaj informacje i kliknij przycisk **Pobierz i utwórz pakiet instalacyjny**.

   Jeśli pakiet dystrybucyjny nie może zostać przekonwertowany na pakiet instalacyjny, wyświetlany jest przycisk **Pobierz pakiet dystrybucyjny** zamiast **Pobierz i utwórz pakiet instalacyjny**.

   Rozpocznie się pobieranie pakietu instalacyjnego na Serwer administracyjny. Możesz zamknąć okno kreatora lub przejść do następnego kroku instrukcji. Jeśli zamkniesz okno kreatora, proces pobierania będzie kontynuowany w tle.

   Jeśli chcesz śledzić proces pobierania pakietu instalacyjnego:

   a. W menu głównym przejdź do **Operacje → Repozytoria → Pakiety instalacyjne → W toku ()**.

   b. Śledź proces działania w kolumnie **Postęp pobierania** oraz w kolumnie **Stan pobierania** tabeli.

   Po zakończeniu procesu pakiet instalacyjny zostanie dodany do listy na zakładce **Pobrano**. Jeśli proces pobierania zostanie zatrzymany, a stan pobierania przełączy się na **Zaakceptuj Umowę licencyjną**, kliknij nazwę pakietu instalacyjnego, a następnie przejdź do kolejnego kroku instrukcji.

   > Jeśli rozmiar danych znajdujących się w wybranym pakiecie dystrybucyjnym przekracza bieżące ograniczenie, zostanie wyświetlona wiadomość o błędzie. Możesz zmienić ograniczoną wartość, a następnie przejdź do tworzenia pakietu instalacyjnego.

6. Dla niektórych aplikacji Kaspersky, podczas pobierania wyświetlany jest przycisk **Pokaż Umowę licencyjną**. Jeśli przycisk jest wyświetlany, wykonaj następujące czynności:

   a. Kliknij przycisk **Pokaż Umowę licencyjną**, aby przeczytać Umowę licencyjną użytkownika końcowego (EULA).

   b. Przeczytaj Umowę licencyjną użytkownika końcowego, która zostanie wyświetlona na ekranie, i kliknij **Zaakceptuj**.

      Po zaakceptowaniu Umowy licencyjnej użytkownika końcowego, proces pobierania będzie kontynuowany. Jeśli klikniesz **Odrzuć**, proces pobierania zostanie zatrzymany.

7. Po zakończeniu pobierania kliknij przycisk **Zamknij**.

Wybrany pakiet instalacyjny zostanie pobrany do folderu współdzielonego Serwera administracyjnego, do podfolderu Pakiety. Po pobraniu, pakiet instalacyjny jest wyświetlany na liście pakietów instalacyjnych.

Zmienianie ograniczenia rozmiaru danych niestandardowego pakietu instalacyjnego

Całkowity rozmiar danych wypakowanych podczas tworzenia niestandardowego pakietu instalacyjnego jest ograniczony. Domyślne ograniczenie to 1 GB.

Jeśli spróbujesz przesłać plik archiwum, który zawiera dane przekraczające bieżące ograniczenie, zostanie wyświetlony komunikat o błędzie. Konieczne może być zwiększenie tej wartości ograniczenia podczas tworzenia pakietów instalacyjnych z dużych pakietów dystrybucyjnych.

W celu zmiany wartości ograniczenia dla rozmiaru niestandardowego pakietu instalacyjnego:

1. Na urządzeniu Serwera administracyjnego uruchom wiersz poleceń z poziomu konta, które zostało użyte do zainstalowania Serwera administracyjnego.

2. Zmień bieżący katalog na folder instalacyjny Kaspersky Security Center (zwykle <dysk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. W zależności od rodzaju instalacji serwera administracyjnego, wprowadź jedno z poniższych poleceń, korzystając z uprawnień administratora:

   - Normalna instalacja lokalna:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <liczba bajtów>
     ```

   - Instalacja klastra trybu failover Kaspersky Security Center:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <liczba bajtów> --stp klfoc
     ```

   - Instalowanie klastra trybu failover Windows Server:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <liczba bajtów> --stp cluster
     ```

   Gdzie <liczba bajtów> to liczba bajtów w formacie szesnastkowym lub dziesiętnym.

   Na przykład, jeśli wymagany limit wynosi 2 GB, można określić wartość dziesiętną 2147483648 lub wartość szesnastkową 0x80000000. W takim przypadku w przypadku lokalnej instalacji Serwera administracyjnego możesz użyć następującego polecenia:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Ograniczenie rozmiaru danych niestandardowego pakietu instalacyjnego zostanie zmienione.

Pobieranie pakietów dystrybucyjnych dla aplikacji Kaspersky

W Kaspersky Security Center Web Console możesz pobrać i zapisać pakiety dystrybucyjne dla aplikacji firmy Kaspersky. Możesz użyć pakietów dystrybucyjnych do ręcznego zainstalowania aplikacji, bez użycia Kaspersky Security Center.

W celu pobrania i zapisania pakietów dystrybucyjnych dla aplikacji Kaspersky:

1. W menu głównym przejdź do **Operations → Kaspersky applications → Current application versions**.

   Zostanie otwarta lista dostępnych pakietów dystrybucyjnych, wtyczek i łat. Kaspersky Security Center wyświetla tylko te elementy, które są kompatybilne z jego bieżącą wersją.

2. Na liście kliknij nazwę pakietu, który chcesz pobrać.

   Zostanie otwarty opis pakietu.

3. Przeczytaj opis i kliknij przycisk **Pobierz i utwórz pakiet instalacyjny**.

   Jeśli pakiet dystrybucyjny nie może zostać przekonwertowany na pakiet instalacyjny, wyświetlany jest przycisk **Pobierz pakiet dystrybucyjny** zamiast **Pobierz i utwórz pakiet instalacyjny**.

   Rozpocznie się pobieranie pakietu instalacyjnego na Serwer administracyjny.

Wybrany pakiet instalacyjny lub dystrybucyjny zostanie pobrany do folderu współdzielonego Serwera administracyjnego, do podfolderu **Pakiety**. Po pobraniu, pakiet instalacyjny jest wyświetlany na liście pakietów instalacyjnych.

Sprawdzanie, czy pomyślnie wdrożono Kaspersky Endpoint Security

W celu zapewnienia poprawnego zainstalowania aplikacji firmy Kaspersky, takich jak Kaspersky Endpoint Security:

1. Korzystając z Kaspersky Security Center Web Console, upewnij się, że posiadasz:

   - Zasada dla Kaspersky Endpoint Security i/lub innych aplikacji zabezpieczających, których używasz.
   - Zadania dla Kaspersky Endpoint Security for Windows: zadanie *Szybkie skanowanie* i zadanie *Zainstaluj aktualizację* (jeśli używasz Kaspersky Endpoint Security for Windows).
   - Zadania dla innych aplikacji zabezpieczających, których używasz.

2. Na jednym z zarządzanych urządzeń, wybranym dla instalacji, upewnij się, że:

   - Zainstalowany jest program Kaspersky Endpoint Security lub inna aplikacja zabezpieczająca firmy Kaspersky.
   - W Kaspersky Endpoint Security ustawienia Ochrony plików, Ochrony WWW i Ochrony poczty odpowiadają zasadzie, którą utworzyłeś dla tego urządzenia.
   - Usługa Kaspersky Endpoint Security może zostać zatrzymana i uruchomiona ręcznie.
   - Zadania grupowe mogą być zatrzymywane i uruchamiane ręcznie.

Tworzenie autonomicznych pakietów instalacyjnych

Ty oraz użytkownicy urządzeń w Twojej organizacji mogą używać autonomicznych pakietów instalacyjnych, aby ręcznie instalować aplikacje na urządzeniach.

Autonomiczny pakiet instalacyjny jest plikiem wykonywalnym (installer.exe), który można umieścić na serwerze sieciowym lub w folderze sieciowym, wysłać za pośrednictwem poczty elektronicznej lub przenieść na urządzenie klienckie w dowolny sposób. Na urządzeniu klienckim użytkownik może uruchomić otrzymany plik lokalnie, aby zainstalować aplikację bez udziału Kaspersky Security Center. Możesz tworzyć autonomiczne pakiety instalacyjne dla aplikacji Kaspersky i aplikacji innych firm na platformy Windows, macOS i Linux. Aby utworzyć autonomiczny pakiet instalacyjny dla aplikacji firmy trzeciej, należy utworzyć niestandardowy pakiet instalacyjny.

Upewnij się, że autonomiczny pakiet instalacyjny nie jest dostępny dla nieupoważnionych osób.

W celu utworzenia autonomicznego pakietu instalacyjnego:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym przejdź do **Wykrywanie i wdrażanie → Wdrażanie i przypisywanie → Pakiety instalacyjne**.
   - W menu głównym przejdź do **Operacje → Repozytoria → Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Na liście pakietów instalacyjnych wybierz pakiet instalacyjny i nad listą kliknij przycisk **Wdrażaj**.

3. Wybierz opcję **Przy użyciu pakietów autonomicznych**.

   Zostanie uruchomiony Kreator tworzenia autonomicznego pakietu instalacyjnego. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

4. Upewnij się, że opcja **Zainstaluj Agenta sieciowego wraz z aplikacją** jest włączona, jeśli chcesz zainstalować Agenta sieciowego wraz z wybraną aplikacją.

   Opcja jest wyświetlana w zależności od aplikacji, dla której tworzysz autonomiczny pakiet instalacyjny.

   Domyślnie opcja ta jest włączona. Zalecane jest włączenie tej opcji, jeśli nie jesteś pewien, czy Agent sieciowy jest zainstalowany na urządzeniu. Jeśli Agent sieciowy jest już zainstalowany na urządzeniu, po zainstalowaniu autonomicznego pakietu instalacyjnego wraz z Agentem sieciowym, Agent sieciowy zostanie zaktualizowany do nowszej wersji.

   Jeśli wyłączysz tę opcję, Agent sieciowy nie zostanie zainstalowany na urządzeniu, a urządzenie będzie niezarządzane.

   Jeśli autonomiczny pakiet instalacyjny dla wybranej aplikacji już istnieje na Serwerze administracyjnym, kreator poinformuje o tym fakcie. W tym przypadku powinieneś wybrać jedno z następujących działań:

   - **Utwórz autonomiczny pakiet instalacyjny**. Wybierz tę opcję, na przykład, jeśli chcesz utworzyć autonomiczny pakiet instalacyjny dla nowej wersji aplikacji oraz chcesz zachować autonomiczny pakiet instalacyjny, który utworzyłeś dla poprzedniej wersji aplikacji. Nowy autonomiczny pakiet instalacyjny zostanie umieszczony w innym folderze.
   - **Użyj istniejącego autonomicznego pakietu instalacyjnego**. Wybierz tę opcję, jeśli chcesz użyć istniejącego autonomicznego pakietu instalacyjnego. Proces tworzenia pakietu nie zostanie uruchomiony.
   - **Ponownie skompiluj istniejący autonomiczny pakiet instalacyjny**. Wybierz tę opcję, jeśli ponownie chcesz utworzyć autonomiczny pakiet instalacyjny dla tej samej aplikacji. Autonomiczny pakiet instalacyjny znajduje się w tym samym folderze.

5. W kroku **Przenieś do listy zarządzanych urządzeń** domyślnie jest włączona opcja **Nie przenoś urządzeń**. Jeśli chcesz przenieść urządzenie klienckie do dowolnej grupy administracyjnej po zainstalowaniu Agenta sieciowego, pozostaw tę opcję włączoną.

   Jeśli chcesz przenieść urządzenie klienckie po instalacji Agenta sieciowego, wybierz opcję **Przenieś nieprzypisane urządzenia do tej grupy** i określ grupę administracyjną, do której chcesz przenieść urządzenie klienckie. Domyślnie, urządzenie zostanie przeniesione do grupy **Zarządzane urządzenia**.

6. Po zakończeniu procesu tworzenia autonomicznego pakietu instalacyjnego kliknij przycisk **ZAKOŃCZ**.

   Kreator tworzenia autonomicznego pakietu instalacyjnego zostanie zamknięty.

Autonomiczny pakiet instalacyjny jest tworzony i umieszczany w podfolderze PkgInst folderu współdzielonego Serwera administracyjnego. Możesz przejrzeć listę pakietów autonomicznych, klikając przycisk **Wyświetl listę pakietów autonomicznych** nad listą pakietów instalacyjnych.

Przeglądanie listy autonomicznych pakietów instalacyjnych

Możesz przejrzeć listę autonomicznych pakietów instalacyjnych i właściwości każdego autonomicznego pakietu instalacyjnego.

W celu przejrzenia listy autonomicznych pakietów instalacyjnych dla wszystkich pakietów instalacyjnych:

Nad listą kliknij przycisk **Wyświetl listę pakietów autonomicznych**.

Na liście autonomicznych pakietów instalacyjnych ich właściwości są wyświetlane w następujący sposób:

- **Nazwa pakietu**. Nazwa autonomicznego pakietu instalacyjnego, który jest automatycznie tworzony jako nazwa aplikacji znajdującej się w pakiecie oraz wersja aplikacji.
- **Nazwa aplikacji**. Nazwa aplikacji znajdującej się w autonomicznym pakiecie instalacyjnym.
- **Wersja aplikacji**.
- **Nazwa pakietu instalacyjnego Agenta sieciowego**. Właściwość jest wyświetlana tylko wtedy, gdy Agent sieciowy znajduje się w autonomicznym pakiecie instalacyjnym.
- **Wersja Agenta sieciowego**. Właściwość jest wyświetlana tylko wtedy, gdy Agent sieciowy znajduje się w autonomicznym pakiecie instalacyjnym.
- **Rozmiar**. Rozmiar pliku w MB.
- **Grupa**. Nazwa grupy, do której urządzenie klienckie jest przenoszone po zainstalowaniu Agenta sieciowego.
- **Utworzono**. Data i godzina utworzenia autonomicznego pakietu instalacyjnego.
- **Zmodyfikowano**. Data i godzina modyfikacji autonomicznego pakietu instalacyjnego.
- **Ścieżka dostępu**. Pełna ścieżka do folderu, w którym znajduje się autonomiczny pakiet instalacyjny.
- **Adres internetowy**. Adres internetowy lokalizacji autonomicznego pakietu instalacyjnego.
- **Suma kontrolna pliku**. Właściwość jest używana do potwierdzenia, że autonomiczny pakiet instalacyjny nie został zmieniony przez osoby trzecie, a użytkownik posiada ten sam plik, który utworzyłeś i przesłałeś do użytkownika.

W celu przejrzenia listy autonomicznych pakietów instalacyjnych dla określonego pakietu instalacyjnego:

Wybierz pakiet instalacyjny na liście i, nad listą, kliknij przycisk **Wyświetl listę pakietów autonomicznych**.

Na liście autonomicznych pakietów instalacyjnych możesz zrobić co następuje:

- Opublikować autonomiczny pakiet instalacyjny na serwerze sieciowym, klikając przycisk **Publikuj**. Opublikowany autonomiczny pakiet instalacyjny jest dostępny do pobrania dla użytkowników, do których wysłałeś odnośnik do autonomicznego pakietu instalacyjnego.
- Anulować publikację autonomicznego pakietu instalacyjnego na serwerze sieciowym, klikając przycisk **Cofnij publikowanie**. Nieopublikowany autonomiczny pakiet instalacyjny jest dostępny do pobrania tylko przez Ciebie i administratora.
- Pobrać autonomiczny pakiet instalacyjny na swoje urządzenie, klikając przycisk **Pobierz**.
- Wysłać e-mail z odnośnikiem do autonomicznego pakietu instalacyjnego, klikając przycisk **Wyślij przez e-mail**.
- Usunąć autonomiczny pakiet instalacyjny, klikając przycisk **Usuń**.

Tworzenie niestandardowego pakietu instalacyjnego

W celu wykonania następujących czynności możesz użyć niestandardowych pakietów instalacyjnych:

- Aby zainstalować dowolną aplikację (taką jak edytor tekstu) na urządzeniu klienckim, na przykład, przy użyciu zadania.
- Aby utworzyć autonomiczny pakiet instalacyjny.

Niestandardowy pakiet instalacyjny to folder z zestawem plików. Źródło utworzenia niestandardowego pakietu instalacyjnego to *plik archiwum*. Plik archiwum zawiera plik lub pliki, które muszą znajdować się w niestandardowym pakiecie instalacyjnym. Podczas tworzenia niestandardowego pakietu instalacyjnego możesz określić parametry wiersza poleceń, na przykład, aby zainstalować aplikację w trybie cichym.

Jeśli masz aktywny klucz licencyjny dla funkcji Zarządzanie lukami i poprawkami (VAPM), możesz przekonwertować domyślne ustawienia instalacji dla odpowiedniego niestandardowego pakietu instalacyjnego i użyć wartości zalecanych przez ekspertów z firmy Kaspersky. Ustawienia są automatycznie konwertowane podczas tworzenia niestandardowego pakietu instalacyjnego tylko wtedy, gdy odpowiedni plik wykonywalny znajduje się w bazie danych aplikacji firm trzecich Kaspersky.

W celu utworzenia niestandardowego pakietu instalacyjnego:

1. Wykonaj jedną z poniższych czynności:
   - W menu głównym przejdź do **Wykrywanie i wdrażanie → Wdrażanie i przypisywanie → Pakiety instalacyjne**.
   - W menu głównym przejdź do **Operacje → Repozytoria → Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Wybierz opcję **Utwórz pakiet instalacyjny z pliku**.

4. Podaj nazwę pakietu i kliknij przycisk **Przeglądaj**.

   Zostanie otwarte standardowe okno **Otwórz** w przeglądarce, aby pomóc w wybraniu pliku do utworzenia pakietu instalacyjnego.

5. Wybierz plik archiwum znajdujący się na dostępnych dyskach.

   Możesz przesłać plik archiwum ZIP, CAB, TAR lub TAR.GZ. Nie jest możliwe utworzenie pakietu instalacyjnego z pliku SFX (samorozpakowujące się archiwum).

   > Jeśli chcesz, aby ustawienia zostały przekonwertowane podczas instalacji pakietu, upewnij się, że pole wyboru **Konwertuj ustawienia na zalecane wartości dla aplikacji rozpoznawanych przez Kaspersky Security Center po zakończeniu pracy kreatora** jest zaznaczone, a następnie kliknij **Dalej**.

   Rozpocznie się przesyłanie pliku na Serwer administracyjny Kaspersky Security Center.

   > Jeśli włączono korzystanie z zalecanych ustawień instalacji, Kaspersky Security Center 15.1 sprawdzi, czy plik wykonywalny znajduje się w bazie danych aplikacji firm trzecich Kaspersky. Jeśli sprawdzenie się powiedzie, otrzymasz powiadomienie informujące, że plik został rozpoznany. Ustawienia są konwertowane i tworzony jest niestandardowy pakiet instalacyjny. Dalsze działania nie są wymagane. W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

6. Wybierz plik (z listy plików, które są wypakowywane z wybranego pliku archiwum) i określ parametry wiersza poleceń pliku wykonywalnego.

   Możesz określić parametry wiersza poleceń, aby zainstalować aplikację z pakietu instalacyjnego w trybie cichym. Określanie parametrów wiersza poleceń jest opcjonalne.

   Zostanie uruchomiony proces tworzenia pakietu instalacyjnego.

   Kreator informuje, gdy proces zostanie zakończony.

   Jeśli pakiet instalacyjny nie zostanie utworzony, zostanie wyświetlona odpowiednia wiadomość.

7. W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

Pakiet instalacyjny, który utworzyłeś, zostanie pobrany do podfolderu Packages folderu współdzielonego Serwera administracyjnego. Po pobraniu, pakiet instalacyjny pojawi się na liście pakietów instalacyjnych.

Na liście pakietów instalacyjnych dostępnych na Serwerze administracyjnym, klikając odnośnik z nazwą niestandardowego pakietu instalacyjnego, możesz:

- Wyświetl następujące właściwości pakietu instalacyjnego:
  - **Nazwa**. Nazwa niestandardowego pakietu instalacyjnego.
  - **Źródło**. Nazwa producenta aplikacji.
  - **Aplikacja**. Nazwa aplikacji spakowanej w niestandardowy pakiet instalacyjny.
  - **Wersja**. Wersja aplikacji.

- **Język**. Wersja językowa aplikacji spakowanej w niestandardowy pakiet instalacyjny.
- **Rozmiar (MB)**. Rozmiar pakietu instalacyjnego.
- **System operacyjny**. Typ systemu operacyjnego, dla którego przeznaczony jest pakiet instalacyjny.
- **Utworzono**. Data utworzenia pakietu instalacyjnego.
- **Zmodyfikowano**. Data modyfikacji pakietu instalacyjnego.
- **Typ**. Typ pakietu instalacyjnego.

- Zmień nazwę pakietu instalacyjnego i parametry wiersza poleceń. Ta funkcja jest dostępna tylko dla pakietów, które nie są tworzone w oparciu o aplikacje Kaspersky.

Jeśli dla procesu tworzenia pakietu niestandardowego przekonwertowałeś ustawienia instalacji pakietu na zalecane wartości, na zakładce **Ustawienia** we właściwościach niestandardowego pakietu instalacyjnego mogą pojawić się dwie dodatkowe sekcje: **Ustawienia** i **Procedura instalacji**.

Sekcja **Ustawienia** zawiera następujące właściwości, wyświetlane w tabeli:

- **Nazwa**. W tej kolumnie wyświetlana jest nazwa przypisana do parametru instalacji.
- **Typ**. Ta kolumna pokazuje typ parametru instalacji.
- **Wartość**. Ta kolumna pokazuje typ danych zdefiniowany przez parametr instalacji (Boolowski, Ścieżka pliku, Liczbowy, Ścieżka lub Ciąg znaków).

Sekcja **Procedura instalacji** zawiera tabelę opisującą następujące właściwości aktualizacji zawartej w niestandardowym pakiecie instalacyjnym:

- **Nazwa**. Nazwa aktualizacji.
- **Opis**. Opis aktualizacji.
- **Źródło**. Źródło aktualizacji, czyli czy została ona wydana przez firmę Microsoft, czy przez inną niezależną firmę.
- **Typ**. Rodzaj aktualizacji, czyli czy jest przeznaczona dla sterownika czy aplikacji.
- **Kategoria**. Kategoria Windows Server Update Services (WSUS) wyświetlana dla aktualizacji firmy Microsoft (aktualizacje krytyczne, aktualizacje definicji, sterowniki, pakiety funkcji, aktualizacje zabezpieczeń, dodatki Service Pack, narzędzia, pakiety zbiorcze aktualizacji, aktualizacje lub uaktualnienie).
- **Poziom ważności zgodnie z MSRC**. Istotność aktualizacji określona przez Microsoft Security Response Center (MSRC).
- **Priorytet**. Istotność aktualizacji określona przez Kaspersky.
- **Poziom ważności poprawki (dla poprawek przeznaczonych dla aplikacji Kaspersky)**. Istotność poprawki, jeśli jest ona przeznaczona dla aplikacji Kaspersky.
- **Artykuł**. Identyfikator (ID) artykułu w bazie wiedzy opisującego aktualizację.
- **Biuletyn**. Identyfikator biuletynu zabezpieczeń opisującego aktualizację.

- **Nie jest przeznaczony do instalacji**. Wyświetla, czy aktualizacja ma stan Nieprzypisane do instalacji.
- **Do zainstalowania**. Wyświetla, czy aktualizacja ma stan Do zainstalowania.
- **Instalowanie**. Wyświetla, czy aktualizacja ma stan Instalowanie.
- **Zainstalowana**. Wyświetla, czy aktualizacja ma stan Zainstalowana.
- **Niepowodzenie**. Wyświetla, czy aktualizacja ma stan Niepowodzenie.
- **Wymagane ponowne uruchomienie**. Wyświetla, czy aktualizacja ma stan Wymagane ponowne uruchomienie.
- **Zarejestrowano**. Wyświetla datę i godzinę rejestracji aktualizacji.
- **Instalacja w trybie interaktywnym**. Wyświetla, czy aktualizacja wymaga interakcji z użytkownikiem podczas instalacji.
- **Odwołano**. Wyświetla datę i godzinę odwołania aktualizacji.
- **Stan zatwierdzenia aktualizacji**. Wyświetla, czy aktualizacja została zatwierdzona do instalacji.
- **Wersja**. Wyświetla aktualny numer wersji aktualizacji.
- **Identyfikator aktualizacji**. Wyświetla identyfikator aktualizacji.
- **Wersja aplikacji**. Wyświetla numer wersji, do jakiej aplikacja zostanie zaktualizowana.
- **Zastąpiono**. Wyświetla inne aktualizacje, które mogą zastąpić aktualizację.
- **Zastępowanie**. Wyświetla inne aktualizacje, które mogą zostać zastąpione przez aktualizację.
- **Należy zaakceptować warunki Umowy licencyjnej**. Wyświetla, czy aktualizacja wymaga akceptacji warunków Umowy licencyjnej użytkownika końcowego (EULA).
- **Producent**. Wyświetla nazwę producenta aktualizacji.
- **Rodzina aplikacji**. Wyświetla nazwę rodziny aplikacji, do której należy aktualizacja.
- **Aplikacja**. Wyświetla nazwę aplikacji, do której należy aktualizacja.
- **Język**. Wyświetla język aktualizacji.
- **Nie przypisano do instalacji (nowa wersja)**. Wyświetla, czy aktualizacja ma stan Nie przypisano do instalacji (nowa wersja).
- **Wymaga instalacji wymagań wstępnych**. Wyświetla, czy aktualizacja ma stan Wymaga instalacji wymagań wstępnych.
- **Tryb pobierania**. Wyświetla tryb pobierania aktualizacji.
- **To aktualizacja**. Wyświetla, czy aktualizacja jest poprawką.
- **Nie zainstalowano**. Wyświetla, czy aktualizacja ma stan Nie zainstalowano.

Rozsyłanie pakietów instalacyjnych na podrzędne Serwery administracyjne

Kaspersky Security Center umożliwia tworzenie pakietów instalacyjnych dla aplikacji firmy Kaspersky i aplikacji firm trzecich, a także dystrybucję pakietów instalacyjnych na urządzeniach klienckich i instalowanie aplikacji z pakietów. Aby zoptymalizować obciążenie głównego Serwera administracyjnego, możesz rozesłać pakiety instalacyjne do podrzędnych Serwerów administracyjnych. Serwery pomocnicze przesyłają pakiety do urządzeń klienckich, a następnie można przeprowadzić zdalną instalację aplikacji na urządzeniach klienckich.

W celu rozesłania pakietów instalacyjnych na podrzędne Serwery administracyjne:

1. Upewnij się, że podrzędne Serwery administracyjne są połączone z głównym Serwerem administracyjnym.
2. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.

   Zostanie wyświetlona lista zadań.
3. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
4. Na stronie **Ustawienia nowych zadań**, z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Security Center**. Następnie z listy rozwijanej **Typ zadania** wybierz opcję **Rozsyłanie pakietu instalacyjnego**, a następnie określ nazwę zadania.
5. Na stronie **Zakres zadania** wybierz urządzenia, do których zadanie jest przypisane w jeden z następujących sposobów:
   - Jeśli chcesz utworzyć zadanie dla wszystkich podrzędnych Serwerów administracyjnych w określonej grupie administracyjnej, wybierz tę grupę, a następnie utwórz dla niej zadanie grupowe.
   - Jeśli chcesz utworzyć zadanie dla określonych podrzędnych Serwerów administracyjnych, wybierz te Serwery, a następnie utwórz dla nich zadanie.
6. Na stronie **Rozesłane pakiety instalacyjne** wybierz pakiety instalacyjne, które mają zostać skopiowane na podrzędne Serwery administracyjne.
7. Określ konto, aby uruchomić zadanie *Dystrybucja pakietu instalacyjnego w* ramach tego konta. Możesz użyć swojego konta i pozostawić włączoną opcję **Konto domyślne**. Alternatywnie można określić, że zadanie powinno być uruchamiane na innym koncie, które ma niezbędne prawa dostępu. Aby to zrobić, wybierz opcję **Określ konto**, a następnie wprowadź poświadczenia tego konta.
8. Na stronie **Zakończ tworzenie zadania** możesz włączyć opcję **Otwórz szczegóły zadania po jego utworzeniu**, aby otworzyć okno właściwości zadania i zmodyfikować domyślne ustawienia zadania. W przeciwnym razie możesz skonfigurować ustawienia zadania później, w dowolnym momencie.

9. Kliknij przycisk **Zakończ**.

   Zadanie utworzone w celu dystrybucji pakietów instalacyjnych na podrzędne Serwery administracyjne jest wyświetlane na liście zadań.

10. Możesz uruchomić zadanie ręcznie lub poczekać na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania wybrane pakiety instalacyjne są kopiowane na określone podrzędne Serwery administracyjne.

Instalowanie aplikacji przy pomocy zadania zdalnej instalacji

Kaspersky Security Center umożliwia zdalne instalowanie aplikacji na urządzeniach przy użyciu zadań zdalnej instalacji. Te zadania są tworzone i przydzielane do urządzeń za pośrednictwem dedykowanego kreatora. W celu szybkiego i łatwego przypisywania zadań do urządzeń, możesz wskazać urządzenia (maksymalnie do 1000 urządzeń) w oknie kreatora w jeden z następujących sposobów:

- **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**. W tym przypadku zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**. Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.
- **Przypisz zadanie do wyboru urządzeń**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonym wyborze. Możesz określić predefiniowany lub niestandardowy wybór, który utworzyłeś.
- **Przypisz zadanie do grupy administracyjnej**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonej grupie administracyjnej.

Aby uniknąć problemów, które mogą wystąpić podczas instalacji aplikacji na urządzeniu klienckim bez zainstalowanego Agenta sieciowego, należy postępować zgodnie z opisem procedury wymuszonego wdrożenie przy użyciu zadania zdalnej instalacji z Kaspersky Security Center.

Zdalna instalacja aplikacji

Ta sekcja zawiera informacje na temat zdalnej instalacji aplikacji na grupie administracyjnej, urządzeniach o określonych adresach IP lub wybranych zarządzanych urządzeniach.

W celu zainstalowania aplikacji na określonych urządzeniach:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.

3. W polu **Typ zadania** wybierz **Zdalna instalacja aplikacji**.

4. Wybierz jedną z następujących opcji:

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

     Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

   - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

     Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

     Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

   - **Przypisz zadanie do wyboru urządzeń**

     Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

   Zadanie *Zdalna instalacja aplikacji* jest tworzone dla określonych urządzeń. Jeśli wybrano opcję **Przypisz zadanie do grupy administracyjnej**, zadanie jest zadaniem grupowym.

5. W kroku **Zakres zadania** określ grupę administracyjną, urządzenia o określonych adresach lub wybór urządzeń.

   Dostępne ustawienia zależą od opcji wybranej w poprzednim kroku.

6. W kroku **Pakiety instalacyjne** określ następujące ustawienia:

   - W polu **Wybierz pakiet instalacyjny** wskaż pakiet instalacyjny aplikacji, którą chcesz zainstalować.

   - W grupie ustawień **Wymuś pobranie pakietu instalacyjnego** określ sposób rozsyłania na urządzenia klienckie plików, które są niezbędne do zainstalowania aplikacji.

     - **Przy użyciu Agenta sieciowego**

       Jeśli ta opcja jest włączona, pakiety instalacyjne są dostarczane na urządzenia klienckie przez Agenta sieciowego zainstalowanego na tych urządzeniach klienckich.

       Jeśli ta opcja jest wyłączona, pakiety instalacyjne są dostarczane przy użyciu narzędzi systemu operacyjnego urządzeń klienckich.

       Zalecane jest włączenie tej opcji, jeśli zadanie zostało przypisane do urządzeń z zainstalowanymi Agentami sieciowymi.

       Domyślnie opcja ta jest włączona.

     - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**

       Jeśli ta opcja jest włączona, pakiety instalacyjne są przesyłane na urządzenia klienckie przy użyciu narzędzi systemu operacyjnego za pośrednictwem punktów dystrybucyjnych. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny.

Jeśli opcja **Przy użyciu Agenta sieciowego** jest włączona, pliki będą dostarczane przy użyciu narzędzi systemu operacyjnego, jeśli narzędzia Agenta sieciowego są niedostępne.

Domyślnie ta opcja jest włączona dla zadań zdalnej instalacji utworzonych na wirtualnym Serwerze administracyjnym.

> Jeśli wszystkie punkty dystrybucji przypisane do urządzenia okażą się wadliwe, urządzenie nie będzie otrzymywać aktualizacji (baz wirusów i poprawek) ani pakietów instalacyjnych.

- **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**

  Jeśli ta opcja jest włączona, pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego urządzeń klienckich za pośrednictwem Serwera administracyjnego. Możesz włączyć tę opcję, jeśli na urządzeniu klienckim nie ma zainstalowanego Agenta sieciowego, ale urządzenie klienckie jest w tej samej sieci co Serwer administracyjny.

  Domyślnie opcja ta jest włączona.

- W polu **Maksymalna liczba dla jednoczesnego pobierania** określ maksymalną dozwoloną liczbę urządzeń klienckich, do których Serwer administracyjny może jednocześnie przesyłać pliki.

- W polu **Maksymalna liczba prób instalacji** określ maksymalną dozwoloną liczbę uruchomień instalatora.

  Jeśli liczba prób określona w parametrze zostanie przekroczona, Kaspersky Security Center nie uruchomi już instalatora na urządzeniu. Aby ponownie uruchomić zadanie *Zainstaluj aplikację zdalnie*, zwiększ wartość parametru **Maksymalna liczba prób instalacji** i uruchom zadanie. W razie czego możesz utworzyć nowe zadanie *Install application remotely*.

- Jeśli przeprowadzasz migrację z jednej aplikacji Kaspersky do drugiej, a bieżąca aplikacja jest chroniona hasłem, wprowadź hasło w polu **Hasło do odinstalowania bieżącej aplikacji Kaspersky**. Pamiętaj, że podczas migracji bieżąca aplikacja Kaspersky zostanie odinstalowana.

  > Pole **Hasło do odinstalowania bieżącej aplikacji Kaspersky** jest dostępne tylko wtedy, gdy w grupie ustawień **Przy użyciu Agenta sieciowego** została wybrana opcja **Wymuś pobranie pakietu instalacyjnego**.

  > Hasła dezinstalacji możesz użyć tylko w przypadku scenariusza migracji Kaspersky Security for Windows Server do Kaspersky Endpoint Security for Windows podczas instalacji Kaspersky Endpoint Security for Windows przy użyciu zadania Zdalna instalacja aplikacji. Użycie hasła dezinstalacyjnego podczas instalowania innych komponentów może spowodować błędy instalacji.

  Aby pomyślnie zakończyć scenariusz migracji, upewnij się, że spełnione są następujące wymagania wstępne:

  - Używasz Agenta sieciowego Kaspersky Security Center 14.2 dla Windows lub nowszej wersji.
  - Instalujesz aplikację na urządzeniach z systemem Windows.

- Określ ustawienie dodatkowe:

  - **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana**

    Jeśli ta opcja jest włączona, wybrana aplikacja nie zostanie ponownie zainstalowana, jeśli już jest zainstalowana na tym urządzeniu klienckim.

    Jeśli ta opcja jest wyłączona, aplikacja zostanie zainstalowana mimo wszystko.

Domyślnie opcja ta jest włączona.

- **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**

  Przed przesłaniem plików na urządzenia klienckie program Kaspersky Security Center sprawdza, czy ustawienia narzędzia do instalacji są stosowane do systemu operacyjnego urządzenia klienckiego. Jeśli ustawienia nie są stosowane, Kaspersky Security Center nie przesyła plików i nie próbuje zainstalować aplikacji. Na przykład, aby zainstalować aplikację Windows na urządzenia grupy administracyjnej, która zawiera urządzenia działające pod kontrolą różnych systemów operacyjnych, możesz przypisać zadanie instalacji do grupy administracyjnej, a następnie włączyć tę opcję, aby pominąć urządzenia, na których jest uruchomiony system operacyjny inny niż Windows.

  Podczas zdalnej instalacji Agenta sieciowego na nieprzypisanych urządzeniach, Kaspersky Security Center lub punkt dystrybucji automatycznie ustala typ systemu operacyjnego urządzenia, niezależnie od ustawienia **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**.

- **Przypisz pakiet instalacyjny do zasad grupy Active Directory**

  Jeśli ta opcja jest włączona, pakiet instalacyjny jest instalowany przy użyciu zasad grupy Active Directory.

  Ta opcja jest dostępna, jeśli wybrany jest pakiet instalacyjny Agenta sieciowego.

  Domyślnie opcja ta jest wyłączona.

- **Poproś użytkowników o zamknięcie uruchomionych aplikacji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

- Wybierz na jakich urządzeniach chcesz zainstalować aplikację:

  - **Zainstaluj na wszystkich urządzeniach**

    Aplikacja zostanie zainstalowana nawet na urządzeniach zarządzanych przez inne Serwery administracyjne.

    Opcja ta jest wybrana domyślnie. Nie musisz zmieniać tego ustawienia, jeśli masz tylko jeden Serwer administracyjny w swojej sieci.

  - **Zainstaluj tylko na urządzeniach zarządzanych przez ten Serwer administracyjny**

    Aplikacja zostanie zainstalowana tylko na urządzeniach zarządzanych przez ten Serwer administracyjny. Wybierz tę opcję, jeśli posiadasz więcej niż jeden Serwer administracyjny w swojej sieci i chcesz uniknąć konfliktów między nimi.

- Określ, czy urządzenia powinny zostać przeniesione do grupy administracyjnej po instalacji:

  - **Nie przenoś urządzeń**

    Urządzenia pozostają w grupach, w których aktualnie się znajdują. Urządzenia, które zostały umieszczone w dowolnej grupie, pozostaną nieprzypisane.

  - **Przenieś urządzenia nieprzypisane do wybranej grupy (można wybrać tylko jedną grupę)**

    Urządzenia są przenoszone do wybranej grupy administracyjnej.

  Zwróć uwagę, że opcja **Nie przenoś urządzeń** została wybrana domyślnie. W celach bezpieczeństwa możesz ręcznie przenieść urządzenia.

7. W tym kroku kreatora określ, czy urządzenia mają zostać ponownie uruchomione podczas instalacji aplikacji:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

  - **Uruchom ponownie po (min)**

    Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

    Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

8. W razie potrzeby w kroku **Wybierz konta w celu uzyskania dostępu do urządzeń** dodaj konta, które będą używane do uruchomienia zadania *Zdalna instalacja aplikacji*.

   - **Konto nie jest wymagane (Agent sieciowy jest zainstalowany)**

     Jeśli ta opcja jest zaznaczona, nie musisz określić konta, z poziomu którego zostanie uruchomiony instalator aplikacji. Zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

     Jeśli Agent sieciowy nie został zainstalowany na urządzeniach klienckich, ta opcja nie będzie dostępna.

   - **Konto wymagane (Agent sieciowy nie jest używany)**

     Wybierz tę opcję, jeśli Agent sieciowy nie jest zainstalowany na urządzeniach, do których przypisano zadanie zdalnej instalacji. W takim przypadku możesz określić konto użytkownika lub certyfikat SSH, aby zainstalować aplikację.

     - **Konto lokalne**. Jeśli ta opcja jest zaznaczona, określ konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji. Kliknij przycisk **Dodaj**, wybierz **Konto lokalne**, a następnie określ poświadczenia konta użytkownika.

       Możesz określić wiele kont użytkowników, jeśli na przykład żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, do których przypisujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

     - **Certyfikat SSH**. Jeśli chcesz zainstalować aplikację na urządzeniu klienckim opartym na systemie Linux, możesz określić certyfikat SSH zamiast konta użytkownika. Kliknij przycisk **Dodaj**, wybierz **Certyfikat SSH**, a następnie określ klucze prywatny i publiczny certyfikatu.

       Aby wygenerować klucz prywatny, możesz użyć narzędzia ssh-keygen. Należy zauważyć, że Kaspersky Security Center obsługuje format PEM kluczy prywatnych, ale narzędzie ssh-keygen domyślnie generuje klucze SSH w formacie OPENSSH. Format OPENSSH nie jest obsługiwany przez Kaspersky Security Center. Aby utworzyć klucz prywatny w obsługiwanym formacie PEM, dodaj opcję -m PEM w poleceniu ssh-keygen. Na przykład:

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "< adres e-mail użytkownika >"
       ```

9. Na etapie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby utworzyć zadanie i zamknąć kreatora.

   Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, zostanie otwarte okno ustawień zadania. W tym oknie możesz sprawdzić parametry zadania, zmodyfikować je lub skonfigurować harmonogram uruchamiania zadania, jeśli to konieczne.

10. Na liście zadań wybierz utworzone zadanie, a następnie kliknij przycisk **Start**.

    Ewentualnie poczekaj na uruchomienie zadania zgodnie z harmonogramem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji wybrana aplikacja zostanie zainstalowana na określonych urządzeniach.

Instalowanie aplikacji przy użyciu zasad grupy Active Directory

Kaspersky Security Center pozwala na instalowanie aplikacji Kaspersky na zarządzanych urządzeniach przy użyciu zasad grupy Active Directory.

Możesz zainstalować aplikacje, korzystając z zasad grupy Active Directory jedynie przy pomocy pakietów instalacyjnych, które zawierają Agenta sieciowego.

W celu zainstalowania aplikacji przy użyciu zasad grupy Active Directory:

1. Uruchom Kreator wdrażania ochrony. Postępuj zgodnie z instrukcjami kreatora.
2. Na stronie **Ustawienia zadania zdalnej instalacji** Kreatora wdrażania ochrony włącz opcję **Przypisz pakiet instalacyjny do zasad grupy Active Directory**.
3. Na stronie **Wybierz konta w celu uzyskania dostępu do urządzeń** wybierz opcję **Konto wymagane (Agent sieciowy nie jest używany)**.
4. Dodaj konto z uprawnieniami administratora na urządzeniu, na którym jest zainstalowany program Kaspersky Security Center, lub konto, które należy do grupy domeny Twórcy-właściciele zasad grupy.
5. Nadaj wybranemu kontu następujące uprawnienia:
   a. Przejdź do **Panel sterowania** → **Narzędzia administracyjne** i otwórz **Zarządzanie zasadami grupy**.
   b. Kliknij węzeł z żądaną domeną.
   c. Kliknij sekcję **Delegowanie**.
   d. Na liście rozwijanej **Uprawnienia** wybierz opcję **Połącz obiekty zasad grupy**.
   e. Kliknij **Dodaj**.
   f. W otwartym oknie **Wybierz Użytkownika, Komputer lub Grupę** wybierz żądane konto.
   g. Kliknij **OK**, aby zamknąć okno **Wybierz Użytkownika, Komputer lub Grupę**.
   h. Na liście **Grupy i użytkownicy** wybierz konto, które zostało dodane, a następnie kliknij **Zaawansowane** → **Zaawansowane**.
   i. Na liście **Wpisy uprawnień** kliknij dwukrotnie konto, które tyle co dodałeś.
   j. Nadaj następujące uprawnienia:
      - **Utwórz obiekty grupy**
      - **Usuń obiekty grupy**

- **Utwórz obiekty kontenera zasad grupy**
- **Usuń obiekty kontenera zasad grupy**

k. Kliknij **OK**, aby zachować zmiany.

6. Określ inne ustawienia, postępując zgodnie z instrukcjami kreatora.
7. Uruchom utworzone zadanie zdalnej instalacji ręcznie lub zaczekaj na jego uruchomienie zgodne z terminarzem.

Rozpocznie się następująca sekwencja zdalnej instalacji:

1. Po uruchomieniu zadania, w każdej domenie, do której należą urządzenia klienckie z określonego zbioru, zostaną utworzone następujące obiekty:
   - Obiekt zasad grupy (GPO) o nazwie **Kaspersky_AK{GUID}**.
   - Grupa bezpieczeństwa, która odpowiada GPO. Ta grupa bezpieczeństwa zawiera urządzenia klienckie objęte zadaniem. Zawartość grupy bezpieczeństwa określa zakres GPO.
2. Kaspersky Security Center instaluje wybrane aplikacje firmy Kaspersky na urządzeniach klienckich bezpośrednio z sieciowego folderu współdzielonego KLSHARE. W folderze instalacyjnym Kaspersky Security Center zostanie utworzony pomocniczy podfolder, zawierający plik .msi potrzebny do zainstalowania aplikacji.
3. Po dodaniu nowych urządzeń do obszaru zadania, są one dodawane do grupy bezpieczeństwa podczas kolejnego uruchomienia zadania. Jeśli w harmonogramie zadań wybrana jest opcja **Uruchom pominięte zadania**, urządzenia są dodawane do grupy zabezpieczeń od razu.
4. Po usunięciu urządzeń z obszaru zadania, są one usuwane z grupy zabezpieczeń podczas kolejnego uruchomienia zadania.
5. Po usunięciu zadania z Active Directory, usuwany jest GPO, odnośnik do GPO oraz odpowiadająca mu grupa zabezpieczeń.

Jeżeli chcesz zastosować inny schemat instalacji przy użyciu Active Directory, możesz ręcznie skonfigurować żądane ustawienia. Na przykład, może to być wymagane w następujących wypadkach:

- Jeśli administrator ochrony antywirusowej nie ma uprawnień do wprowadzania zmian w Active Directory pewnych domen
- Jeśli oryginalny pakiet instalacyjny musi być przechowywany w oddzielnym zasobie sieciowym
- Jeśli konieczne jest połączenie GPO z określonymi jednostkami Active Directory

Dostępne są następujące opcje korzystania z alternatywnego scenariusza instalacji poprzez Active Directory:

- W przypadku, gdy instalacja musi być przeprowadzona bezpośrednio z folderu współdzielonego Kaspersky Security Center, we właściwościach GPO musisz określić plik msi zlokalizowany w podfolderze exec folderu pakietu instalacyjnego żądanej aplikacji.
- Jeżeli pakiet instalacyjny ma znajdować się w innym zasobie sieciowym, skopiuj do niego całą zawartość foldera exec. Jest to konieczne, gdyż oprócz pliku z rozszerzeniem .msi folder zawiera pliki konfiguracyjne wygenerowane podczas tworzenia pakietu. W celu zainstalowania aplikacji wraz z kluczem licencyjnym, skopiuj do tego folderu także plik klucza.

Instalowanie aplikacji na podrzędnych Serwerach administracyjnych

W celu zainstalowania aplikacji na podrzędnych Serwerach administracyjnych:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednie podrzędne Serwery administracyjne.
2. Upewnij się, że pakiet instalacyjny dla instalowanej aplikacji znajduje się na każdym z wybranych podrzędnych Serwerów administracyjnych. Jeśli nie możesz znaleźć pakietu instalacyjnego na żadnym z serwerów podrzędnych, dystrybuuj go. W tym celu utwórz zadanie z typem zadania **Rozsyłanie pakietu instalacyjnego**.
3. Utwórz zadanie zdalnej instalacji aplikacji na podrzędnych Serwerach administracyjnych. Wybierz typ zadania **Zdalna instalacja aplikacji na podrzędnym Serwerze administracyjnym**.

   Kreator nowego zadania tworzy zadanie zdalnej instalacji aplikacji wybranej w Kreatorze na określonych podrzędnych Serwerach administracyjnych.
4. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji wybrana aplikacja zostanie zainstalowana na podrzędnych Serwerach administracyjnych.

Określanie ustawień zdalnej instalacji na urządzeniach z systemem Unix

Podczas instalowania aplikacji na urządzeniu z systemem UNIX przy użyciu zadania instalacji zdalnej można określić ustawienia zadania specyficzne dla systemu Unix. Te ustawienia są dostępne we właściwościach zadania po jego utworzeniu.

W celu określenia ustawień specyficznych dla systemu Unix dla zadania zdalnej instalacji:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij nazwę zadania zdalnej instalacji, dla którego chcesz określić ustawienia specyficzne dla systemu Unix.

   Zostanie otwarte okno właściwości zadania.
3. Przejdź do **Ustawienia aplikacji** → **Ustawienia specyficzne dla systemu Unix**.
4. Określ następujące ustawienia:

   - **Ustaw hasło do konta root (tylko do wdrożenia przez SSH)**

     Jeśli polecenie `sudo` nie może być używane na urządzeniu docelowym bez określenia hasła, wybierz tę opcję, a następnie określ hasło dla konta root. Kaspersky Security Center przesyła hasło w postaci zaszyfrowanej na urządzenie docelowe, odszyfrowuje hasło, a następnie rozpoczyna procedurę instalacji w imieniu konta root z określonym hasłem.

     Kaspersky Security Center nie używa konta ani określonego hasła do tworzenia połączenia SSH.

- **Określ ścieżkę do folderu tymczasowego z uprawnieniami do wykonywania na urządzeniu docelowym (tylko do wdrożenia przez SSH)**

  Jeśli katalog /tmp na urządzeniu docelowym nie ma uprawnień do wykonywania, wybierz tę opcję, a następnie określ ścieżkę do katalogu z uprawnieniem do wykonywania. Kaspersky Security Center używa określonego katalogu jako katalogu tymczasowego w celu uzyskania dostępu przez SSH. Aplikacja umieszcza pakiet instalacyjny w katalogu i uruchamia procedurę instalacji.

5. Kliknij przycisk **Zapisz**.

Określone ustawienia zadania zostaną zapisane.

Uruchamianie i zatrzymywania działania aplikacji Kaspersky

Możesz użyć zadania *Uruchom lub zatrzymaj aplikację* do uruchamiania i zatrzymywania aplikacji Kaspersky na zarządzanych urządzeniach.

Aby utworzyć zadanie Uruchom lub zatrzymaj aplikację:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Z listy rozwijanej **Aplikacja** wybierz aplikację, do której chcesz utworzyć zadanie.

   Aplikacje Kaspersky są wyświetlane na liście, jeśli wcześniej dodałeś webowe wtyczki administracyjne dla tych aplikacji.
4. Z listy **Typ zadania** wybierz zadanie **Aktywacja aplikacji**.
5. W polu **Nazwa zadania** podaj nazwę nowego zadania.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).
6. Wybierz urządzenia, do których zadanie zostanie przypisane.
7. W oknie **Aplikacje** wykonaj następujące czynności:

   - Zaznacza pola obok nazw aplikacji, dla których chcesz utworzyć zadanie.
   - Wybierz opcję **Uruchom aplikację** lub **Zatrzymaj aplikację**.
8. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** w kroku **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
9. Kliknij przycisk **Zakończ**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

10. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

11. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami, a następnie zapisz ustawienia.

Zadanie zostało utworzone i skonfigurowane.

Aby uruchomić zadanie, na liście zadań wybierz zadanie i kliknij przycisk **Uruchom**.

Zarządzanie urządzeniami mobilnymi

Zarządzanie ochroną urządzeń mobilnych poprzez Kaspersky Security Center jest realizowane przy użyciu funkcji Zarządzanie urządzeniami mobilnymi, która wymaga dedykowanej licencji. Jeśli zamierzasz zarządzać urządzeniami mobilnymi należącymi do pracowników Twojej organizacji, włącz i skonfigurować Zarządzanie urządzeniami mobilnymi.

Zarządzanie urządzeniami mobilnymi umożliwia zarządzanie urządzeniami z systemem Android należącymi do pracowników. Ochronę zapewnia aplikacja mobilna Kaspersky Endpoint Security for Android zainstalowana na urządzeniach. Ta aplikacja mobilna zapewnia ochronę urządzeń mobilnych przed zagrożeniami internetowymi, wirusami i innymi programami stanowiącymi zagrożenie. W celu scentralizowanego zarządzania przez konsolę Kaspersky Security Center Web Console musisz zainstalować następujące wtyczki do zarządzania siecią na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console:

- Wtyczka Kaspersky Security for Mobile
- Wtyczka Kaspersky Endpoint Security for Android

Aby uzyskać informacje na temat wdrażania ochrony i zarządzania urządzeniami mobilnymi, zapoznaj się z pomocą dla Kaspersky Security for Mobile.

Modyfikowanie ustawień Zarządzania urządzeniami mobilnymi w Kaspersky Security Center Web Console

W celu zmodyfikowania ustawień Zarządzania urządzeniami mobilnymi:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Porty dodatkowe**.

3. Zmodyfikuj odpowiednie ustawienia:

   - **Otwórz port dla urządzeń mobilnych**

     Jeśli ta opcja jest włączona, port dla urządzeń mobilnych zostanie otwarty na Serwerze administracyjnym.

     Port dla urządzeń mobilnych może zostać użyty tylko wtedy, gdy zainstalowany jest komponent Zarządzanie urządzeniami mobilnymi.

     Jeśli ten przełącznik jest wyłączony, port dla urządzeń mobilnych na Serwerze administracyjnym nie będzie używany.

     Domyślnie ten przełącznik jest wyłączony.

- **Port do synchronizacji urządzeń mobilnych**

  Numer portu używanego dla połączenia nawiązywanego między urządzeniami mobilnymi a Serwerem administracyjnym. Domyślny numer portu to 13292.

  Używany jest system dziesiętny.

- **Port do aktywacji urządzeń mobilnych**

  Port do łączenia Kaspersky Endpoint Security for Android z serwerami aktywacji Kaspersky.

  Domyślny numer portu to 17100.

4. Kliknij przycisk **Zapisz**.

Urządzenia mobilne mogą nawiązywać połączenie z Serwerem administracyjnym.

Zastępowanie aplikacji zabezpieczających firm trzecich

Instalacja aplikacji zabezpieczających firmy Kaspersky poprzez Kaspersky Security Center może wymagać usunięcia oprogramowania firmy trzeciej niekompatybilnego z instalowaną aplikacją. Kaspersky Security Center oferuje kilka sposobów usunięcia aplikacji firm trzecich.

Usuwanie niekompatybilnych aplikacji przy użyciu instalatora

Ta opcja jest dostępna tylko w Konsoli administracyjnej opartej na konsoli Microsoft Management Console.

Metoda instalatora dotycząca usuwania niekompatybilnych aplikacji jest obsługiwana przez różne typy instalacji. Przed zainstalowaniem aplikacji zabezpieczającej wszystkie niekompatybilne aplikacje są usuwane automatycznie, jeśli w oknie właściwości pakietu instalacyjnego tej aplikacji zabezpieczającej (sekcja **Niekompatybilne aplikacje**) wybrano opcję **Automatycznie odinstaluj niekompatybilne aplikacje**.

Usuwanie niekompatybilnych aplikacji podczas konfigurowania zdalnej instalacji aplikacji

Możesz włączyć opcję **Automatycznie odinstaluj niekompatybilne aplikacje**, gdy konfigurujesz zdalną instalację aplikacji zabezpieczającej. W Konsoli administracyjnej opartej na Microsoft Management Console (MMC) ta opcja jest dostępna w kreatorze zdalnej instalacji. W Kaspersky Security Center Web Console tę opcję można znaleźć w kreatorze wdrażania ochrony. Jeśli ta opcja jest włączona, Kaspersky Security Center usunie niekompatybilne aplikacje przed zainstalowaniem aplikacji zabezpieczającej na zarządzanym urządzeniu.

Dostępne instrukcje:

- Konsola administracyjna: Usuwanie niekompatybilnych aplikacji przy pomocy Kreatora zdalnej instalacji
- Kaspersky Security Center Web Console: Usuwanie niekompatybilnych aplikacji przed instalacją

Dezinstalowanie niekompatybilnych aplikacji przy użyciu dedykowanego zadania

Aby usunąć niekompatybilne aplikacje, użyj zadania **Zdalna dezinstalacja aplikacji**. Zadanie to powinno być uruchomione na urządzeniach przed zadaniem instalacji aplikacji zabezpieczającej. Na przykład, w zadaniu instalacji możesz wybrać opcję terminarza **Po zakończeniu wykonywania innego zadania**, gdzie inne zadanie to **Zdalna dezinstalacja aplikacji**.

Ta metoda dezinstalacji jest przydatna, jeśli instalator aplikacji zabezpieczającej nie może skutecznie usunąć niekompatybilnej aplikacji.

Instrukcje dotyczące Konsoli administracyjnej: Tworzenie zadania.

Wykrywanie urządzeń w sieci

Ta sekcja opisuje wyszukiwanie i wykrywanie urządzeń w sieci.

Kaspersky Security Center umożliwia wyszukiwanie urządzeń w oparciu o określone kryteria. Wyniki wyszukiwania możesz zapisać do pliku tekstowego.

Opcja wyszukiwania i wykrywania pozwala znaleźć następujące urządzenia:

- Zarządzane urządzenia w grupach administracyjnych Serwera administracyjnego Kaspersky Security Center i jego podrzędnych Serwerów administracyjnych.
- Urządzenia nieprzypisane zarządzane przez Serwer administracyjny Kaspersky Security Center i jego podrzędne Serwery administracyjne.

Scenariusz: Wykrywanie urządzeń w sieci

Przed zainstalowaniem aplikacji zabezpieczających musisz przeprowadzić wykrywanie urządzeń. Serwer administracyjny otrzymuje informacje o wykrytych urządzeniach i umożliwia zarządzanie urządzeniami za pomocą zasad. Do aktualizacji listy urządzeń dostępnych w sieci potrzebne są regularne ankiety sieciowe.

Przed rozpoczęciem odpytywania sieci upewnij się, że protokół SMB jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Aby włączyć protokół SMB, postępuj zgodnie z instrukcjami dla swojego systemu operacyjnego.

Wykrywanie urządzeń sieciowych przebiega w następujących etapach:

1. **Odkryj urządzenia**

   Kreator wstępnej konfiguracji poprowadzi Cię przez wstępne wyszukiwanie urządzeń i pomoże w odnalezieniu urządzeń w sieci, takich jak komputery, tablety i telefony komórkowe. Możesz także ręcznie przeprowadzić wykrywanie urządzeń.

2. **Skonfiguruj zaplanowane ankiety**

   Zdecyduj, których typów przeszukiwania chcesz używać regularnie. Włącz żądane typy i skonfiguruj harmonogram ankiety. Możesz zapoznać się z zaleceniami dotyczącymi częstotliwości odpytywania sieci.

3. **Konfiguracja reguł dodawania wykrytych urządzeń do grup administracyjnych (opcjonalne)**

   Jeśli nowe urządzenia pojawią się w Twojej sieci, zostaną wykryte podczas regularnych przeszukiwań i zostaną automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**. Możesz skonfigurować reguły przenoszenia urządzeń, aby zautomatyzować przydzielanie urządzeń do grupy **Zarządzane urządzenia**. Możesz także skonfigurować reguły zatrzymania.

   Jeśli pominiesz krok 3, nowo wykryte urządzenia zostaną przydzielone do grupy **Urządzenia nieprzypisane**. Jeśli chcesz, możesz ręcznie przenieść te urządzenia do grupy **Zarządzane urządzenia**. Jeśli ręcznie przeniesiesz te urządzenia do grupy **Zarządzane urządzenia**, możesz przeanalizować informacje o każdym urządzeniu i zdecydować, czy chcesz przenieść je do grupy administracyjnej i do jakiej grupy.

Wyniki

Zakończenie scenariusza powoduje, że:

- Serwer administracyjny Kaspersky Security Center wykrywa urządzenia, które znajdują się w sieci, i zapewnia informacje o nich.
- Przyszłe przeszukiwania zostają skonfigurowane i przeprowadzone zgodnie z określonym terminarzem.
- Nowo wykryte urządzenia zostaną rozmieszczone zgodnie ze skonfigurowanymi regułami (lub jeśli nie ma skonfigurowanych reguł, urządzenia pozostają w grupie **Urządzenia nieprzypisane**).

Wykrywanie urządzeń

Ta sekcja opisuje typy wykrywania urządzeń dostępne w Kaspersky Security Center i oferuje informacje dotyczące korzystania z każdego typu.

Serwer administracyjny otrzymuje informacje o strukturze sieci i urządzeń w tej sieci poprzez regularne przeszukiwanie. Informacje są zapisywane w bazie danych Serwera administracyjnego. Serwer administracyjny może wykorzystywać następujące typy przeszukiwania:

- **Przeszukiwanie sieci Windows**. Serwer administracyjny może wykonywać dwa rodzaje przeszukiwań sieci Windows: szybkie i pełne. Podczas szybkiego przeszukiwania Serwer administracyjny pobiera wyłącznie informacje o urządzeniach znajdujących się na liście nazw NetBIOS wszystkich domen sieci i grup roboczych. Podczas pełnego przeszukiwania wymaganych jest więcej informacji z urządzenia klienckiego, takich jak: nazwa systemu operacyjnego, adres IP, nazwa DNS, nazwa NetBIOS. Domyślnie włączone są oba przeszukiwania: szybkie i pełne. Przeszukiwanie sieci Windows może nie wykryć urządzeń, na przykład, jeśli porty UDP 137, UDP 138, TCP 139 są zamknięte na routerze lub przez zaporę sieciową.
- **Przeszukiwanie sterowników domeny**. Serwer administracyjny lub punkt dystrybucji pobiera informacje o strukturze domeny i nazwach DNS urządzeń, które są zawarte w domenie. Domyślnie ten typ przeszukiwania jest włączony. Zalecamy korzystanie z przeszukiwania kontrolera domeny, jeśli wszystkie urządzenia sieciowe są członkami domeny. Jeśli niektóre urządzenia sieciowe nie znajdują się w domenie, nie można ich wykryć przez przeszukiwanie kontrolera domeny.

- **Przeszukiwanie zakresu IP**. Serwer administracyjny przeszukuje określone zakresy IP przy użyciu pakietów ICMP lub protokołu NBNS i sporządza pełen zestaw danych na temat urządzeń znajdujących się w tych zakresach IP. Domyślnie ten typ przeszukiwania jest wyłączony. Nie jest zalecane korzystanie z tego typu przeszukiwania, jeśli korzystasz z przeszukiwania sieci Windows i/lub przeszukiwania Active Directory.

- **Przeszukiwanie Zeroconf**. Punkt dystrybucji, który odpytuje sieć IPv6 za pomocą zero-configuration networking (zwany również *Zeroconf*). Domyślnie ten typ przeszukiwania jest wyłączony. Możesz użyć przeszukiwania Zeroconf, jeśli na punkcie dystrybucji działa system Linux.

Jeśli skonfigurowałeś i włączyłeś reguły przenoszenia urządzeń, nowo wykryte urządzenia są automatycznie umieszczane w grupie **Zarządzane urządzenia**. Jeśli nie włączono żadnych reguł przenoszenia, nowo wykryte urządzenia zostają automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**.

Możesz zmodyfikować ustawienia wykrywania urządzeń dla każdego typu. Na przykład, możesz chcieć zmodyfikować terminarz przeszukiwania lub ustawić, czy przeszukiwany ma być cały las domeny lub tylko określona domena.

Przed rozpoczęciem przeszukiwania sieci upewnij się, że protokół SMB jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Aby włączyć protokół SMB, postępuj zgodnie z instrukcjami dla swojego systemu operacyjnego.

Przeszukiwanie sieci Windows

Informacje o przeszukiwaniu sieci Windows

Podczas szybkiego przeszukiwania Serwer administracyjny pobiera wyłącznie informacje o urządzeniach znajdujących się na liście nazw NetBIOS wszystkich domen sieci i grup roboczych. Podczas pełnego przeszukiwania wymagane są następujące informacje o każdym urządzeniu klienckim:

- Nazwa systemu operacyjnego
- Adres IP
- Nazwa DNS
- Nazwa NetBIOS

Szybkie przeszukiwanie i pełne przeszukiwanie wymagają:

- Porty UDP 137/138, TCP 139, UDP 445, TCP 445 muszą być dostępne w sieci.
- Protokół SMB jest włączony.
- Usługa Przeglądarka komputera Microsoft musi być używana, a główna przeglądarka komputera musi być włączona na Serwerze administracyjnym.

- Usługa Przeglądarka komputera Microsoft musi być używana, a główna przeglądarka komputera musi być włączona na urządzeniach klienckich:
  - Przynajmniej na jednym urządzeniu, jeśli liczba urządzeń w sieci nie przekracza 32.
  - Przynajmniej na jednym urządzeniu dla każdego z 32 urządzeń w sieci.

Pełne przeszukiwanie może być uruchomione tylko wtedy, gdy szybkie przeszukiwanie było uruchomione przynajmniej raz.

Przeglądanie i modyfikowanie ustawień przeszukiwania sieci Windows

W celu zmodyfikowania właściwości przeszukiwania sieci Windows:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Domeny Windows**.
2. Kliknij przycisk **Właściwości**.

   Zostanie otwarte okno właściwości domeny Windows.
3. Włącz lub wyłącz przeszukiwanie sieci Windows przy użyciu przycisku przełącznika **Włącz przeszukiwanie sieci Windows**.
4. Skonfiguruj terminarz przeszukiwania. Domyślnie, szybkie przeszukiwanie jest uruchamiane co 15 minut, a pełne przeszukiwanie jest uruchamiane co 60 minut.

   Dostępne są następujące opcje terminarza przeszukiwania:

   - **Co N dni**

     Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

     Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.
   - **Co N minut**

     Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.
   - **Według dni tygodnia**

     Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.
   - **Co miesiąc, w określone dni wybranych tygodni**

     Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.
   - **Uruchom pominięte zadania**

     Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

     Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

     Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

Domyślnie opcja ta jest wyłączona.

5. Zapisz właściwości przeszukiwania sieci Windows.

Właściwości są zapisywane i stosowane do wszystkich wykrytych domen i podgrup systemu Windows.

Ręczne uruchamianie przeszukiwania

W celu natychmiastowego uruchomienia przeszukiwania:

Kliknij **Uruchom szybkie przeszukiwanie** lub **Uruchom pełne przeszukiwanie**.

Po zakończeniu przeszukiwania, możesz przejrzeć listę wykrytych urządzeń na stronie **Domeny Windows**, zaznaczając pole obok nazwy domeny, a następnie klikając przycisk **Urządzenia**.

Przeszukiwanie zakresu IP

Na początku program Kaspersky Security Center uzyskuje zakresy adresów IP dla przeszukiwania z ustawień sieciowych urządzenia, na którym jest zainstalowany. Jeśli adres urządzenia to 192.168.0.1, a maska podsieci to 255.255.255.0, Kaspersky Security Center uwzględnia sieć 192.168.0.0/24 na liście automatycznego przeszukiwania adresów. Kaspersky Security Center przeszukuje wszystkie adresy od 192.168.0.1 do 192.168.0.254.

Dla hostów z systemem Linux w ramach kontrolera domeny Microsoft Active Directory lub Samba, określ parametry `netbios name` i `workgroup` w pliku `/etc/samba/smb.conf`. W przeciwnym razie wyniki przeszukiwania mogą zawierać zduplikowane hosty.

Kaspersky Security Center może odpytywać zakresy adresów IP przez odwrotne wyszukiwanie DNS lub przy użyciu protokołu NBNS:

- **Odwrotne wyszukiwanie DNS**

  Kaspersky Security Center próbuje przeprowadzić odwrotne rozwiązanie nazwy dla każdego adresu IP z określonego zakresu do nazwy DNS przy użyciu standardowych żądań DNS. Jeśli to działanie zakończy się sukcesem, serwer wyśle `ICMP ECHO REQUEST` (to samo co polecenie ping) do otrzymanej nazwy. Jeśli urządzenie odpowie, informacje o tym zostaną dodane do bazy danych Kaspersky Security Center. Odwrotne rozwiązanie nazwy jest potrzebne do wykluczenia urządzeń sieciowych, które mogą mieć adres IP, ale nie komputery, na przykład, drukarki sieciowe lub routery.

  Ta metoda przeszukiwania polega na poprawnie skonfigurowanej lokalnej usłudze DNS. Musi mieć strefę wyszukiwania wstecznego. W sieciach, w których używane jest Active Directory, taka strefa jest obsługiwana automatycznie. Ale w tych sieciach przeszukiwanie podsieci IP nie zawiera więcej informacji niż przeszukiwanie Active Directory. Co więcej, administratorzy małych sieci często nie konfigurują strefy wyszukiwania wstecznego, ponieważ nie jest to konieczne dla pracy wielu usług sieciowych. Z tych powodów przeszukiwanie podsieci IP jest wyłączone domyślnie.

- **Protokół NBNS**

  Jeśli z jakiegoś powodu odwrotne rozpoznawanie nazw nie jest możliwe w Twojej sieci, Kaspersky Security Center używa protokołu NBNS do odpytywania zakresów IP. Jeśli żądanie skierowane do adresu IP zwróci nazwę NetBIOS, informacje o tym urządzeniu zostaną dodane do bazy danych Kaspersky Security Center.

Przed rozpoczęciem przeszukiwania sieci upewnij się, że protokół SMB jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Aby włączyć protokół SMB, postępuj zgodnie z instrukcjami dla swojego systemu operacyjnego.

Przeglądanie i modyfikowanie ustawień przeszukiwania zakresu IP

W celu przejrzenia i zmodyfikowania właściwości przeszukiwania zakresu IP:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.
2. Kliknij przycisk **Właściwości**.

   Zostanie otwarte okno właściwości przeszukiwania IP.
3. Włącz lub wyłącz przeszukiwanie IP przy użyciu przycisku przełącznika **Zezwól na przeszukiwanie**.
4. Skonfiguruj terminarz przeszukiwania. Domyślnie, przeszukiwanie IP jest uruchamiane co 420 minut (siedem godzin).

   Podczas określania przedziału czasu przeszukiwania upewnij się, że to ustawienie nie przekracza wartości Parametr czasu dzierżawy adresu IP. Jeśli adres IP nie został zweryfikowany przez przeszukiwanie w trakcie czasu dzierżawy adresu IP, ten adres IP jest automatycznie usuwany z wyników przeszukiwania. Domyślnie, wyniki przeszukiwania są ważne 24 godziny, ponieważ dynamiczne adresy IP (przypisane przy użyciu Protokołu dynamicznej konfiguracji hosta (DHCP)) zmieniają się co 24 godziny.

   Dostępne są następujące opcje terminarza przeszukiwania:

   - **Co N dni**

     Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

     Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

   - **Co N minut**

     Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

   - **Według dni tygodnia**

     Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

   - **Co miesiąc, w określone dni wybranych tygodni**

     Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

   - **Uruchom pominięte zadania**

     Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

Domyślnie opcja ta jest wyłączona.

5. Kliknij przycisk **Zapisz**.

Właściwości zostaną zapisane i zastosowane do wszystkich zakresów IP.

Ręczne uruchamianie przeszukiwania

W celu natychmiastowego uruchomienia przeszukiwania:

Kliknij **Uruchom przeszukiwanie**.

Dodawanie i modyfikowanie zakresu IP

Na początku program Kaspersky Security Center uzyskuje zakresy adresów IP dla przeszukiwania z ustawień sieciowych urządzenia, na którym jest zainstalowany. Jeśli adres urządzenia to 192.168.0.1, a maska podsieci to 255.255.255.0, Kaspersky Security Center uwzględnia sieć 192.168.0.0/24 na liście automatycznego przeszukiwania adresów. Kaspersky Security Center przeszukuje wszystkie adresy od 192.168.0.1 do 192.168.0.254. Możesz zmodyfikować automatycznie definiowany zakres adresów IP lub dodać niestandardowe zakresy adresów IP.

Możesz utworzyć zakres tylko dla adresów IPv4. Jeśli włączysz Przeszukiwanie Zeroconf, Kaspersky Security Center przeszuka całą sieć.

W celu dodania nowego zakresu IP:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.
2. Aby dodać nowy zakres IP, kliknij przycisk **Dodaj**.
3. W otwartym oknie określ następujące ustawienia:
   - **Nazwa zakresu IP**

     Nazwa zakresu IP. Możesz określić sam zakres IP jako nazwę, na przykład: „192.168.0.0/24”.

   - **Zakres IP lub adres podsieci i maska**

     Ustaw zakres IP, określając początkowy i końcowy adres IP lub adres podsieci i maskę podsieci. Możesz także wybrać jeden z już istniejących zakresów IP, klikając przycisk **Przeglądaj**.

   - **Okres istnienia adresu IP (godz.)**

     Podczas określania tego parametru upewnij się, że przekracza on czas przeszukiwania ustawiony w terminarzu przeszukiwania. Jeśli adres IP nie został zweryfikowany przez przeszukiwanie w trakcie czasu dzierżawy adresu IP, ten adres IP jest automatycznie usuwany z wyników przeszukiwania. Domyślnie, wyniki przeszukiwania są ważne 24 godziny, ponieważ dynamiczne adresy IP (przypisane przy użyciu Protokołu dynamicznej konfiguracji hosta (DHCP)) zmieniają się co 24 godziny.

4. Wybierz **Włącz przeszukiwanie zakresu IP**, jeśli chcesz przeszukać podsieć lub przedział, które dodałeś. W przeciwnym razie, dodana podsieć lub przedział nie zostaną przeszukane.

5. Kliknij przycisk **Zapisz**.

   Nowy zakres IP jest dodawany do listy zakresów IP.

Możesz uruchomić przeszukiwanie każdego zakresu IP oddzielnie, korzystając z przycisku **Uruchom przeszukiwanie**. Po zakończeniu przeszukiwania, możesz przejrzeć listę wykrytych urządzeń, korzystając z przycisku **Urządzenia**. Domyślnie, wyniki przeszukiwania są ważne 24 godziny, co jest równe ustawieniu czasu dzierżawy adresu IP.

W celu dodania podsieci do istniejącego zakresu IP:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.

2. Kliknij nazwę zakresu IP, do którego chcesz dodać podsieć.

3. W otwartym oknie kliknij przycisk **Dodaj**.

4. Określ podsieć, używając jej adresu i maski lub używając pierwszego i ostatniego adresu IP w zakresie IP. Lub dodaj istniejącą podsieć, klikając przycisk **Przeglądaj**.

5. Kliknij przycisk **Zapisz**.

   Nowa podsieć zostanie dodana do zakresu IP.

6. Kliknij przycisk **Zapisz**.

   Zostaną zapisane nowe ustawienia zakresu IP.

   Możesz dodać tyle podsieci, ile potrzebujesz. Nazwane zakresy IP nie mogą się nakładać, ale nienazwane podsieci wewnątrz zakresu IP nie posiadają takich ograniczeń. Możesz włączać i wyłączać przeszukiwanie niezależnie dla każdego zakresu IP.

Przeszukiwanie Zeroconf

Ten typ przeszukiwania jest obsługiwany tylko w przypadku punktów dystrybucji opartych na systemie Linux.

Punkt dystrybucji może przeszukiwać sieci, które mają urządzenia z adresami IPv6. W takim przypadku zakresy adresów IP nie są określone, a punkt dystrybucji przeszukuje całą sieć za pomocą zero-configuration networking (zwany również *Zeroconf*). Aby rozpocząć korzystanie z Zeroconf, musisz zainstalować narzędzie avahi-browse w punkcie dystrybucji.

W celu włączenia przeszukiwania sieci IPv6:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.

2. Kliknij przycisk **Właściwości**.

3. W otwartym oknie przełącz przycisk przełącznika **Użyj Zeroconf do przeszukiwania sieci IPv6**.

Następnie punkt dystrybucji zaczyna przeszukiwać sieć. W takim przypadku określone zakresy adresów IP są ignorowane.

Przeszukiwanie kontrolera domeny

Kaspersky Security Center obsługuje przeszukiwanie kontrolera domeny Microsoft Active Directory i kontrolera domeny Samba.

> Kaspersky Security Center umożliwia przeszukiwanie kontrolera domeny Samba wyłącznie przy użyciu punktu dystrybucji systemu Linux. W przypadku kontrolera domeny Samba kontroler Samba 4 jest używany jako kontroler domeny Active Directory.

Kiedy przeszukujesz kontroler domeny, Serwer administracyjny lub punkt dystrybucji pobiera informacje o strukturze domeny, kontach użytkowników, grupach zabezpieczeń i nazwach DNS urządzeń znajdujących się w domenie.

Zalecamy korzystanie z przeszukiwania kontrolera domeny, jeśli wszystkie urządzenia sieciowe są członkami domeny. Jeśli niektóre urządzenia sieciowe nie znajdują się w domenie, nie można ich wykryć przez przeszukiwanie kontrolera domeny.

Wymagania wstępne

Przed odpytywaniem kontrolera domeny upewnij się, że zezwalasz na połączenia z kontrolerem domeny przez zaporę lub serwer proxy. Upewnij się także, że na kontrolerze domeny włączone są następujące protokoły:

- Lightweight Directory Access Protocol (LDAP)
- Simple Authentication and Security Layer (SASL)

  Protokół ten jest używany, jeśli połączenie z kontrolerem domeny jest nawiązywane przy użyciu uwierzytelniania SASL. Serwer administracyjny i punkty dystrybucji obsługują jedynie mechanizm DIGEST-MD5.
- Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS)

  Ten protokół jest używany, jeśli chcesz połączyć się z kontrolerem domeny za pomocą połączenia szyfrowanego.

Upewnij się, że na urządzeniu kontrolera domeny są dostępne następujące porty:

- 389 dla protokołu LDAP i prostego uwierzytelniania (w tym SASL)
- 636 w przypadku protokołu LDAPS

Dla hostów z systemem Linux w ramach kontrolera domeny Microsoft Active Directory lub Samba, określ parametry `netbios name` i `workgroup` w pliku `/etc/samba/smb.conf`. W przeciwnym razie wyniki przeszukiwania mogą zawierać zduplikowane hosty.

Jeśli domena Microsoft Active Directory zawiera wiele kontrolerów domeny, wybór konkretnego kontrolera podczas przeszukiwania domeny nie jest obsługiwany. Połączenie jest nawiązywane z pierwszym wykrytym kontrolerem domeny. Aby zapewnić prawidłowe uwierzytelnianie w domenie Microsoft Active Directory, pole Alternatywna nazwa podmiotu (SAN) certyfikatu musi zawierać wszystkie adresy kontrolerów domeny należących do tej domeny, a także nazwę NetBIOS domeny Microsoft Active Directory.

Przeszukiwanie kontrolera domeny przy użyciu Serwera administracyjnego

Za pomocą Serwera administracyjnego można przeprowadzać wyłącznie przeszukiwanie kontrolera domeny Microsoft Active Directory.

Aby przeszukać kontroler domeny przy użyciu Serwera administracyjnego:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Sterowniki domeny**.
2. Kliknij **Ustawienia przeszukiwania**.

   Zostanie otwarte okno **Ustawienia odpytywania sterowników domeny**.
3. Wybierz opcję **Włącz przeszukiwanie sterowników domeny**.
4. W sekcji **Ustawienia zaawansowane** określ zakres przeszukiwania:

   - **Przeszukaj bieżącą domenę**

     Wybierz tę opcję, aby sprawdzić domenę, do której należy Kaspersky Security Center.
   - **Przeszukaj cały las domeny**

     Wybierz tę opcję, aby przeprowadzić przeszukiwanie lasu domeny, do której należy Kaspersky Security Center.
   - **Przeszukaj określone domeny**

     Wybierz tę opcję, aby sprawdzić domenę o określonym adresie i danych logowania użytkownika.
5. Jeśli to konieczne, określ harmonogram przeszukiwania. Domyślny przedział czasu wynosi jedną godzinę. Dane otrzymane przy kolejnym przeszukiwaniu całkowicie zastępują starsze dane.

   Dostępne są następujące opcje terminarza przeszukiwania:

   - **Co N dni**

     Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

     Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.
   - **Co N minut**

     Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

- **Według dni tygodnia**

  Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

- **Co miesiąc, w określone dni wybranych tygodni**

  Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

- **Uruchom pominięte zadania**

  Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

  Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

  Domyślnie opcja ta jest wyłączona.

Jeśli zmienisz konta użytkowników w grupie zabezpieczeń domeny, zmiany te zostaną wyświetlone w Kaspersky Security Center godzinę po przeszukiwaniu kontrolera domeny.

6. Kliknij **Zapisz**, aby zastosować zmiany.

7. Jeśli chcesz przeprowadzić przeszukiwanie natychmiast, kliknij przycisk **Uruchom przeszukiwanie**.

Przeszukiwanie kontrolera domeny przy użyciu punktu dystrybucji

Można również przeszukiwać kontroler domeny Microsoft Active Directory i kontroler domeny Samba, korzystając z punktu dystrybucji. Zarządzane urządzenie z systemem Windows lub Linux może działać jako punkt dystrybucji.

W przypadku punktu dystrybucji z systemem Linux obsługiwane jest przeszukiwanie kontrolera domeny Microsoft Active Directory oraz kontrolera domeny Samba.
W przypadku punktu dystrybucji z systemem Windows obsługiwane jest tylko przeszukiwanie kontrolera domeny Microsoft Active Directory.
Przeszukiwanie przy użyciu punktu dystrybucji na komputerze Mac nie jest obsługiwane.

Aby skonfigurować przeszukiwanie kontrolera domeny przy użyciu punktu dystrybucji:

1. Otwórz właściwości punktu dystrybucji.

2. Wybierz sekcję **Przeszukiwanie sterowników domeny**.

3. Wybierz opcję **Włącz przeszukiwanie sterowników domeny**.

4. Wybierz kontroler domeny, który chcesz przeszukać.

   Jeśli korzystasz z punktu dystrybucji systemu Linux, w sekcji **Przeszukaj określone domeny** kliknij opcję **Dodaj**, a następnie określ adres i dane uwierzytelniające użytkownika kontrolera domeny.

Jeśli korzystasz z punktu dystrybucji systemu Windows, możesz wybrać jedną z następujących opcji:

- **Przeszukaj bieżącą domenę**
- **Przeszukaj cały las domeny**
- **Przeszukaj określone domeny**

5. Kliknij przycisk **Ustaw terminarz przeszukiwania**, aby w razie potrzeby określić opcje terminarza przeszukiwania.

   Przeszukiwanie rozpoczyna się wyłącznie zgodnie z określonym terminarzem. Ręczne rozpoczęcie przeszukiwania nie jest dostępne.

Po zakończeniu przeszukiwania struktura domeny zostanie wyświetlona w sekcji **Sterowniki domeny**.

Jeśli skonfigurowałeś i włączyłeś reguły przenoszenia urządzeń, nowo wykryte urządzenia są automatycznie umieszczane w grupie **Zarządzane urządzenia**. Jeśli nie włączono żadnych reguł przenoszenia, nowo wykryte urządzenia zostają automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**.

Wykryte konta użytkowników można wykorzystać do uwierzytelnienia domeny w Kaspersky Security Center Web Console.

Uwierzytelnianie i połączenie z kontrolerem domeny

Uwierzytelnianie i połączenie z kontrolerem domeny podczas przeszukiwania domeny

Podczas przeszukiwania kontrolera domeny za pomocą punktu dystrybucji Linux, punkt dystrybucji identyfikuje protokół połączenia w celu nawiązania początkowego połączenia z kontrolerem domeny. Protokół ten będzie używany do wszystkich przyszłych połączeń z kontrolerem domeny. Podczas nawiązywania początkowego połączenia z kontrolerem domeny można zmienić opcje połączenia, korzystając z flag Agenta sieciowego `KLNAG_LDAP_TLS_REQCERT` i `KLNAG_LDAP_SSL_CACERT`. Flagi Agenta sieciowego można skonfigurować za pomocą polecenia klscflag, zgodnie z opisem w tym artykule.

Początkowe połączenie z kontrolerem domeny przebiega w następujący sposób:

1. Serwer administracyjny lub punkt dystrybucji próbuje połączyć się z kontrolerem domeny poprzez protokół LDAPS.

   Domyślnie weryfikacja certyfikatu nie jest wymagana. Ustaw flagę `KLNAG_LDAP_TLS_REQCERT` na 1, aby wymusić weryfikację certyfikatu.

   Możliwe wartości flagi `KLNAG_LDAP_TLS_REQCERT`:

   - `0`—Żądano certyfikatu, ale jeśli nie został on dostarczony lub weryfikacja certyfikatu nie powiodła się, połączenie TLS nadal uważa się za pomyślnie utworzone (wartość domyślna).
   - `1`—Wymagana jest ścisła weryfikacja certyfikatu serwera LDAP.

   Domyślnie, w przypadku gdy flaga `KLNAG_LDAP_SSL_CACERT` nie jest określona, do uzyskania dostępu do łańcucha certyfikatów używana jest ścieżka do urzędu certyfikacji (CA) zależna od systemu operacyjnego. Użyj flagi `KLNAG_LDAP_SSL_CACERT`, aby określić ścieżkę niestandardową.

2. Jeżeli połączenie LDAPS nie powiedzie się, punkt dystrybucji Linux podejmie próbę połączenia się z kontrolerem domeny poprzez nieszyfrowane połączenie TCP przy użyciu protokołu SASL (DIGEST-MD5).

Konfiguracja flag

Do konfigurowania flag można użyć narzędzia klscflag.

Uruchom wiersz poleceń w punkcie dystrybucji Linux, a następnie zmień bieżący katalog na katalog z narzędziem klscflag. Domyślnie w punkcie dystrybucji Linux narzędzie klscflag znajduje się w /opt/kaspersky/ksc64/sbin.

Na przykład następujące polecenie wymusza weryfikację certyfikatu:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Konfigurowanie kontrolera domeny Samba

Kaspersky Security Center obsługuje kontroler domeny Linux działający tylko w systemie Samba 4.

Kontroler domeny Samba obsługuje te same rozszerzenia schematu, co kontroler domeny Microsoft Active Directory. Można włączyć pełną kompatybilność kontrolera domeny Samba z kontrolerem domeny Microsoft Active Directory, używając rozszerzenia schematu Samba 4. Jest to akcja opcjonalna.

Zalecamy włączenie pełnej kompatybilności kontrolera domeny Samba z kontrolerem domeny Microsoft Active Directory. Zapewni to poprawną interakcję pomiędzy kontrolerem domeny Kaspersky Security Center a kontrolerem domeny Samba.

Aby włączyć pełną kompatybilność kontrolera domeny Samba z kontrolerem domeny Microsoft Active Directory:

1. Wykonaj następujące polecenie, aby użyć rozszerzenia schematu RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Włącz aktualizację schematu w kontrolerze domeny Samba. W tym celu, do pliku `/etc/samba/smb.conf` dodaj następujący wiersz:

   ```
   dsdb:schema update allowed = true
   ```

   Jeśli aktualizacja schematu zakończy się błędem, należy wykonać pełne przywrócenie kontrolera domeny pełniącego funkcję głównego schematu.

Dla wszystkich hostów z systemem Linux w ramach kontrolera domeny Samba określ parametry `netbios name` i `workgroup` w pliku `/etc/samba/smb.conf`. W przeciwnym razie wyniki przeszukiwania mogą zawierać zduplikowane hosty.

Konfigurowanie reguły zatrzymania dla urządzeń nieprzypisanych

Po zakończeniu przeszukiwania sieci Windows, wykryte urządzenia zostały umieszczone w podgrupach grupy administracyjnej Urządzenia nieprzypisane. Tę grupę administracyjną można znaleźć w **Wykrywanie i wdrażanie** → **Wykrywanie** → **Domeny Windows**. Folder **Domeny Windows** to grupa nadrzędna. Zawiera grupy potomne, które zostały nazwane po odpowiednich domenach i grupach roboczych, które zostały wykryte podczas przeszukiwania. Grupa nadrzędna może także zawierać grupę administracyjną urządzeń mobilnych. Możesz skonfigurować reguły zatrzymania urządzeń nieprzypisanych dla grupy nadrzędnej i dla każdej grupy potomnej. Reguły zatrzymania nie zależą od ustawień wyszukiwania urządzeń i działają nawet wtedy, gdy wyszukiwanie urządzeń jest wyłączone.

Reguły przechowywania urządzeń nie mają wpływu na urządzenia, które mają jeden lub więcej napędów zaszyfrowanych za pomocą pełnego szyfrowania dysku. Takie urządzenia nie są usuwane automatycznie — można je usunąć tylko ręcznie. Jeśli potrzebujesz usunąć urządzenie z zaszyfrowanym dyskiem, najpierw odszyfruj dysk, a następnie usuń urządzenie.

W celu skonfigurowania reguł zatrzymania dla urządzeń nieprzypisanych:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Domeny Windows**.
2. Wykonaj jedną z poniższych czynności:
   - Aby skonfigurować ustawienia grupy nadrzędnej, kliknij przycisk **Właściwości**.

     Zostanie otwarte okno właściwości domeny Windows.
   - Aby skonfigurować ustawienia grupy potomnej, kliknij jej nazwę.

     Zostanie otwarte okno właściwości grupy potomnej.
3. Określ następujące ustawienia:
   - **Usuń urządzenie z grupy, jeżeli było nieaktywne dłużej niż (dni)**

     Jeśli ta opcja jest włączona, możesz określić przedział czasu, po upływie którego urządzenie zostanie automatycznie usunięte z grupy. Domyślnie, ta opcja jest także rozsyłana do grup potomnych. Domyślny przedział czasu wynosi 7 dni.

     Domyślnie opcja ta jest włączona.
   - **Dziedzicz z grupy nadrzędnej**

     Jeśli ta opcja jest włączona, okres zatrzymania dla urządzeń w bieżącej grupie jest dziedziczony z grupy nadrzędnej nie może zostać zmieniony.

     Ta opcja jest dostępna tylko dla grup potomnych.

     Domyślnie opcja ta jest włączona.
   - **Wymuś dziedziczenie w grupach podrzędnych**

     Wartości ustawień zostaną rozesłane do grup podrzędnych ale we właściwościach grup podrzędnych te ustawienia są zablokowane.

     Domyślnie opcja ta jest wyłączona.
4. Kliknij przycisk **Zaakceptuj**.

Twoje zmiany zostaną zapisane i zastosowane.

Inwentaryzacja sprzętu

Lista sprzętu (**Operacje → Repozytoria → Sprzęt**) którego używasz do przeprowadzenia inwentaryzacji sprzętu, jest uzupełniana na dwa sposoby: automatycznie i ręcznie. Po każdym przeszukaniu sieci, wszystkie wykryte urządzenia zostają dodane do listy automatycznie; jednakże możesz także ręcznie dodać urządzenia, jeśli nie chcesz przeszukiwać sieci. Możesz ręcznie dodać inne urządzenia do listy, na przykład, routery, drukarki lub sprzęt komputerowy.

We właściwościach urządzenia możesz wyświetlić i zmodyfikować szczegółowe informacje o tym urządzeniu.

Lista sprzętu może zawierać następujące typy urządzeń:

- Komputery
- Urządzenia mobilne
- Urządzenia sieciowe
- Urządzenia wirtualne
- Składniki OEM
- Peryferia komputerowe
- Podłączone urządzenia
- Telefony VoIP
- Repozytoria sieciowe

Administrator może przypisać atrybut *Sprzęt firmowy* do wykrytych urządzeń. Ten atrybut jest przypisywany ręcznie we właściwościach urządzenia, administrator może również określić kryteria automatycznego przypisywania dla tego atrybutu. W takim przypadku atrybut *Sprzęt firmowy* jest przypisywany zgodnie z typem urządzenia.

Kaspersky Security Center pozwala na wyrejestrowywanie sprzętu. W tym celu wybierz opcję **Wyrejestrowane** we właściwościach urządzenia. Takie urządzenie nie jest wyświetlane na liście sprzętu.

Administrator może zarządzać listą programowalnych sterowników logicznych (PLC) w folderze **Sprzęt**. Szczegółowe informacje na temat zarządzania listą PLC można znaleźć w *podręczniku użytkownika dla Kaspersky Industrial CyberSecurity for Nodes*.

Dodawanie informacji o nowych urządzeniach

W celu dodania informacji o nowych urządzeniach w sieci:

1. W menu głównym przejdź do **Operacje → Repozytoria → Sprzęt**.
2. Kliknij przycisk **Dodaj**, aby otworzyć okno **Nowe urządzenie**.
3. W oknie **Nowe urządzenie**, na liście rozwijalnej **Typ urządzenia** wybierz typ urządzenia, które chcesz dodać.

4. Kliknij **OK**.

   Okno właściwości urządzenia zostanie otwarte na sekcji **Ogólne**.

5. W sekcji **Ogólne** wypełnij pola wejściowe danymi urządzenia. Sekcja **Ogólne** wyświetla następujące ustawienia:

   - **Urządzenie firmowe**. Zaznacz to pole, jeśli chcesz przypisać atrybut *Firmowy* do urządzenia. Przy użyciu tego atrybutu można wyszukiwać urządzenia w folderze **Sprzęt**.
   - **Wyrejestrowane**. Zaznacz pole, jeśli nie chcesz, aby urządzenie było wyświetlane na liście urządzeń w folderze **Sprzęt**.

6. Kliknij **Zastosuj**.

Nowe urządzenie będzie wyświetlane w obszarze roboczym strony **Sprzęt**.

Konfigurowanie kryteriów wykorzystywanych do określania urządzeń firmowych

W celu skonfigurowania kryteriów wykrywania dla urządzeń firmowych:

1. W menu głównym przejdź do **Operacje** → **Repozytoria** → **Sprzęt**.
2. Na górze strony **Sprzęt** kliknij łącze **Ustaw regułę dla urządzeń firmowych**.

   Wywołany zostanie panel **Ustaw regułę dla urządzeń firmowych**.

3. W panelu **Ustaw regułę dla urządzeń firmowych** włącz opcję **Ustaw dla urządzenia atrybut urządzenie firmowego automatycznie**. Określ typy urządzeń, do których atrybut *firmowy* jest przypisywany automatycznie.

   Ta opcja dotyczy tylko urządzeń, które zostały dodane przez przeszukiwanie sieci. W przypadku urządzeń dodanych ręcznie ustaw atrybut *Firmowy* ręcznie.

4. Kliknij **OK**.

Skonfigurowano kryteria wykrywania dla urządzeń firmowych.

Aplikacje Kaspersky: licencjonowanie i aktywacja

Ta sekcja opisuje funkcje Kaspersky Security Center związane z pracą z kluczami licencyjnymi dla zarządzanych aplikacji Kaspersky.

Kaspersky Security Center pozwala na wykonywanie scentralizowanego rozsyłania kluczy licencyjnych dla aplikacji Kaspersky na urządzenia klienckie, monitorowanie ich wykorzystania i odnawianie licencji.

Dodając klucz licencyjny przy pomocy Kaspersky Security Center, jego ustawienia są zapisywane na Serwerze administracyjnym. W oparciu o te informacje, aplikacja generuje raport użycia klucza licencyjnego i powiadamia administratora o wygaśnięciu licencji oraz naruszeniu ograniczeń licencyjnych, określonych we właściwościach kluczy licencyjnych. Możesz skonfigurować powiadomienia związane z korzystaniem z kluczy licencyjnych w ustawieniach Serwera administracyjnego.

Licencjonowanie zarządzanych aplikacji

Aplikacje Kaspersky, zainstalowane na zarządzanych urządzeniach, muszą być licencjonowane poprzez zastosowanie pliku klucza lub kodu aktywacyjnego do każdej z aplikacji. Plik klucza lub kod aktywacyjny może zostać rozesłany w następujące sposoby:

- Automatyczne wdrażanie
- Pakiet instalacyjny zarządzanej aplikacji
- Zadanie *Dodaj klucz licencyjny* dla zarządzanej aplikacji
- Ręczna aktywacja zarządzaną aplikacją

Możesz dodać nowy aktywny lub zapasowy klucz licencyjny za pomocą dowolnej z metod wymienionych powyżej. Aplikacja firmy Kaspersky używa w danej chwili aktywnego klucza i przechowuje klucz rezerwowy do zastosowania po wygaśnięciu aktywnego klucza. Aplikacja, dla której dodajesz klucz licencyjny, określa, czy klucz jest aktywny, czy zapasowy. Definicja klucza nie zależy od metody użytej do dodania nowego klucza licencyjnego.

Automatyczne wdrażanie

Jeśli używasz różnych zarządzanych aplikacji i musisz rozesłać określony plik klucza lub kod aktywacyjny na urządzenia, zdecyduj się na inne sposoby wdrożenia tego kodu aktywacyjnego lub pliku klucza.

Kaspersky Security Center umożliwia automatyczne rozesłanie dostępnych kluczy licencyjnych na urządzenia. Na przykład, trzy klucze licencyjne są przechowywane w repozytorium Serwera administracyjnego. Zaznaczyłeś pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia** dla wszystkich trzech kluczy licencyjnych. Aplikacja zabezpieczająca Kaspersky—na przykład Kaspersky Endpoint Security for Windows—jest zainstalowana na urządzeniach w organizacji. Zostanie wykryte nowe urządzenie, do którego musi być rozesłany klucz licencyjny. Aplikacja określi, na przykład, że na urządzenie mogą zostać rozesłane dwa klucze licencyjne z repozytorium: klucz licencyjny o nazwie *Key_1* oraz klucz licencyjny o nazwie *Key_2*. Jeden z tych kluczy licencyjnych zostanie zastosowany na urządzeniu. W tym przypadku nie można przewidzieć, który z dwóch kluczy licencyjnych zostanie wdrożony na urządzeniu, ponieważ automatyczne wdrażanie kluczy licencyjnych nie oferuje administratorowi podejmowania żadnych działań.

Podczas rozsyłania klucza licencyjnego urządzenia są zliczane dla tego klucza licencyjnego. Musisz upewnić się, że liczba urządzeń, na których klucz licencyjny został zastosowany, nie przekracza limitu określonego przez licencję. Jeśli liczba urządzeń przekracza limit określony przez licencję, wszystkie urządzenia, które nie zostały objęte licencją, otrzymają stan *Krytyczny*.

Przed wdrożeniem, plik klucza lub kod aktywacyjny musi zostać dodany do repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Automatyczne rozsyłanie kluczy licencyjnych

  lub
- Kaspersky Security Center Web Console:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Automatyczne rozsyłanie kluczy licencyjnych

Należy pamiętać, że automatycznie dystrybuowany klucz licencyjny może nie zostać wyświetlony w repozytorium wirtualnego Serwera administracyjnego w następujących przypadkach:

- Klucz licencyjny nie jest ważny dla aplikacji.
- Wirtualny Serwer administracyjny nie ma zarządzanych urządzeń.
- Klucz licencyjny został już użyty dla urządzeń zarządzanych przez inny wirtualny Serwer administracyjny i osiągnięto limit liczby urządzeń.

Dodawanie pliku klucza lub kodu aktywacyjnego do pakietu instalacyjnego zarządzanej aplikacji

Z powodów bezpieczeństwa, ta opcja nie jest zalecana. Plik klucza lub kod aktywacyjny dodane do pakietu instalacyjnego mogą być zagrożone.

Jeśli instalujesz zarządzaną aplikację przy użyciu pakietu instalacyjnego, możesz określić kod aktywacyjny lub plik klucza w tym pakiecie instalacyjnym lub w zasadzie aplikacji. Klucz licencyjny zostanie rozesłany na zarządzane urządzenia podczas kolejnej synchronizacji urządzenia z Serwerem administracyjnym.

Dostępne instrukcje:

- Konsola administracyjna:
  - Tworzenie pakietu instalacyjnego
  - Instalowanie aplikacji na urządzeniach klienckich

  lub
- Kaspersky Security Center Web Console: Dodawanie klucza licencyjnego do pakietu instalacyjnego

Wdrażanie poprzez zadanie Dodaj klucz licencyjny dla zarządzanej aplikacji

Jeśli zdecydujesz się na użycie zadania *Dodaj klucz licencyjny* dla zarządzanej aplikacji, możesz wybrać klucz licencyjny, który musi zostać rozesłany na urządzenia, oraz wybrać urządzenia w dowolny sposób—na przykład, wybierając grupę administracyjną lub wybór urządzeń.

Przed wdrożeniem, plik klucza lub kod aktywacyjny musi zostać dodany do repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Rozsyłanie klucza licencyjnego na urządzenia klienckie

  lub
- Kaspersky Security Center Web Console:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Rozsyłanie klucza licencyjnego na urządzenia klienckie

Ręczne dodawanie kodu aktywacyjnego lub pliku klucza do urządzeń

Możesz aktywować zainstalowaną aplikację Kaspersky lokalnie, przy użyciu narzędzi dostępnych w interfejsie aplikacji. Więcej informacji można znaleźć w dokumentacji dla zainstalowanej aplikacji.

Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego

W celu dodania klucza licencyjnego do repozytorium Serwera administracyjnego:

1. W menu głównym przejdź do **Operacje** → **Licencjonowanie** → **Licencje Kaspersky**.
2. Kliknij przycisk **Dodaj**.
3. Wybierz, co chcesz dodać:
   - **Dodaj plik klucza**
     Kliknij przycisk **Wybierz plik klucza** i odszukaj plik .key, który chcesz dodać.

- **Wprowadź kod aktywacyjny**

  Określ kod aktywacyjny w polu tekstowym i kliknij przycisk **Wyślij**.

4. Kliknij przycisk **Zamknij**.

Klucz licencyjny lub kilka kluczy licencyjnych zostaną dodane do repozytorium Serwera administracyjnego.

Dodawanie klucza licencyjnego z Serwera administracyjnego

W celu dodania klucza licencyjnego z Serwera administracyjnego:

1. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego wybierz sekcję **Klucze licencyjne**.
3. W sekcji **Aktywny klucz licencyjny** kliknij przycisk **Edytuj**.
4. W oknie, które zostanie otwarte, dodaj klucz licencyjny, klikając przycisk **Dodaj**.

   Zostanie uruchomiony kreator Add license key wizard.

Po zakończeniu działania kreatora można sprawdzić, czy funkcje są wyświetlane w Konsoli administracyjnej zgodnie z odpowiednią licencją.

Rozsyłanie klucza licencyjnego na urządzenia klienckie

Kaspersky Security Center Web Console umożliwia rozesłanie klucza licencyjnego na urządzenia klienckie automatycznie lub przy pomocy zadania **Aktywacja aplikacji**. Za pomocą tego zadania można przydzielić klucze określonej grupie urządzeń. Podczas rozsyłania klucza licencyjnego za pomocą zadania, limit licencji dotyczący liczby urządzeń nie jest uwzględniany. Użyj opcji automatycznego rozsyłania kluczy, aby automatycznie zakończyć rozsyłanie klucza licencyjnego po osiągnięciu limitu licencji.

Jeśli włączysz automatyczne rozsyłanie kluczy licencyjnych, nie twórz zadania **Aktywacja aplikacji** w celu rozsyłania kluczy na urządzenia klienckie. W przeciwnym wypadku obciążenie Serwera administracyjnego wzrośnie ze względu na częstą synchronizację.

Przed wdrożeniem należy dodać klucz licencyjny do repozytorium Serwera administracyjnego.

*Aby rozesłać klucz licencyjny do urządzeń klienckich za pomocą zadania **Aktywacja aplikacji**:*

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony **Kreator tworzenia nowego zadania**. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Z listy rozwijanej **Aplikacja** wybierz aplikację, do której chcesz dodać klucz licencyjny.
4. Z listy **Typ zadania** wybierz zadanie **Aktywacja aplikacji**.
5. W polu **Nazwa zadania** podaj nazwę nowego zadania.

6. Wybierz urządzenia, do których zadanie zostanie przypisane.

7. Na etapie **Wybór klucza licencyjnego** kreatora kliknij łącze **Dodaj klucz**, aby dodać klucz licencyjny.

8. W oknie dodawania klucza dodaj klucz licencyjny, korzystając z jednej z następujących opcji:

   Musisz dodać klucz licencyjny tylko wtedy, gdy nie dodałeś go do repozytorium Serwera administracyjnego przed utworzeniem zadania /**Aktywacja aplikacji**.

   - Wybierz opcję **Wprowadź kod aktywacyjny**, aby wprowadzić kod aktywacyjny, a następnie wykonaj następujące czynności:

     a. Podaj kod aktywacyjny, a następnie kliknij przycisk **Wyślij**.

     Informacja o kluczu licencyjnym pojawi się w oknie dodawania klucza.

     b. Kliknij przycisk **Zapisz**.

     Jeśli chcesz automatycznie rozsyłać klucz licencyjny do zarządzanych urządzeń, włącz opcję **Automatycznie roześlij klucz licencyjny do zarządzanych urządzeń**.

     Okno dodawania klucza zostanie zamknięte.

   - Wybierz opcję **Dodaj plik klucza**, aby dodać plik klucza, a następnie wykonaj następujące czynności:

     a. Kliknij przycisk **Wybierz plik klucza**.

     b. W otwartym oknie wybierz plik klucza, a następnie kliknij przycisk **Otwórz**.

     Informacje o kluczu licencyjnym pojawią się w oknie dodawania klucza licencyjnego.

     c. Kliknij przycisk **Zapisz**.

     Jeśli chcesz automatycznie rozsyłać klucz licencyjny do zarządzanych urządzeń, włącz opcję **Automatycznie roześlij klucz licencyjny do zarządzanych urządzeń**.

     Okno dodawania klucza zostanie zamknięte.

9. Wybierz klucz licencyjny w tabeli kluczy.

10. Na etapie **informacji o licencji** kreatora usuń zaznaczenie domyślnego pola wyboru **Użyj jako klucza rezerwowego**, jeśli chcesz zastąpić bieżący aktywny klucz licencyjny.

    Na przykład jest to konieczne w przypadku zmiany organizacji i urządzenie wymaga klucza innej organizacji; lub jeśli klucz został wydany ponownie, a nowa licencja wygasa wcześniej niż bieżąca. Aby uniknąć błędów, odznacz pole wyboru **Użyj jako klucza zapasowego**.

    Jeśli chcesz uzyskać więcej informacji o problemach, które mogą wystąpić podczas dodawania klucza licencyjnego do Kaspersky Security Center oraz o sposobach ich rozwiązania, zapoznaj się z bazą wiedzy Kaspersky Security Center.

11. W kroku **Zakończ tworzenie zadania** kreatora, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**, aby zmodyfikować domyślne ustawienia zadania.

    Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później.

12. Kliknij przycisk **Zakończ**.

    Kreator tworzy zadanie. Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, automatycznie zostanie otwarte okno właściwości zadania. W tym oknie możesz określić ogólne ustawienia zadania oraz w razie potrzeby zmienić ustawienia określone podczas tworzenia zadania.

    > Możesz także otworzyć okno właściwości zadania, klikając nazwę utworzonego zadania na liście zadań.

    Zadanie zostanie utworzone, skonfigurowane i będzie wyświetlane na liście zadań.

13. Aby uruchomić zadanie, na liście zadań wybierz zadanie i kliknij przycisk **Uruchom**.

    Możesz także ustawić harmonogram uruchamiania zadania na karcie **Terminarz** w oknie właściwości zadania.

    Szczegółowy opis ustawień zaplanowanego uruchomienia znajduje się w ogólnych ustawieniach zadania.

Po wykonaniu zadania, klucz licencyjny zostanie rozesłany na wybrane urządzenia.

Automatyczne rozsyłanie kluczy licencyjnych

Kaspersky Security Center umożliwia automatyczne instalowanie kluczy licencyjnych na zarządzanych urządzeniach, jeśli znajdują się one w repozytorium kluczy licencyjnych na Serwerze administracyjnym.

W celu automatycznego rozsyłania kluczy licencyjnych do zarządzanych urządzeń:

1. W menu głównym przejdź do **Operacje → Licencjonowanie → Licencje Kaspersky**.
2. Kliknij nazwę klucza licencyjnego, który chcesz automatycznie rozesłać na urządzenia.
3. W otwartym oknie właściwości klucza licencyjnego zaznacz pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**.
4. Kliknij przycisk **Zapisz**.

Klucz licencyjny jest automatycznie rozsyłany do wszystkich kompatybilnych urządzeń.

Rozsyłanie klucza licencyjnego odbywa się przy pomocy Agenta sieciowego. Dla aplikacji nie są tworzone żadne zadania rozsyłania kluczy licencyjnych.

Podczas automatycznego rozsyłania klucza licencyjnego brane jest pod uwagę ograniczenie licencyjne dotyczące liczby urządzeń. Ograniczenie licencyjne jest ustawione we właściwościach klucza licencyjnego. Jeśli ograniczenie licencji zostanie osiągnięte, rozesłanie tego klucza licencyjnego na urządzenia zostanie przerwane automatycznie.

Należy pamiętać, że automatycznie dystrybuowany klucz licencyjny może nie zostać wyświetlony w repozytorium wirtualnego Serwera administracyjnego w następujących przypadkach:

- Klucz licencyjny nie jest ważny dla aplikacji.
- Wirtualny Serwer administracyjny nie ma zarządzanych urządzeń.
- Klucz licencyjny został już użyty dla urządzeń zarządzanych przez inny wirtualny Serwer administracyjny i osiągnięto limit liczby urządzeń.

Wirtualny Serwer administracyjny automatycznie dystrybuuje klucze licencyjne ze swojego repozytorium oraz z repozytorium Serwera administracyjnego. Zalecamy:

- Użyj zadania *Dodaj klucz licencyjny*, aby wybrać klucz licencyjny do wdrożenia na urządzeniach.
- Unikaj wyłączania opcji **Zezwól na automatyczne wdrażanie kluczy licencyjnych z tego wirtualnego Serwera administracyjnego do jego urządzeń** w ustawieniach wirtualnego Serwera administracyjnego. W przeciwnym razie wirtualny Serwer administracyjny nie będzie dystrybuował kluczy licencyjnych do urządzeń, łącznie z kluczami licencyjnymi z repozytorium Serwera administracyjnego.

Jeśli zaznaczysz pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia** w oknie właściwości klucza licencyjnego, klucz licencyjny jest natychmiast rozpowszechniany w Twojej sieci. Jeśli nie wybierzesz tej opcji, możesz użyć zadania do rozpowszechniania klucza licencyjnego później.

Automatyczna dystrybucja kluczy licencyjnych skonfigurowana na głównym Serwerze administracyjnym nie obejmuje urządzeń zarządzanych przez inne niż wirtualne podrzędne Serwery administracyjne.

Wyświetlanie informacji o używanych kluczach licencyjnych

W celu przejrzenia listy kluczy licencyjnych dodanych do repozytorium Serwera administracyjnego:

W menu głównym przejdź do **Operacje → Licencjonowanie → Licencje Kaspersky**.

Wyświetlona lista zawiera pliki klucza i kody aktywacyjne dodane do repozytorium Serwera administracyjnego.

W celu wyświetlenia szczegółowych informacji i kluczu licencyjnym:

1. W menu głównym przejdź do **Operacje → Licencjonowanie → Licencje Kaspersky**.
2. Kliknij nazwę żądanego klucza licencyjnego.

W otwartym oknie właściwości klucza licencyjnego możesz przejrzeć:

- Na zakładce **Ogólne**—główne informacje o kluczu licencyjnym
- Na zakładce **Urządzenia**—lista urządzeń klienckich, na których klucz licencyjny został użyty do aktywacji zainstalowanej aplikacji Kaspersky

W celu sprawdzenia, które klucze licencyjne zostały rozesłane na określone urządzenie klienckie:

1. W menu głównym przejdź do **Zasoby (urządzenia) → Zarządzane urządzenia**.
2. Kliknij nazwę żądanego urządzenia.

3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Aplikacje**.

4. Kliknij nazwę aplikacji, dla której chcesz sprawdzić informacje o kluczu licencyjnym.

5. W otwartym oknie właściwości aplikacji wybierz zakładkę **Ogólne**, a następnie otwórz sekcję **Licencja**.

Zostaną wyświetlone główne informacje o aktywnych i zapasowych kluczach licencyjnych.

Aby określić aktualne ustawienia kluczy licencyjnych wirtualnego Serwera administracyjnego, Serwer administracyjny wysyła żądanie do serwerów aktywacji Kaspersky przynajmniej raz dziennie. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS.

Usuwanie klucza licencyjnego z repozytorium

Jeśli usuniesz aktywny klucz licencyjny dla dodatkowej funkcji Serwera administracyjnego, na przykład Zarządzanie lukami i poprawkami lub Zarządzanie urządzeniami mobilnymi, odpowiednia funkcja stanie się niedostępna. Jeśli dodano zapasowy klucz licencyjny, zapasowy klucz licencyjny automatycznie staje się aktywnym kluczem licencyjnym po wcześniejszym usunięciu aktywnego klucza licencyjnego.

Jeśli usuniesz aktywny klucz licencyjny rozesłany na zarządzane urządzenie, aplikacja będzie kontynuować pracę na zarządzanym urządzeniu.

W celu usunięcia pliku klucza lub kodu aktywacyjnego z repozytorium Serwera administracyjnego:

1. Sprawdź, czy Serwer administracyjny nie używa pliku klucza lub kodu aktywacyjnego, który chcesz usunąć. Jeśli tak, nie możesz usunąć klucza. Aby przeprowadzić kontrolę:

   a. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

   b. Na zakładce **Ogólne** wybierz sekcję **Klucze licencyjne**.

   c. Jeżeli w sekcji, która zostanie otwarta, pojawi się wymagany plik klucza lub kod aktywacyjny, kliknij przycisk **Usuń aktywny klucz licencyjny**, a następnie potwierdź operację. Następnie Serwer administracyjny nie używa usuniętego klucza licencyjnego, ale klucz pozostaje w repozytorium Serwera administracyjnego. Jeśli wymagany plik klucza lub kod aktywacyjny nie jest wyświetlany, serwer administracyjny go nie używa.

2. W menu głównym przejdź do **Operacje** → **Licencjonowanie** → **Licencje Kaspersky**.

3. Wybierz wymagany plik klucza lub kod aktywacyjny, a następnie kliknij przycisk **Usuń**.

Wybrany plik klucza lub kod aktywacyjny zostanie usunięty z repozytorium.

Możesz ponownie dodać usunięty klucz licencyjny lub dodać nowy klucz licencyjny.

Wycofanie zgody z Umową Licencyjną Użytkownika Końcowego

Jeśli zdecydujesz się na zatrzymanie ochrony niektórych swoich urządzeń klienckich, możesz wycofać zgodę z Umową licencyjną użytkownika końcowego dla każdej zarządzanej aplikacji firmy Kaspersky. Przed wycofaniem zgody z Umową licencyjną użytkownika końcowego należy odinstalować wybraną aplikację.

Umowy licencyjne, które zostały zaakceptowane na wirtualnym Serwerze administracyjnym, mogą zostać odrzucone na wirtualnym Serwerze administracyjnym lub na głównym Serwerze administracyjnym. Umowy licencyjne, które zostały zaakceptowane na głównym Serwerze administracyjnym, mogą zostać odrzucone tylko na głównym Serwerze administracyjnym.

W celu anulowania Umowy licencyjnej użytkownika końcowego dla zarządzanych aplikacji Kaspersky:

1. Otwórz okno właściwości Serwera administracyjnego i na zakładce **Ogólne** wybierz sekcję **Umowy licencyjne użytkownika końcowego**.

   Wyświetlana jest lista Umów licencyjnych użytkownika końcowego, zaakceptowanych po utworzeniu pakietów instalacyjnych, w momencie bezproblemowej instalacji aktualizacji lub po wdrożeniu Kaspersky Security for Mobile.

2. Z listy wybierz Umowę licencyjną użytkownika końcowego, którą chcesz anulować.

   Możesz sprawdzić następujące właściwości Umowy licencyjnej użytkownika końcowego:

   - Datę zaakceptowania Umowy licencyjnej użytkownika końcowego
   - Nazwę użytkownika, który zaakceptował Umowę licencyjną użytkownika końcowego

3. Kliknij datę zaakceptowania dowolnej Umowy licencyjnej użytkownika końcowego, aby otworzyć jej okno właściwości wyświetlające następujące dane:

   - Nazwę użytkownika, który zaakceptował Umowę licencyjną użytkownika końcowego
   - Datę zaakceptowania Umowy licencyjnej użytkownika końcowego
   - Unikatowy identyfikator (UID) Umowy licencyjnej użytkownika końcowego
   - Pełną treść Umowy licencyjnej użytkownika końcowego
   - Listę obiektów (pakiety instalacyjne, aktualizacje typu seamless, aplikacje mobilne) powiązanych z Umową licencyjną użytkownika końcowego oraz ich odpowiednie nazwy i typy

4. W lewej części okna właściwości Umowy licencyjnej użytkownika końcowego kliknij przycisk **Odrzuć Umowę licencyjną**.

   Jeśli istnieją jakiekolwiek obiekty (pakiety instalacyjne i ich odpowiednie zadania), które uniemożliwiają wycofanie Umowy licencyjnej użytkownika końcowego, zostanie wyświetlone odpowiednie powiadomienie. Jeśli nie usunąłeś tych obiektów, nie możesz przejść do wycofania.

W otwartym oknie zostanie wyświetlona informacja, że w pierwszej kolejności musisz odinstalować aplikację firmy Kaspersky odpowiadającą Umowie licencyjnej użytkownika końcowego.

5. Kliknij przycisk, aby potwierdzić wycofanie.

Umowa licencyjna użytkownika końcowego zostanie wycofana. Nie jest już wyświetlana na liście Umów licencyjnych w sekcji **Umowy licencyjne użytkownika końcowego**. Okno właściwości Umowy licencyjnej użytkownika końcowego zostanie zamknięte; aplikacja nie będzie już zainstalowana.

Odnawianie licencji dla aplikacji Kaspersky

Możesz odnowić licencję dla aplikacji Kaspersky, która utraciła ważność lub wkrótce utraci ważność (za mniej niż 30 dni).

W celu odnowienia licencji, która utraciła ważność, lub licencji, która wkrótce utraci ważność:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym przejdź do **Operacje → Licencjonowanie → Licencje Kaspersky**.
   - W oknie głównym przejdź do **Monitorowanie i raportowanie → Pulpit nawigacyjny**, a następnie kliknij odnośnik **Zobacz wygasające licencje** obok powiadomienia.

   Zostanie otwarte okno **Licencje Kaspersky**, w którym możesz przejrzeć i odnowić licencje.

2. Kliknij łącze **Odnów licencję** obok wymaganej licencji.

   Klikając odnośnik do odnowienia licencji, wyrażasz zgodę na przeniesienie do Kaspersky następujących informacji o programie Kaspersky Security Center: jego wersję, wersję językową, której używasz, identyfikator licencji oprogramowania (czyli identyfikator odnawianej licencji), a także, czy zakupiłeś licencję u partnera firmy.

3. W otwartym oknie usługi odnowienia licencji wykonaj instrukcje w celu odnowienia licencji.

   Licencja zostanie odnowiona.

W Kaspersky Security Center Web Console powiadomienia o licencji, która wkrótce utraci ważność, są wyświetlane zgodnie z następującym terminarzem:

- 30 dni przed utratą ważności
- 7 dni przed utratą ważności
- 3 dni przed utratą ważności
- 24 godziny przed utratą ważności
- Po wygaśnięciu licencji

Korzystanie z Kaspersky Marketplace do wyboru rozwiązań biznesowych firmy Kaspersky

Platforma handlowa to sekcja w menu głównym, która umożliwia przeglądanie całej gamy rozwiązań biznesowych firmy Kaspersky, wybranie tych, których potrzebujesz, i przejście do zakupu na stronie internetowej Kaspersky. Możesz użyć filtrów, aby wyświetlić tylko te rozwiązania, które pasują do Twojej organizacji i wymagań systemu bezpieczeństwa informacji. Po wybraniu rozwiązania Kaspersky Security Center przekieruje Cię do powiązanej strony internetowej w witrynie Kaspersky, aby dowiedzieć się więcej o tym rozwiązaniu. Każda strona internetowa umożliwia przejście do zakupu lub zawiera instrukcje dotyczące procesu zakupu.

W sekcji **Platforma handlowa** możesz filtrować rozwiązania firmy Kaspersky z użyciem następujących kryteriów:

- Liczba urządzeń (punktów końcowych, serwerów i innych typów zasobów), które chcesz chronić:
  - 50–250
  - 250–1000
  - Więcej niż 1000
- Poziom dojrzałości zespołu ds. bezpieczeństwa informacji w Twojej organizacji:
  - **Podstawowy**

    Ten poziom jest typowy dla przedsiębiorstw, które posiadają tylko zespół ds. IT. Maksymalna możliwa liczba zagrożeń jest blokowana automatycznie.
  - **Optymalny**

    Ten poziom jest typowy dla przedsiębiorstw, które posiadają określoną funkcję bezpieczeństwa IT w zespole ds. IT. Na tym poziomie firmy potrzebują rozwiązań, które umożliwią im przeciwdziałanie zagrożeniom towarowym oraz zagrożeniom omijającym istniejące mechanizmy prewencyjne.
  - **Ekspert**

    Ten poziom jest typowy dla przedsiębiorstw o złożonych i rozproszonych środowiskach IT. Zespół ds. bezpieczeństwa IT jest dojrzały lub firma posiada zespół SOC (Security Operations Center). Wymagane rozwiązania umożliwiają firmom przeciwdziałanie złożonym zagrożeniom i atakom ukierunkowanym.
- Typy zasobów, które chcesz chronić:
  - **Punkty końcowe**: stacje robocze pracowników, maszyny fizyczne i wirtualne, systemy wbudowane
  - **Serwery**: serwery fizyczne i wirtualne
  - **Chmura**: środowiska chmury publicznej, prywatnej lub hybrydowej; usługi w chmurze
  - **Sieć**: sieć lokalna, infrastruktura IT
  - **Usługa**: usługi związane z bezpieczeństwem świadczone przez Kaspersky

W celu znalezienia i zakupu rozwiązania biznesowego firmy Kaspersky:

1. W oknie głównym przejdź do **Platforma handlowa**.

   Domyślnie sekcja wyświetla wszystkie dostępne rozwiązania biznesowe firmy Kaspersky.

2. Aby wyświetlić tylko te rozwiązania, które odpowiadają Twojej organizacji, wybierz wymagane wartości w filtrach.

3. Kliknij rozwiązanie, które chcesz kupić lub chcesz dowiedzieć się więcej.

   Zostaniesz przekierowany na stronę rozwiązania. Możesz postępować zgodnie z instrukcjami wyświetlanymi na ekranie, aby przejść do zakupu.

Konfigurowanie ochrony sieci

Ta sekcja zawiera informacje o ręcznej konfiguracji zasad i zadań, informacje o rolach użytkownika, informacje o tworzeniu struktury grupy administracyjnej oraz hierarchii zadań.

Scenariusz: Konfigurowanie ochrony sieci

Kreator wstępnej konfiguracji tworzy zasady i zadania z domyślnymi ustawieniami. Te ustawienia mogą okazać się nieoptymalne lub nawet niedopuszczalne przez organizację. Dlatego zalecane jest dostrojenie tych zasad i zadań oraz utworzenie innych zasad i zadań, jeśli są konieczne w Twojej sieci.

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Zainstalowano Serwer administracyjny Kaspersky Security Center
- Zainstalowano Kaspersky Security Center Web Console (opcjonalne)
- Zakończyłeś główny scenariusz instalacji Kaspersky Security Center
- Zakończono działanie kreatora wstępnej konfiguracji lub ręcznie utworzono następujące zasady i zadania w grupie administracyjnej **Zarządzane urządzenia**:
  - Zasada Kaspersky Endpoint Security
  - Grupowe zadanie aktualizacji Kaspersky Endpoint Security
  - Zasada Agenta sieciowego
  - Zadanie *Wyszukiwania luk i wymaganych aktualizacji*

Konfigurowanie ochrony sieci odbywa się w etapach:

1. **Konfiguracja i przesyłanie zasad i profili zasad aplikacji firmy Kaspersky**

   Aby skonfigurować i przesłać ustawienia dla aplikacji Kaspersky, zainstalowanych na zarządzanych urządzeniach, możesz użyć dwóch różnych metod zarządzania ochroną—skoncentrowaną na urządzeniu lub skoncentrowaną na użytkowniku. Te dwie metody można także połączyć. Aby zaimplementować zarządzanie ochroną skoncentrowaną na urządzeniu, możesz użyć narzędzi dostarczonych w Konsoli administracyjnej opartej na Microsoft Management Console lub Kaspersky Security Center Web Console. Zarządzanie ochroną skoncentrowaną na użytkowniku może zostać zaimplementowane tylko poprzez Kaspersky Security Center Web Console.

2. **Konfigurowanie zadań zdalnego zarządzania aplikacjami firmy Kaspersky**

   Sprawdź zadania utworzone przy pomocy kreatora wstępnej konfiguracji i dostosuj je (jeśli to konieczne).

   Dostępne instrukcje:

   - Konsola administracyjna:
     - Konfigurowanie grupowego zadania aktualizacji Kaspersky Endpoint Security
     - Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
   - Kaspersky Security Center Web Console:
     - Konfigurowanie grupowego zadania aktualizacji Kaspersky Endpoint Security
     - Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

   Jeśli to konieczne, utwórz dodatkowe zadania do zarządzania aplikacjami firmy Kaspersky, zainstalowanymi na urządzeniach klienckich.

3. **Oszacowanie i ograniczenie nagromadzenia zdarzeń w bazie danych**

   Informacje o zdarzeniach występujących podczas działania zarządzanych aplikacji są przesyłane z urządzenia klienckiego i zapisywane w bazie danych Serwera administracyjnego. Aby zmniejszyć obciążenie na Serwerze administracyjnym, oszacuj i ogranicz maksymalną liczbę zdarzeń przechowywanych w bazie danych.

   Dostępne instrukcje:

   - Konsola administracyjna: Konfigurowanie maksymalnej liczby zdarzeń
   - Kaspersky Security Center Web Console: Konfigurowanie maksymalnej liczby zdarzeń

Wyniki

Po zakończeniu tego scenariusza, Twoja sieć będzie chroniona przez konfigurację aplikacji Kaspersky, zadania i zdarzenia otrzymane przez Serwer administracyjny:

- Aplikacje firmy Kaspersky są konfigurowane zgodnie z zasadami i profilami zasad.
- Aplikacje są zarządzane za pośrednictwem zestawu zadań.
- Maksymalna liczba zdarzeń, jaka może być przechowywana w bazie danych, została ustawiona.

Jeśli konfiguracja ochrony sieci zostanie zakończona, możesz przejść do konfigurowania regularnych aktualizacji baz danych i aplikacji Kaspersky.

Więcej informacji o sposobie konfiguracji automatycznych odpowiedzi na zagrożenia wykryte przez Kaspersky Sandbox można znaleźć w pomocy online Kaspersky Sandbox 2.0.

Informacje o metodach zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku

Możesz zarządzać ustawieniami zabezpieczeń z poziomu funkcji urządzenia i z poziomu roli użytkownika. Pierwsza metoda nosi nazwę *zarządzanie ochroną skoncentrowaną na urządzeniu*, a druga nazywa się *zarządzania ochroną skoncentrowaną na użytkowniku*. Aby zastosować różne ustawienia aplikacji na różnych urządzeniach, możesz użyć połączonych typów zarządzania. Aby zaimplementować zarządzanie ochroną skoncentrowaną na urządzeniu, możesz użyć narzędzi dostarczonych w Konsoli administracyjnej opartej na Microsoft Management Console lub Kaspersky Security Center Web Console. Zarządzanie ochroną skoncentrowaną na użytkowniku może zostać zaimplementowane tylko poprzez Kaspersky Security Center Web Console.

Zarządzanie bezpieczeństwem skoncentrowane na urządzeniu umożliwia zastosowanie różnych ustawień aplikacji zabezpieczającej na zarządzanych urządzeniach w zależności od funkcji charakterystycznych dla urządzeń. Na przykład, możesz zastosować różne ustawienia do urządzeń przydzielonych w różnych grupach administracyjnych. Możesz także rozróżnić urządzenia przy użyciu tych urządzeń w Active Directory lub ich specyfikacji sprzętowej.

Zarządzanie bezpieczeństwem skoncentrowanym na użytkowniku umożliwia zastosowanie różnych ustawień aplikacji zabezpieczającej do różnych ról użytkownika. Możesz utworzyć kilka ról użytkownika, przypisać odpowiednią rolę użytkownika do każdego użytkownika oraz określić różne ustawienia aplikacji do urządzeń należących do użytkowników z różnymi rolami. Na przykład, chcesz zastosować różne ustawienia aplikacji na urządzeniach księgowych i specjalistów z działu HR. W rezultacie, gdy zaimplementowane jest zarządzanie ochroną skoncentrowaną na użytkowniku, każdy dział—dział księgowych i dział HR—posiada swoją własną konfigurację ustawień dla aplikacji firmy Kaspersky. Konfiguracja ustawień definiuje, które ustawienia aplikacji mogą być zmieniane przez użytkowników i dla których wymuszone jest ustawienie i zablokowanie przez administratora.

Korzystając z zarządzania ochroną skoncentrowaną na użytkowniku, możesz zastosować określone ustawienia aplikacji do pojedynczych użytkowników. Może to być wymagane, gdy pracownik posiada unikatową rolę w firmie lub gdy chcesz monitorować problemy bezpieczeństwa dotyczące urządzeń określonej osoby. W zależności od roli tego pracownika w firmie, możesz rozszerzyć lub ograniczyć uprawnienia tej osoby do zmiany ustawień aplikacji. Na przykład, możesz rozszerzyć uprawnienia administratora systemu, który zarządza urządzeniami klienckimi w biurze lokalnym.

Możesz połączyć metody zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku. Na przykład, możesz skonfigurować określoną zasadę aplikacji dla każdej grupy administracyjnej, a następnie utworzyć profile zasad dla jednej lub kilku ról użytkownika Twojej firmy. W tym przypadku zasady i profile zasad są stosowane w następującej kolejności:

1. Zostaną zastosowane zasady utworzone dla zarządzania ochroną skoncentrowaną na urządzeniu.
2. Są one modyfikowane przez profile zasad zgodnie z priorytetami profili zasad.
3. Zasady są modyfikowane przez profile zasad skojarzone z rolami użytkownika.

Konfiguracja i przydzielanie zasad: Metoda skoncentrowana na urządzeniu

Po zakończeniu tego scenariusza, aplikacje zostaną skonfigurowane na wszystkich zarządzanych urządzeniach zgodnie z zasadami i profilami zasad aplikacji, które określiłeś.

Wymagania wstępne

Przed rozpoczęciem konfiguracji upewnij się, że pomyślnie zainstalowano Serwer administracyjny Kaspersky Security Center i Kaspersky Security Center Web Console (opcjonalnie). Jeśli zainstalowałeś Kaspersky Security Center Web Console, możesz wziąć pod uwagę zarządzania ochroną skoncentrowaną na użytkowniku jako alternatywę lub dodatkową opcję dla metody skoncentrowanej na urządzeniu.

Etapy

Scenariusz skoncentrowanego na urządzeniu zarządzania aplikacjami Kaspersky obejmuje następujące kroki:

1. **Konfigurowanie zasad aplikacji**

   Skonfiguruj ustawienia dla aplikacji firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach poprzez utworzenie zasady dla każdej aplikacji. Zestaw zasad zostanie przesłany na urządzenia klienckie.

   Podczas konfigurowania ochrony sieci w kreatorze szybkiego startu Kaspersky Security Center tworzy domyślną zasadę dla następujących aplikacji:

   - Kaspersky Endpoint Security for Windows — dla urządzeń klienckich z systemem Windows
   - Kaspersky Endpoint Security for Linux — dla urządzeń klienckich z Linux

   Jeśli zakończyłeś proces konfiguracji przy użyciu tego kreatora, nie musisz tworzyć nowej zasady dla tej aplikacji. Przejdź do ręcznej konfiguracji zasady Kaspersky Endpoint Security.

   Jeśli masz hierarchiczną strukturę kilku Serwerów administracyjnych i/lub grup administracyjnych, domyślnie podrzędne Serwery administracyjne i podrzędne grupy administracyjne dziedziczą zasady z głównego Serwera administracyjnego. Możesz wymusić dziedziczenie przez grupy podrzędne i podrzędne Serwery administracyjne, aby zabronić wszelkich modyfikacji ustawień skonfigurowanych w nadrzędnej zasadzie. Jeśli chcesz, żeby wymuszone było dziedziczenie tylko części ustawień, możesz zablokować je w zasadzie nadrzędnej. Pozostałe niezablokowane ustawienia będą dostępne do modyfikacji w zasadach podrzędnych. Utworzona hierarchia zasad umożliwi efektywne zarządzanie urządzeniami w grupach administracyjnych.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie zasady
   - Kaspersky Security Center Web Console: Tworzenie zasady

2. **Tworzenie profili zasad (opcjonalnie)**

Jeśli chcesz, żeby urządzenia w jednej grupie administracyjnej były uruchamiane z różnymi ustawieniami zasady, utwórz profile zasad dla tych urządzeń. Profil zasad jest to inaczej podzbiór ustawień zasady. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z zasadą i uzupełnia ją zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowej" zasady, która jest aktywna na zarządzanym urządzeniu.

Korzystając z warunków aktywacji profilu, możesz zastosować różne profile zasad, na przykład, do urządzeń znajdujących się w określonej jednostce lub grupie bezpieczeństwa Active Directory, posiadającej określoną konfigurację sprzętową lub oznaczoną określonymi znacznikami. Użyj znaczników do filtrowania urządzeń, które spełniają określone kryteria. Na przykład, możesz utworzyć znacznik nazwany *Windows*, oznaczyć tym znacznikiem wszystkie urządzenia działające pod kontrolą systemu operacyjnego Windows, a następnie określić ten znacznik jako warunek aktywacji profilu zasad. W wyniku tego działania, aplikacje Kaspersky zainstalowane na wszystkich urządzeniach działających pod kontrolą systemu Windows będą zarządzane przez swój własny profil zasad.

Dostępne instrukcje:

- Konsola administracyjna:
  - Tworzenie profilu zasad
  - Tworzenie reguły aktywacji profilu zasad
- Kaspersky Security Center Web Console:
  - Tworzenie profilu zasad
  - Tworzenie reguły aktywacji profilu zasad

3. **Przesyłanie zasad i profili zasad na zarządzane urządzenia**

   Domyślnie Serwer administracyjny automatycznie synchronizuje się z zarządzanymi urządzeniami co 15 minut. Możesz obejść automatyczną synchronizację i ręcznie uruchomić synchronizację przy pomocy polecenia Wymuś synchronizację. Synchronizacja jest również wymuszana po utworzeniu lub zmianie zasady lub profilu zasady. Podczas synchronizacji nowe lub zmienione zasady i profile zasad zostają rozesłane na zarządzane urządzenia.

   Jeśli używasz Kaspersky Security Center Web Console, możesz sprawdzić, czy profile i profile zasad zostały dostarczone na urządzenie. Kaspersky Security Center określa datę i godzinę dostarczenia we właściwościach urządzenia.

   Dostępne instrukcje:

   - Konsola administracyjna: Wymuszona synchronizacja
   - Kaspersky Security Center Web Console: Wymuszona synchronizacja

Wyniki

Po zakończeniu scenariusza skoncentrowanego na urządzeniu, aplikacje Kaspersky są konfigurowane zgodnie z ustawieniami określonymi i przesłanymi poprzez hierarchię zasad.

Skonfigurowane zasady i profile zasad aplikacji zostaną automatycznie zastosowane do nowych urządzeń dodanych do grup administracyjnych.

Konfiguracja i przydzielanie zasad: Metoda skoncentrowana na użytkowniku

Ta sekcja opisuje scenariusz skoncentrowanej na użytkowniku scentralizowanej konfiguracji aplikacji Kaspersky zainstalowanych na zarządzanych urządzeniach. Po zakończeniu tego scenariusza, aplikacje zostaną skonfigurowane na wszystkich zarządzanych urządzeniach zgodnie z zasadami i profilami zasad aplikacji, które określiłeś.

Ten scenariusz można zaimplementować za pomocą Kaspersky Security Center Web Console w wersji 13 lub nowszej.

Wymagania wstępne

Przed rozpoczęciem konfiguracji upewnij się, że pomyślnie zainstalowano Serwer administracyjny Kaspersky Security Center i Kaspersky Security Center Web Console, a także zakończono główny scenariusz instalacji. Możesz wziąć pod uwagę zarządzanie ochroną skoncentrowaną na urządzeniu jako alternatywę lub dodatkową opcję dla metody skoncentrowanej na użytkowniku. Dowiedz się więcej na temat dwóch metod zarządzania.

Proces

Scenariusz skoncentrowanego na użytkowniku zarządzania aplikacjami Kaspersky obejmuje następujące kroki:

1. **Konfigurowanie zasad aplikacji**

   Skonfiguruj ustawienia dla aplikacji firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach poprzez utworzenie zasady dla każdej aplikacji. Zestaw zasad zostanie przesłany na urządzenia klienckie.

   Jeśli konfigurujesz ochronę swojej sieci w kreatorze wstępnej konfiguracji, Kaspersky Security Center tworzy domyślną zasadę dla Kaspersky Endpoint Security. Jeśli zakończyłeś proces konfiguracji przy użyciu tego kreatora, nie musisz tworzyć nowej zasady dla tej aplikacji. Przejdź do ręcznej konfiguracji zasady Kaspersky Endpoint Security.

   Jeśli masz hierarchiczną strukturę kilku Serwerów administracyjnych i/lub grup administracyjnych, domyślnie podrzędne Serwery administracyjne i podrzędne grupy administracyjne dziedziczą zasady z głównego Serwera administracyjnego. Możesz wymusić dziedziczenie przez grupy podrzędne i podrzędne Serwery administracyjne, aby zabronić wszelkich modyfikacji ustawień skonfigurowanych w nadrzędnej zasadzie. Jeśli chcesz, żeby wymuszone było dziedziczenie tylko części ustawień, możesz zablokować je w zasadzie nadrzędnej. Pozostałe niezablokowane ustawienia będą dostępne do modyfikacji w zasadach podrzędnych. Utworzona hierarchia zasad umożliwi efektywne zarządzanie urządzeniami w grupach administracyjnych.

   Dostępne instrukcje: Tworzenie zasady

2. **Określanie właścicieli urządzeń**

   Przypisz zarządzane urządzenia do odpowiednich użytkowników.

   Dostępne instrukcje: Wskazywanie użytkownika jako właściciela urządzenia

3. **Określanie ról użytkownika typowych dla Twojej firmy**

   Pomyśl o różnych rodzajach pracy, jaką pracownicy Twojej firmy zazwyczaj wykonują. Musisz podzielić wszystkich pracowników zgodnie z ich rolami. Na przykład, możesz podzielić ich według działów, profesji lub pozycji. Następnie musisz utworzyć rolę użytkownika dla każdej grupy. Pamiętaj, że każda rola użytkownika będzie posiadała swój własny profil zasad zawierający ustawienia aplikacji specyficzne dla tej roli.

4. **Tworzenie ról użytkownika**

   Utwórz i skonfiguruj rolę użytkownika dla każdej grupy pracowników, którą określiłeś w poprzednim kroku, lub użyj predefiniowanej roli użytkownika. Role użytkownika będą zawierały zestaw uprawnień dostępu do funkcji aplikacji.

   Dostępne instrukcje: Tworzenie roli użytkownika

5. **Określanie obszaru każdej roli użytkownika**

   Dla każdej utworzone roli użytkownika określ użytkowników i/lub grupy bezpieczeństwa oraz grupy administracyjne. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup podrzędnych.

   Dostępne instrukcje: Edytowanie obszaru roli użytkownika

6. **Tworzenie profili zasad**

   Utwórz profil zasad dla każdej roli użytkownika w Twojej firmie. Profile zasad określają, które ustawienia zostaną zastosowane w aplikacjach zainstalowanych na urządzeniach użytkowników w zależności od roli każdego użytkownika.

   Dostępne instrukcje: Tworzenie profilu zasad

7. **Kojarzenie profili zasad z rolami użytkownika**

   Skojarz utworzone profile zasad z rolami użytkownika. Następnie: profil zasad stanie się aktywny dla użytkowników, którzy posiadają określoną rolę. Ustawienia skonfigurowane w profilu zasad zostaną zastosowane do aplikacji Kaspersky zainstalowanych na urządzeniach użytkownika.

   Dostępne instrukcje: Kojarzenie profili zasad z rolami

8. **Przesyłanie zasad i profili zasad na zarządzane urządzenia**

   Domyślnie Serwer administracyjny automatycznie synchronizuje się z zarządzanymi urządzeniami co 15 minut. Podczas synchronizacji nowe lub zmienione zasady i profile zasad zostają rozesłane na zarządzane urządzenia. Możesz obejść automatyczną synchronizację i ręcznie uruchomić synchronizację przy pomocy polecenia Wymuś synchronizację. Po zakończeniu synchronizacji, aby zapewnić dostarczenie i zastosowanie zasad i profili zasad do zainstalowanych aplikacji Kaspersky.

   Możesz sprawdzić, czy zasady i profile zasad zostały dostarczone na urządzenie. Kaspersky Security Center określa datę i godzinę dostarczenia we właściwościach urządzenia.

   Dostępne instrukcje: Wymuszona synchronizacja

Wyniki

Po zakończeniu scenariusza skoncentrowanego na użytkowniku, aplikacje Kaspersky są konfigurowane zgodnie z określonymi ustawieniami i przesyłane poprzez hierarchię zasad i profili zasad.

Dla nowego użytkownika konieczne będzie utworzenie nowego konta, przypisanie użytkownikowi jednej z utworzonych ról użytkownika, a także przypisane urządzeń do użytkownika. Skonfigurowane zasady i profile zasad aplikacji zostaną automatycznie zastosowane do urządzeń tego użytkownika.

Ustawienia zasady Agenta sieciowego

W celu skonfigurowania zasady Agenta sieciowego:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Kliknij nazwę zasady Agenta sieciowego.

   Zostanie otwarte okno właściwości zasady Agenta sieciowego.

Zobacz tabelę porównawczą, w której szczegółowo opisano, jak poniższe ustawienia mają zastosowanie w zależności od używanego systemu operacyjnego.

Ogólne

Na tej zakładce możesz zmodyfikować stan zasady oraz określić dziedziczenie ustawień zasady:

- W sekcji **Stan zasady** możesz wybrać jeden z trybów zasady:
  - **Aktywny**

    Jeśli wybrano tę opcję, zasada jest aktywna.

    Domyślnie opcja ta jest zaznaczona.
  - **Nieaktywny**

    Jeśli ta opcja jest zaznaczona, zasada stanie się nieaktywna, ale wciąż będzie przechowywana w folderze **Zasady**. Jeśli jest to wymagane, zasadę można aktywować.
- W grupie ustawień **Dziedziczenie ustawień** możesz skonfigurować dziedziczenie zasady:
  - **Dziedzicz ustawienia z zasady nadrzędnej**

    Jeśli ta opcja jest włączona, wartości ustawień zasady są dziedziczone z zasady grupy najwyższego poziomu, są więc zablokowane.

    Domyślnie opcja ta jest włączona.
  - **Wymuś dziedziczenie ustawień w zasadach podrzędnych**

    Jeśli ta opcja jest włączona, po zastosowaniu zmian w zasadzie zostaną wykonane następujące czynności:
    - Wartości ustawień zasady zostaną rozesłane do zasad podgrup administracyjnych, czyli do zasad podrzędnych.
    - Opcja **Dziedzicz ustawienia z zasady nadrzędnej** będzie automatycznie włączona w podsekcji **Dziedziczenie ustawień** sekcji **Ogólne** okna właściwości każdej zasady podrzędnej.

    Jeśli ta opcja jest włączona, ustawienia zasad podrzędnych są zablokowane.

    Domyślnie opcja ta jest wyłączona.

Konfiguracja zdarzenia

Na tej zakładce możesz skonfigurować rejestrowania zdarzeń oraz powiadamianie o zdarzeniach. Zdarzenia są rozsyłane zgodnie z priorytetem w następujących sekcjach na zakładce **Konfiguracja zdarzenia**:

- **Błąd funkcjonalny**
- **Ostrzeżenie**
- **Informacja**

W każdej sekcji, lista typów zdarzeń wyświetla typy zdarzeń oraz domyślny czas przechowywania zdarzeń na Serwerze administracyjnym (w dniach). Po kliknięciu typu zdarzenia możesz określić ustawienia zapisywania zdarzeń oraz powiadomień o zdarzeniach wybranych z listy. Domyślnie, podstawowe ustawienia powiadamiania, określone dla całego Serwera administracyjnego, są używane dla wszystkich typów zdarzeń. Jednakże możesz zmienić określone ustawienia dla żądanych typów zdarzeń.

Na przykład, w sekcji **Ostrzeżenie** możesz skonfigurować typ zdarzenia **Wystąpił incydent związany z bezpieczeństwem**. Takie zdarzenia mogą mieć miejsce, na przykład, gdy wolne miejsce na dysku punktu dystrybucji jest mniejsze niż 2 GB (co najmniej 4 GB są wymagane do zdalnego instalowania aplikacji i pobierania aktualizacji). Aby skonfigurować zdarzenie **Wystąpił incydent związany z bezpieczeństwem**, kliknij je i określ, gdzie mają być przechowywane zdarzenia i jak powiadamiać o nich.

Jeśli Agent sieciowy wykrył problem bezpieczeństwa, możesz nim zarządzać za pomocą ustawień zarządzanego urządzenia.

Ustawienia aplikacji

Ustawienia

W sekcji **Ustawienia** możesz skonfigurować zasadę Agenta sieciowego:

- **Rozsyłaj pliki tylko poprzez punkty dystrybucji**

  Jeśli ta opcja jest włączona, Agenty sieciowe na zarządzanych urządzeniach pobierają uaktualnienia tylko z punktów dystrybucji.

  Jeśli ta opcja jest wyłączona, Agenty sieciowe na zarządzanych urządzeniach pobierają uaktualnienia z punktów dystrybucji lub z Serwera administracyjnego.

  Należy pamiętać, że aplikacje zabezpieczające na zarządzanych urządzeniach pobierają uaktualnienia ze źródła ustawionego w zadaniu aktualizacji dla każdej aplikacji zabezpieczającej. Jeśli włączysz opcję **Rozsyłaj pliki tylko poprzez punkty dystrybucji**, upewnij się, że Kaspersky Security Center jest ustawiony jako źródło uaktualnień w zadaniach aktualizacji.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar kolejki zdarzeń, w MB**

  W tym polu możesz określić maksymalny rozmiar przestrzeni dyskowej zajmowanej przez kolejkę zdarzenia.

  Domyślna wartość to 2 megabajty (MB).

- **Aplikacja może pobierać rozszerzone dane zasad na urządzenie**

  Agent sieciowy zainstalowany na zarządzanym urządzeniu przesyła informacje o zastosowanej zasadzie aplikacji zabezpieczającej (na przykład, Kaspersky Endpoint Security for Windows). Przesłane informacje możesz przejrzeć w interfejsie aplikacji zabezpieczającej.

  Agent sieciowy przesyła następujące informacje:

  - Czas dostarczenia zasady na zarządzane urządzenie.
  - Nazwę aktywnej zasady w momencie dostarczenia zasady na zarządzane urządzenie.
  - Nazwę zasady użytkowania mobilnego w momencie dostarczenia jej do zarządzanego urządzenia (niedostępna dla Agenta sieciowego dla systemu Linux).
  - Nazwę i pełną ścieżkę do grupy administracyjnej, która zawierała zarządzane urządzenie w momencie dostarczenia zasady na zarządzane urządzenie.
  - Listę aktywnych profili zasad wraz z ich nazwami i priorytetami w momencie dostarczenia zasad do zarządzanego urządzenia.

  Możesz użyć informacji, aby zapewnić, że poprawna zasada zostanie zastosowana do urządzenia oraz aby rozwiązać problemy. Domyślnie opcja ta jest wyłączona.

- **Chroń usługę Agenta sieciowego przed nieuprawnionym usuwaniem, zatrzymywaniem i zmianami ustawień**

  Gdy ta opcja pozostaje aktywna, po zainstalowaniu Agenta sieciowego na zarządzanym urządzeniu, składnik nie może zostać usunięty ani ponownie skonfigurowany bez wymaganych uprawnień. Usługa Agenta sieciowego nie może zostać zatrzymana. Ta opcja nie ma wpływu na kontrolery domeny.

  Włącz tę opcję, aby chronić Agenta sieciowego na stacjach roboczych obsługiwanych z uprawnieniami lokalnego administratora.

  Domyślnie opcja ta jest wyłączona.

- **Użyj hasła dezinstalacyjnego**

  Jeśli ta opcja jest włączona, klikając przycisk **Modyfikuj**, można określić hasło do narzędzia klmover i zdalnej dezinstalacji Agenta sieciowego.

  Domyślnie opcja ta jest wyłączona.

Repozytoria

W sekcji **Repozytoria** możesz wybrać typy obiektów, których szczegóły zostaną wysłane z Agenta sieciowego na Serwer administracyjny. Jeśli modyfikacja niektórych ustawień w tej sekcji jest zablokowana przez zasadę Agenta sieciowego, nie można ich modyfikować.

- **Szczegóły zainstalowanych aplikacji**

  Jeśli ta opcja jest włączona, informacje o aplikacjach zainstalowanych na urządzeniach klienckich są przesyłane do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Dołącz informacje o poprawkach**

  Informacje o poprawkach aplikacji zainstalowanych na urządzeniach klienckich są wysyłane do Serwera administracyjnego. Włączenie tej opcji może zwiększyć obciążenie na Serwerze administracyjnym oraz DBMS, a także spowodować zwiększenie rozmiaru bazy danych.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

- **Szczegóły aktualizacji Windows Update**

  Jeśli ta opcja jest włączona, informacje o aktualizacjach Microsoft Windows Update, które powinny zostać zainstalowane na urządzeniach klienckich, są przesyłane do Serwera administracyjnego.

  Czasami, nawet wtedy, gdy opcja jest wyłączona, aktualizacje są wyświetlanie we właściwościach urządzenia w sekcji **Dostępne aktualizacje**. To może mieć miejsce, gdy, na przykład, urządzenia w organizacji zawierają luki, które mogłyby zostać wyeliminowane przez te aktualizacje.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

  Informacje o opcjonalnych aktualizacjach Microsoft Windows nie są wysyłane do Serwera administracyjnego.

- **Szczegóły luk w oprogramowaniu oraz odpowiednich aktualizacji**

  Jeśli ta opcja jest włączona, informacje o lukach w oprogramowaniu innej firmy (w tym oprogramowaniu firmy Microsoft), wykrytych na zarządzanych urządzeniach, oraz o aktualizacjach oprogramowania, które eliminują luki innych firm (nie dotyczy oprogramowania firmy Microsoft) są wysyłane do Serwera administracyjnego.

  Wybranie tej opcji (**Szczegóły luk w oprogramowaniu oraz odpowiednich aktualizacji**) zwiększy obciążenie sieci, obciążenie dysku Serwera administracyjnego oraz zużycie zasobów Agenta sieciowego.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

  Aby zarządzać aktualizacjami oprogramowania firmy Microsoft, użyj opcji **Szczegóły aktualizacji Windows Update**.

- **Szczegóły rejestru sprzętu**

  Agent sieciowy zainstalowany na urządzeniu wysyła informacje o sprzęcie urządzenia do Serwera administracyjnego. Możesz przejrzeć szczegóły sprzętu we właściwościach urządzenia.

  Upewnij się, że narzędzie lshw jest zainstalowane na urządzeniach z systemem Linux, z których chcesz pobrać szczegółowe informacje o sprzęcie. Dane sprzętowe przechwytywane z maszyn wirtualnych mogą być niekompletne – w zależności od używanego hipernadzorcy.

Aktualizacje oprogramowania i luki

W sekcji **Aktualizacje oprogramowania i luki** możesz skonfigurować wyszukiwanie i rozsyłanie aktualizacji systemu Windows, a także włączyć skanowanie plików wykonywalnych w poszukiwaniu luk:

- **Użyj Serwera administracyjnego jako serwera WSUS**

  Jeśli ta opcja jest włączona, aktualizacje systemu Windows są pobierane na Serwer administracyjny. Serwer administracyjny dostarcza pobrane aktualizacje usłudze Windows Update na urządzeniach klienckich w trybie scentralizowanym przy użyciu Agentów sieciowych.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie używany do pobierania aktualizacji systemu Windows. W tym przypadku urządzenia klienckie same pobierają aktualizacje systemu Windows.

  Domyślnie opcja ta jest wyłączona.

- Możesz ograniczyć aktualizacje systemu Windows, które użytkownicy mogą zainstalować na swoich urządzeniach ręcznie, korzystając z Windows Update.

  Na urządzeniach działających pod kontrolą systemu Windows 10, jeśli usługa Windows Update już wykryła aktualizacje dla urządzenia, nowa opcja, którą wybierzesz w sekcji **Zezwalaj użytkownikom na zarządzanie instalowaniem aktualizacji Windows Update**, zostaną zastosowane dopiero po zainstalowaniu wykrytych aktualizacji.

  Wybierz element z listy rozwijalnej:

  - **Zezwalaj użytkownikom na instalację wszystkich dostępnych aktualizacji Windows Update**

    Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach.

    Wybierz tę opcję, jeśli nie chcesz uczestniczyć w instalacji aktualizacji.

    Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

  - **Zezwalaj użytkownikom na instalację wszystkich zatwierdzonych aktualizacji Windows Update**

    Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach i które zostały zatwierdzone przez Ciebie.

    Na przykład, możesz chcieć najpierw sprawdzić instalację aktualizacji w środowisku testowym i upewnić się, że nie wpływają negatywnie na działanie urządzeń, a następnie zezwolić na instalację tylko tych zatwierdzonych aktualizacji.

    Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

- **Nie zezwalaj użytkownikom na instalowanie aktualizacji Windows Update**

  Użytkownicy nie mogą ręcznie zainstalować aktualizacji Microsoft Windows Update na swoich urządzeniach. Wszystkie stosowane aktualizacje są instalowane w sposób skonfigurowany przez Ciebie.

  Wybierz tę opcję, jeśli chcesz zarządzać instalacją aktualizacji w sposób scentralizowany.

  Na przykład, możesz chcieć zoptymalizować terminarz aktualizacji, aby sieć nie została przeciążona. Możesz skonfigurować terminarz aktualizacji po godzinach, aby nie przeszkadzały w pracy użytkowników.

- W grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** możesz wybrać tryb wyszukiwania aktualizacji:

  - **Aktywny**

    Jeśli ta opcja jest zaznaczona, Serwer administracyjny z pomocą Agenta sieciowego przesyła żądanie z Agenta Windows Update na urządzeniu klienckim do źródła uaktualnień: Serwery Windows Update lub WSUS. Następnie Agent sieciowy przesyła informacje z usługi Windows Update Agent do Serwera administracyjnego.

    Opcja zaczyna działać tylko wtedy, gdy zaznaczona jest opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

    Domyślnie opcja ta jest zaznaczona.

  - **Pasywny**

    Jeżeli ta opcja jest zaznaczona, Agent sieciowy co jakiś czas przesyła informacje od Serwera administracyjnego dotyczące aktualizacji pobranych przy ostatniej synchronizacji agenta usługi Windows Update ze źródłem uaktualnień. Jeśli nie zostanie przeprowadzona synchronizacja agenta usługi Windows Update ze źródłem uaktualnień, informacje o aktualizacjach Serwera administracyjnego będą przestarzałe.

    Wybierz tę opcję, jeśli chcesz uzyskać aktualizacje z pamięci podręcznej źródła uaktualnień.

  - **Wyłączone**

    Jeśli ta opcja jest zaznaczona, Serwer administracyjny nie żąda informacji dotyczących aktualizacji.

    Wybierz tę opcję, gdy, na przykład, chcesz najpierw przetestować aktualizacje na swoim lokalnym urządzeniu.

- **Skanuj pliki wykonywalne w poszukiwaniu luk podczas ich uruchamiania**

  Jeśli ta opcja jest włączona, pliki wykonywalne są skanowane w poszukiwaniu luk podczas ich uruchamiania.

  Domyślnie opcja ta jest włączona.

Zarządzanie ponownym uruchamianiem

W sekcji **Zarządzanie ponownym uruchamianiem** możesz określić działanie, jakie zostanie wykonane, jeśli system operacyjny urządzenia zarządzanego musi być uruchomiony ponownie, gdy korzystasz, instalujesz lub dezinstalujesz aplikację:

- **Nie uruchamiaj ponownie systemu operacyjnego**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Jeżeli będzie to wymagane, automatycznie uruchom ponownie system operacyjny**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

  - **Wymuś restart po (min)**

    Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

    Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  - **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

    Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

    Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

    Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

    Domyślnie opcja ta jest wyłączona.

Udostępnianie pulpitu Windows

W sekcji **Udostępnianie pulpitu Windows** możesz włączyć i skonfigurować audyt działań administratora wykonywanych na zdalnym urządzeniu podczas współdzielenia dostępu do pulpitu:

- **Włącz audyt**

  Jeśli ta opcja jest włączona, audyt działań administratora na zdalnym urządzeniu jest włączony. Wpisy dotyczące działań administratora na zdalnym urządzeniu są zapisywane w:

  - Raporcie zdarzeń na zdalnym urządzeniu
  - W pliku z rozszerzeniem syslog, znajdującym się w folderze instalacyjnym Agenta sieciowego na zdalnym urządzeniu
  - W bazie danych zdarzeń programu Kaspersky Security Center

  Audyt działań administratora jest dostępny, gdy są spełnione następujące warunki:

  - Licencja Zarządzanie lukami i poprawkami jest w użyciu
  - Administrator posiada uprawnienie do włączania współdzielonego dostępu do pulpitu zdalnego urządzenia

  Jeśli ta opcja jest wyłączona, audyt działań administratora na zdalnym urządzeniu jest wyłączony.

  Domyślnie opcja ta jest wyłączona.

- **Maski plików, które będą monitorowane podczas odczytu**

  Lista zawiera maski plików. Jeśli audyt jest włączony, aplikacja monitoruje odczytywanie plików przez administratora, które odpowiadają maskom, i zapisuje informacje o odczycie plików. Lista jest dostępna, jeśli pole **Włącz audyt** jest zaznaczone. Możesz zmodyfikować maski plików i dodać nowe do listy. Każda nowa maska pliku powinna być określona na liście w nowym wierszu.

  Domyślnie określone są następujące maski plików:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Maski plików, które będą monitorowane podczas modyfikacji**

  Lista zawiera maski plików na zdalnym urządzeniu. Jeśli audyt jest włączony, aplikacja monitoruje zmiany wprowadzone przez administratora w plikach, które odpowiadają maskom, i zapisuje informacje o tych modyfikacjach. Lista jest dostępna, jeśli pole **Włącz audyt** jest zaznaczone. Możesz zmodyfikować maski plików i dodać nowe do listy. Każda nowa maska pliku powinna być określona na liście w nowym wierszu.

  Domyślnie określone są następujące maski plików:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Zarządzaj poprawkami i aktualizacjami

W sekcji **Zarządzaj poprawkami i aktualizacjami** możesz skonfigurować pobieranie i dystrybucję uaktualnień oraz instalację poprawek na zarządzanych urządzeniach:

- **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**

  Jeśli ta opcja jest włączona, poprawki Kaspersky ze stanem zatwierdzenia *Niezdefiniowane* będą automatycznie instalowane na zarządzanych urządzeniach natychmiast po pobraniu z serwerów aktualizacji.

  Jeśli ta opcja jest wyłączona, poprawki Kaspersky, które zostały pobrane i oznaczone jako *Niezdefiniowane*, zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzone*.

Domyślnie opcja ta jest włączona.

- **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)**

  Jeśli ta opcja jest włączona, tryb offline pobierania aktualizacji jest używany. Jeśli Serwer administracyjny pobierze uaktualnienia, powiadomi Agenta sieciowego (na urządzeniach, na których jest zainstalowany) o uaktualnieniach, które będą wymagane dla zarządzanych aplikacji. Jeśli Agent sieciowy otrzyma informacje o tych uaktualnieniach, pobierze odpowiednie pliki z Serwera administracyjnego z wyprzedzeniem. Przy pierwszym nawiązaniu połączenia z Agentem sieciowym, Serwer administracyjny inicjuje pobranie aktualizacji. Jeśli Agent sieciowy pobierze wszystkie uaktualnienia na urządzenie klienckie, staną się one dostępne dla aplikacji na tym urządzeniu.

  Jeśli zarządzana aplikacja na urządzeniu klienckim spróbuje uzyskać dostęp do Agenta sieciowego w celu uzyskania uaktualnień, Agent sieciowy sprawdzi, czy posiada wszystkie wymagane uaktualnienia. Jeśli uaktualnienia zostały pobrane z Serwera administracyjnego nie więcej niż 25 godzin przed zażądaniem ich przez zarządzaną aplikację, Agent sieciowy nie nawiąże połączenia z Serwerem administracyjnym, ale dostarczy zarządzanej aplikacji uaktualnienia z lokalnej pamięci podręcznej. Połączenie z Serwerem administracyjnym może nie zostać nawiązane, gdy Agent sieciowy dostarcza uaktualnienia aplikacji na urządzeniach klienckich, ale połączenie nie jest wymagane w celu przeprowadzenia aktualizacji.

  Jeśli ta opcja jest wyłączona, tryb offline pobierania aktualizacji nie jest używany. Uaktualnienia są rozsyłane zgodnie z terminarzem zadania pobierania aktualizacji.

  Domyślnie opcja ta jest włączona.

Łączność

Sekcja **Łączność** zawiera trzy podsekcje:

- **Sieć**
- **Profile połączenia**
- **Terminarz połączeń**

W podsekcji **Sieć** możesz skonfigurować połączenie z Serwerem administracyjnym, włączyć korzystanie z portu UDP oraz określić numer UDP.

- W grupie ustawień **Połącz z Serwerem administracyjnym** możesz skonfigurować połączenie z serwerem administracyjnym oraz określić przedziału czasu dla synchronizacji pomiędzy urządzeniami klienckimi a serwerem administracyjnym:

  - **Okres synchronizacji (min)**

    Agent sieciowy synchronizuje zarządzane urządzenie z Serwerem administracyjnym. Zalecane jest ustawienie okresu synchronizacji (zwanego także puls) na 15 minut dla 10 000 zarządzanych urządzeń.

  - **Kompresuj ruch sieciowy**

    Jeżeli ta opcja jest włączona, prędkość transferu danych przez Agenta sieciowego zostaje zwiększona poprzez zmniejszenie ilości przesyłanych informacji i tym samym zmniejszenie obciążenia Serwera administracyjnego.

    Obciążenie procesora komputera klienckiego może się zwiększyć.

Domyślnie pole to jest zaznaczone.

- **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows**

  Jeżeli ta opcja jest włączona, porty niezbędny do pracy Agenta sieciowego i serwera administracyjnego, zostaną dodane do listy wykluczeń Zapory systemu Microsoft Windows.

  Domyślnie opcja ta jest włączona.

- **Użyj połączenia SSL**

  Jeśli ta opcja jest włączona, połączenie z Serwerem administracyjnym jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

  Domyślnie opcja ta jest włączona.

- **Użyj bramy połączenia na punkcie dystrybucji (jeśli jest dostępny) w domyślnych ustawieniach połączenia**

  Jeśli ta opcja jest włączona, brama połączenia na punkcie dystrybucji jest używana z ustawieniami określonymi we właściwościach grupy administracyjnej.

  Domyślnie opcja ta jest włączona.

- **Użyj portu UDP**

  Jeśli chcesz, żeby Agent Sieciowy nawiązywał połączenie z Serwerem administracyjnym poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **Numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z Serwerem administracyjnym to 15000.

- **Numer portu UDP**

  W tym polu możesz wprowadzić numer portu UDP. Domyślny numer portu to 15000.

  Używany jest system dziesiętny.

  Jeżeli na urządzeniu klienckim zainstalowany jest system Windows XP Service Pack 2, wówczas wbudowana zapora sieciowa będzie blokowała port UDP o numerze 15000. Port ten należy otworzyć ręcznie.

- **Użyj punktu dystrybucji, aby wymusić połączenie z Serwerem administracyjnym**

  Wybierz tę opcję, jeśli w oknie ustawień punktu dystrybucji zaznaczyłeś opcję **Użyj tego punktu dystrybucji jako serwera push**. W przeciwnym razie punkt dystrybucji nie będzie działał jako serwer push.

W podsekcji **Profile połączenia** możesz określić ustawienia lokalizacji sieciowej i włączyć tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny:

- **Ustawienia lokalizacji sieciowej**

  Ustawienia lokalizacji sieciowej definiują cechy sieci, do której podłączone jest urządzenie klienckie, i określają reguły przełączania Agenta sieciowego z jednego profilu połączenia Serwera administracyjnego do innego, gdy te cechy sieci zostaną zmienione.

- **Profile połączeń Serwera administracyjnego**

  W tej sekcji możesz dodawać i wyświetlać profile połączenia Agenta sieciowego z Serwerem administracyjnym. W tej sekcji możesz także utworzyć reguły przełączania Agenta sieciowego na inne Serwery administracyjne, gdy wystąpią następujące zdarzenia:

  - Gdy urządzenie klienckie zostanie podłączone do innej sieci lokalnej
  - Gdy zostanie zerwane połączenie między urządzeniem a siecią lokalną organizacji
  - Gdy adres bramy połączenia zostanie zmieniony lub adres serwera DNS zostanie zmodyfikowany

  > Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows i macOS.

- **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny**

  Jeśli ta opcja jest włączona, w przypadku połączenia przez ten profil, aplikacje zainstalowane na urządzeniu klienckim będą używać profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

  Jeżeli ta opcja jest wyłączona, aplikacje będą używać zasad aktywnych.

  Domyślnie opcja ta jest wyłączona.

W podsekcji **Terminarz połączeń** możesz określić przedziały czasu, w trakcie których Agent sieciowy wysyła dane do Serwera administracyjnego:

- **Połącz, gdy jest to konieczne**

  Jeśli ta opcja jest zaznaczona, połączenie jest nawiązywane, gdy Agent sieciowy musi wysłać dane na Serwer administracyjny.

  Domyślnie opcja ta jest zaznaczona.

- **Połącz w określonych przedziałach czasu**

  Jeśli ta opcja jest zaznaczona, Agent sieciowy łączy się z Serwerem administracyjnym w określonym czasie. Możesz dodać kilka przedziałów czasu.

Przeszukiwanie sieci według punktów dystrybucji

W sekcji **Przeszukiwanie sieci według punktów dystrybucji** możesz skonfigurować automatyczne przeszukiwanie sieci. W celu włączenia przeszukiwania sieci i skonfigurowania jego częstotliwości możesz użyć następujących opcji:

- **Sieć Windows**

  Jeśli ta opcja jest włączona, Serwer administracyjny automatycznie przeszuka sieć zgodnie z terminarzem skonfigurowanym po kliknięciu odnośników **Ustaw terminarz szybkiego przeszukiwania** i **Ustaw terminarz pełnego przeszukiwania**.

  Jeżeli ta opcja jest wyłączona, Serwer administracyjny przeszukuje sieć z częstotliwością określoną w polu **Częstotliwość przeszukiwania sieci (min)**.

Interwał wykrywania urządzeń dla Agenta sieciowego w wersjach przed 10.2 może zostać skonfigurowany w polach **Częstotliwość pobierania informacji z domen Windows (min)** (w przypadku szybkiego przeszukiwania sieci z domen Windows) i **Częstotliwość przeszukiwania sieci (min)** (w przypadku pełnego przeszukiwania sieci z domen Windows).

Domyślnie opcja ta jest wyłączona.

- **Zeroconf**

  Jeśli ta opcja jest włączona, punkt dystrybucji automatycznie przeszukuje sieć za pomocą urządzeń IPv6, używając zero-configuration networking (zwany również *Zeroconf*). W takim przypadku włączone przeszukiwanie zakresu adresów IP jest ignorowane, ponieważ punkt dystrybucji przeszukuje całą sieć.

  W celu rozpoczęcia korzystania z Zeroconf, muszą być spełnione następujące warunki:

  - Punkt dystrybucji musi działać pod systemem Linux.
  - Musisz zainstalować narzędzie avahi-browse na punkcie dystrybucji.

  Jeśli ta opcja jest wyłączona, punkt dystrybucji nie przeszukuje sieci z urządzeniami IPv6.

  Domyślnie opcja ta jest wyłączona.

- **Zakresy IP**

  Jeśli opcja jest włączona, punkt dystrybucji automatycznie przeszuka zakresy IP zgodnie z terminarzem skonfigurowanym po kliknięciu przycisku **Ustaw terminarz przeszukiwania**.

  Jeśli ta opcja jest wyłączona, Serwer punkt dystrybucji nie będzie przeszukiwał zakresów IP.

  Częstotliwość przeszukiwania zakresu IP dla Agenta sieciowego w wersjach poprzedzających 10.2 może być skonfigurowana w polu **Interwał przeszukiwania (min)**. Pole jest dostępne, jeśli opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

- **Sterowniki domeny**

  Jeśli ta opcja jest włączona, punkt dystrybucji automatycznie przeszuka Active Directory zgodnie z terminarzem skonfigurowanym po kliknięciu odnośnika **Ustaw terminarz przeszukiwania**.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie przeszukiwał Active Directory.

  Częstotliwość przeszukiwania Active Directory dla Agenta sieciowego w wersjach poprzedzających 10.2 może być skonfigurowana w polu **Interwał przeszukiwania (min)**. Pole jest dostępne, jeśli ta opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

  Jeśli opcja jest włączona, punkt dystrybucji automatycznie przeszuka kontrolery domeny zgodnie z terminarzem skonfigurowanym po kliknięciu przycisku **Ustaw terminarz przeszukiwania**.

  Jeśli ta opcja jest wyłączona, punkt dystrybucji nie będzie przeszukiwał kontrolerów domeny.

  Częstotliwość przeszukiwania kontrolera domeny dla Agenta sieciowego w wersjach poprzedzających 10.2 może być skonfigurowana w polu **Interwał przeszukiwania (min)**. Pole jest dostępne, jeśli ta opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

Ustawienia sieci dla punktów dystrybucji

Jeśli Twoje punkty dystrybucji korzystają z serwera proxy podczas łączenia się z Internetem, w sekcji **Ustawienia sieci dla punktów dystrybucji** możesz określić następujące ustawienia:

- **Użyj serwera proxy**
- **Adres**
- **Numer portu**
- **Pomiń serwer proxy dla adresów lokalnych**

  Jeśli ta opcja jest włączona, żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

  Domyślnie opcja ta jest wyłączona.

- **Uwierzytelnianie na serwerze proxy**

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  Domyślnie pole to nie jest zaznaczone.

- **Nazwa użytkownika**
- **Hasło**

KSN Proxy (punkty dystrybucji)

W sekcji **KSN Proxy (punkty dystrybucji)** możesz skonfigurować aplikację tak, aby używała punktu dystrybucji do przekazywania żądań Kaspersky Security Network (KSN) z zarządzanych urządzeń:

- **Włącz KSN Proxy po stronie punktu dystrybucji**

  Usługa KSN proxy jest uruchamiana na urządzeniu, które jest używane jako punkt dystrybucji. Użyj tej funkcji do redystrybucji i optymalizacji ruchu w sieci.

  Punkt dystrybucji wysyła statystyki KSN, które zostały wymienione w Oświadczeniu Kaspersky Security Network, do Kaspersky.

  Domyślnie opcja ta jest wyłączona. Włączenie tej opcji działa, jeśli opcje **Użyj Serwera administracyjnego jako serwera proxy** i **Zgadzam się na korzystanie z Kaspersky Security Network** zostały włączone w oknie właściwości Serwera administracyjnego.

  Możesz przypisać węzeł klastra aktywny-pasywny do punktu dystrybucji i włączyć serwer proxy KSN na tym węźle.

- **Przesyłaj żądania KSN do Serwera administracyjnego**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do chmury KSN lub KPSN. Żądania KSN wygenerowane na samym punkcie dystrybucji są także wysyłane bezpośrednio do chmury KSN lub KPSN.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej), nie mogą uzyskać bezpośredniego dostępu do KPSN. Jeśli chcesz ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do KPSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 12 (lub późniejszej), mogą uzyskać bezpośredni dostęp do KPSN.

- **Port**

  Numer portu TCP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny numer portu to 13111.

- **Port UDP**

  Jeśli chcesz, żeby Agent Sieciowy nawiązywał połączenie z Serwerem administracyjnym poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **Numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z Serwerem administracyjnym to 15000.

Aktualizacje (punkty dystrybucji)

W sekcji **Aktualizacje (punkty dystrybucji)** możesz włączyć funkcję pobierania plików diff, dzięki czemu punkty dystrybucji pobierają aktualizacje w postaci plików diff z serwerów aktualizacji firmy Kaspersky.

Zarządzanie kontem lokalnym (tylko Linux)

Sekcja **Zarządzanie kontem lokalnym (tylko Linux)** zawiera trzy podsekcje:

- **Zarządzanie certyfikatami użytkowników**
- **Dodaj lub edytuj odpowiednie lokalne grupy administratorów**
- **Prześlij plik referencyjny, aby chronić plik sudoers na urządzeniu użytkownika przed zmianami**

W podsekcji **Zarządzanie certyfikatami użytkowników** możesz określić, które certyfikaty główne mają zostać zainstalowane. Certyfikaty te mogą służyć np. do weryfikacji autentyczności stron internetowych czy serwerów internetowych.

- **Zainstaluj certyfikaty główne**

  Jeżeli opcja jest włączona, certyfikaty dodane do tabeli zostaną zainstalowane na określonych urządzeniach.

  Jeśli ta opcja jest wyłączona, na określonych urządzeniach nie zostaną zainstalowane żadne certyfikaty.

  Domyślnie opcja ta jest wyłączona.

- **Dodaj**

  Kliknięcie tego przycisku powoduje otwarcie okna, w którym możesz dodać certyfikat.

Certyfikat musi mieć mniej niż 10 MB.

Kaspersky Security Center obsługuje certyfikaty z rozszerzeniami CER, CRT, CERT, PEM i KEY.

W podsekcji **Dodaj lub edytuj odpowiednie lokalne grupy administratorów** możesz zarządzać grupami administratorów lokalnych. Grupy te są wykorzystywane, na przykład, podczas wycofywania uprawnień administratora lokalnego. Możesz także sprawdzić listę kont użytkowników uprzywilejowanych, korzystając z **Raport o uprzywilejowanych użytkownikach urządzenia (tylko Linux)**.

- **Add**

  Kliknięcie tego przycisku otwiera okno, w którym możesz dodać grupę administratorów lokalnych.

- **Edit**

  Kliknięcie tego przycisku powoduje otwarcie okna, w którym możesz edytować grupę administratorów lokalnych.

  Przycisk ten jest dostępny, jeśli zaznaczone jest pole wyboru obok grupy administratorów lokalnych.

- **Delete**

  Kliknięcie tego przycisku powoduje usunięcie wybranej grupy administratorów lokalnych z tabeli.

  Przycisk ten jest dostępny, jeśli zaznaczone jest pole wyboru obok grupy administratorów lokalnych.

W podsekcji **Prześlij plik referencyjny, aby chronić plik sudoers na urządzeniu użytkownika przed zmianami**, możesz skonfigurować kontrolę nad plikiem sudoers. Grupy uprzywilejowane i użytkownicy urządzeń są definiowani w pliku sudoers na urządzeniu. Plik sudoers znajduje się w folderze `/etc/sudoers`. Możesz przesłać referencyjny plik sudoers, aby chronić plik sudoers przed zmianami. Zapobiegnie to niepożądanym zmianom w pliku sudoers.

Nieprawidłowy plik referencyjny sudoers może spowodować nieprawidłowe działanie urządzenia użytkownika.

- **Plik kontrolny sudoers**

  Jeśli ta opcja jest włączona, plik sudoers zostanie zastąpiony bieżącym plikiem referencyjnym sudoers.

  Jeśli ta opcja jest wyłączona, plik sudoers pozostanie niezmieniony.

  Domyślnie opcja ta jest wyłączona.

- **Plik referencyjny sudoers**

  W tym polu wyświetlana jest nazwa przesłanego pliku referencyjnego sudoers.

- **Prześlij**

  Kliknięcie tego przycisku powoduje otwarcie okna, w którym możesz przesłać referencyjny plik sudoers.

- **Bieżący plik referencyjny sudoers**

  Kliknięcie tego przycisku powoduje wyświetlenie zawartości bieżącego pliku sudoers.

Historia rewizji

Na tej zakładce możesz przejrzeć listę rewizji zasady i wycofać zmiany wprowadzone do zasady (jeśli to konieczne).

Porównanie ustawień zasady Agenta sieciowego według systemów operacyjnych

Poniższa tabela pokazuje, jakich ustawień zasady Agenta sieciowego możesz użyć w Konsoli administracyjnej i Kaspersky Security Center Web Console do skonfigurowania Agenta sieciowego z określonym systemem operacyjnym.

Ustawienia zasady Agenta sieciowego: porównanie według systemów operacyjnych

Sekcja Zasada	Windows	macOS	Linux
Ogólne	✓	✓	✓
Konfiguracja zdarzenia	✓	✓	✓
Ustawienia	✓	✓	✓ Dostępne są następujące opcje: • **Rozsyłaj pliki tylko poprzez punkty dystrybucji** • **Maksymalny rozmiar kolejki zdarzeń, w MB** • **Aplikacja może pobierać rozszerzone dane zasad na urządzenie**
Repozytoria	✓	✓ Dostępna jest opcja **Szczegóły rejestru sprzętu**.	✓ Dostępne są następujące opcje: • **Szczegóły zainstalowanych aplikacji** • **Szczegóły rejestru sprzętu**
Aktualizacje oprogramowania i luki	✓	—	—
Zarządzanie ponownym uruchamianiem	✓	—	—
Udostępnianie pulpitu Windows	✓	—	—
Zarządzaj poprawkami i aktualizacjami	✓	—	—
Łączność → Sieć	✓	✓	✓ Za wyjątkiem opcji **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows**.
Łączność → Profile połączenia	✓	✓	—
Łączność → Terminarz połączeń	✓	✓	✓
Przeszukiwanie sieci według punktów dystrybucji	✓ Dostępne są tylko opcje **Sieć Windows**, **Zakresy IP** oraz **Sterowniki domeny**.	—	✓ Dostępne są następujące opcje: • **Zeroconf** • **Zakresy IP** • **Sterowniki domeny**
Ustawienia sieci dla punktów dystrybucji	✓	✓	✓
KSN Proxy (punkty dystrybucji)	✓	—	✓
Aktualizacje (punkty dystrybucji)	✓	—	✓
Historia rewizji	✓	✓	✓

Włączanie i wyłączanie trybu niskiego zużycia zasobów dla Agenta sieciowego

Tryb niskiego zużycia zasobów umożliwia ograniczenie zużycia pamięci RAM przez Agenta sieciowego zainstalowanego na urządzeniu klienckim. Domyślnie tryb niskiego zużycia zasobów jest wyłączony.

W trybie niskiego zużycia zasobów nie są realizowane następujące funkcje:

- Agenta sieciowego nie można przypisać do działania jako punkt dystrybucji (ręcznie lub automatycznie).
- Agent sieciowy nie rejestruje informacji o stanie Agenta sieciowego w osobnym pliku tekstowym.
- Agent sieciowy nie obsługuje modelu pobierania aktualizacji w trybie offline.
- Następujące komponenty i procesy są wyłączone:
  - Uzyskiwanie informacji o aktualizacjach i lukach w zabezpieczeniach innych firm.
  - Uruchamianie KSN Proxy po stronie punktu dystrybucyjnego.
  - Przesyłanie aktualizacji do repozytorium punktu dystrybucji.
  - Ominięcie blokady serwera DNS.
  - Uzyskiwanie informacji o wolnej przestrzeni dyskowej.

Komponenty i procesy wznawiają działanie po wyłączeniu trybu niskiego zużycia zasobów.

Aby włączyć tryb niskiego zużycia zasobów:

1. Na urządzeniu klienckim wykonaj następujące polecenie w wierszu poleceń:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Uruchom ponownie usługę Agenta sieciowego.
3. Aby sprawdzić, czy tryb niskiego zużycia zasobów jest włączony, w systemie Windows otwórz **Podgląd zdarzeń**, a następnie wybierz **Dzienniki aplikacji i usług → Dziennik zdarzeń aplikacji Kaspersky**.

   Upewnij się, że dziennik zawiera zdarzenia takie jak to, że **Agent sieciowy Kaspersky Security Center działa w trybie niskiego zużycia zasobów**.

Tryb niskiego zużycia zasobów jest włączony.

Aby wyłączyć tryb niskiego zużycia zasobów:

1. Na urządzeniu klienckim wykonaj następujące polecenie w wierszu poleceń:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Uruchom ponownie usługę Agenta sieciowego.

3. Aby sprawdzić, czy tryb niskiego zużycia zasobów jest wyłączony, w systemie Windows otwórz **Podgląd zdarzeń**, a następnie wybierz **Dzienniki aplikacji i usług → Dziennik zdarzeń aplikacji Kaspersky**.

   Upewnij się, że ostatnie zdarzenie klnagent nie zawiera komunikatu **Agent sieciowy Kaspersky Security Center działa w trybie niskiego zużycia zasobów**.

Tryb niskiego zużycia zasobów jest wyłączony.

Tryb niskiego zużycia zasobów można także włączyć zdalnie, korzystając z zadania *Zdalne wykonywanie skryptów*.

Konfigurowanie ustawień ochrony aplikacji zarządzanych

Aby skonfigurować ustawienia ochrony aplikacji zarządzanych firmy Kaspersky, możesz użyć zasad.

Więcej informacji na temat konfigurowania zasad programu Kaspersky Endpoint Security można znaleźć w odpowiedniej pomocy:

- Pomoc Kaspersky Endpoint Security for Windows
- Pomoc Kaspersky Endpoint Security for Linux
- Pomoc dotycząca programu Kaspersky Endpoint Security for Mac

Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security

Optymalną i zalecaną opcją terminarza dla Kaspersky Endpoint Security jest **Po pobraniu nowych aktualizacji do repozytorium**, gdy zaznaczone jest pole **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Zdalne usuwanie aplikacji lub aktualizacji oprogramowania

W celu zdalnego usunięcia aplikacji lub aktualizacji oprogramowania z wybranych urządzeń:

1. W menu głównym przejdź do **Zasoby (urządzenia) → Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Zdalna dezinstalacja aplikacji**.
4. Określ nazwę tworzonego zadania.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.

6. Wybierz rodzaj oprogramowania, które chcesz usunąć, a następnie wybierz określone aplikacje, aktualizacje lub łaty, które chcesz usunąć:

   - **Odinstaluj zarządzane aplikacje**

     Zostanie wyświetlona lista aplikacji Kaspersky. Wybierz aplikację, którą chcesz usunąć.

   - **Odinstaluj niekompatybilną aplikację**

     Zostanie wyświetlona lista aplikacji niekompatybilnych z aplikacjami zabezpieczającymi firmy Kaspersky lub Kaspersky Security Center. Zaznacz pola obok aplikacji, które chcesz usunąć.

   - **Odinstaluj aplikację z rejestru aplikacji**

     Domyślnie, Agenty sieciowe wysyłają do Serwera administracyjnego informacje o aplikacjach zainstalowanych na zarządzanych urządzeniach. Lista zainstalowanych aplikacji jest przechowywana w rejestrze aplikacji.

     W celu wybrania aplikacji z rejestru aplikacji:

     a. Kliknij pole **Aplikacja do odinstalowania**, a następnie wybierz aplikację, którą chcesz usunąć.

     > Jeśli wybierzesz Agenta sieciowego Kaspersky Security Center, po uruchomieniu zadania stan *Ukończono pomyślnie* oznacza, że rozpoczął się proces usuwania. Jeśli Agent sieciowy Kaspersky Security Center zostanie usunięty, jego stan się nie zmieni. Jeśli zadanie nie powiedzie się, status zmieni się na *Niepowodzenie*.

     b. Określ opcje dezinstalacji:

     - **Tryb dezinstalacji**

       Wybierz sposób dezinstalacji aplikacji:

       - **Określ polecenie dezinstalacji automatycznie**

         Jeśli aplikacja posiada polecenie dezinstalacji zdefiniowane przez producenta aplikacji, Kaspersky Security Center użyje tego polecenia. Nie jest zalecane wybranie tej opcji.

       - **Określ polecenie dezinstalacji**

         Wybierz tę opcję, jeśli chcesz określić swoje polecenie do dezinstalacji aplikacji.

         > W pierwszej kolejności zalecane jest usunięcie aplikacji przy użyciu opcji **Określ polecenie dezinstalacji automatycznie**. Jeśli dezinstalacja za pośrednictwem automatycznie zdefiniowanego polecenia nie powiedzie się, wówczas użyj swojego polecenia.

         W polu wpisz polecenie instalacji, a następnie określ następującą opcję:

         Użyj tego polecenia do dezinstalacji, dopóki nie zostanie ono wykryte automatycznie

         Kaspersky Security Center sprawdza, czy wybrana aplikacja posiada polecenie dezinstalacji zdefiniowane przez producenta aplikacji. Jeśli polecenie zostało wykryte, Kaspersky Security Center użyje go zamiast polecenia określonego w polu **Polecenie do dezinstalacji aplikacji**.

         Nie jest zalecane włączenie tej opcji.

- **Wykonaj ponowne uruchomienie po pomyślnym odinstalowaniu aplikacji**

  Jeśli po pomyślnej dezinstalacji aplikacji wymagane jest ponowne uruchomienie systemu operacyjnego na zarządzanym urządzeniu, system operacyjny zostanie automatycznie uruchomiony ponownie.

- **Odinstaluj wybraną aktualizację aplikacji, poprawkę lub aplikację firmy trzeciej**

  Zostanie wyświetlona lista aktualizacji, łat i aplikacji innych firm. Wybierz element, który chcesz usunąć.

  Wyświetlona lista jest ogólną listą aplikacji i aktualizacji i nie odpowiada aplikacjom i aktualizacjom zainstalowanym na zarządzanych urządzeniach. Przed wybraniem elementu zalecane jest zapewnienie, że aplikacja lub aktualizacja jest zainstalowana na urządzeniu zdefiniowanym w obszarze zadania. Listę urządzeń, na których aplikacja lub aktualizacja została zainstalowana, możesz przejrzeć w oknie właściwości.

  W celu wyświetlenia listy urządzeń:

  a. Kliknij nazwę aplikacji lub aktualizacji.

     Zostanie otwarte okno właściwości.

  b. Otwórz sekcję **Urządzenia**.

     Listę zainstalowanych aplikacji i aktualizacji możesz przejrzeć także w oknie właściwości urządzenia.

7. Określ sposób, w jaki urządzenia klienckie pobiorą narzędzie do dezinstalacji:

- **Przy użyciu Agenta sieciowego**

  Pliki są dostarczane do urządzeń klienckich przez Agenta sieciowego zainstalowanego na tych urządzeniach klienckich.

  Jeśli ta opcja została wyłączona, pliki zostaną dostarczone przy użyciu narzędzi Microsoft Windows.

  Zalecane jest włączenie tej opcji, jeśli zadanie zostało przypisane do urządzeń, na których zainstalowano Agenty sieciowe.

- **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**

  Pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego Serwera administracyjnego. Możesz włączyć tę opcję, jeśli na urządzeniu klienckim nie ma zainstalowanego Agenta sieciowego, ale urządzenie klienckie jest w tej samej sieci, co Serwer administracyjny.

- **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**

  Pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego za pośrednictwem punktów dystrybucyjny. Możesz włączyć tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny.

  Jeśli opcja **Przy użyciu Agenta sieciowego** jest włączona, pliki będą dostarczane przy użyciu narzędzi systemu operacyjnego, jeśli narzędzia Agenta sieciowego będą niedostępne.

- **Maksymalna liczba jednoczesnych pobierań**

  Maksymalna dozwolona liczba urządzeń klienckich, do których Serwer administracyjny może jednocześnie przesłać pliki. Im większa ta liczba, tym szybciej aplikacja zostanie odinstalowana, ale obciążenie na Serwerze administracyjnym jest większe.

- **Maksymalna liczba prób dezinstalacji**

  Jeśli podczas wykonywania zadania *Zdalna dezinstalacja aplikacji* programowi Kaspersky Security Center nie uda się zainstalować aplikacji na zarządzanym urządzeniu w obrębie liczby uruchomień instalatora określonych przez parametr, Kaspersky Security Center zatrzyma dostarczanie narzędzia do dezinstalacji na to zarządzane urządzenie i już nie uruchomi instalatora na urządzeniu.

Parametr **Maksymalna liczba prób dezinstalacji** umożliwia zachowanie zasobów zarządzanego urządzenia, a także zmniejszyć ruch sieciowy (dezinstalacja, uruchomienie pliku MSI i wiadomości o błędach).

Powtarzające się próby uruchomienia zadania mogą wskazywać na problem na urządzeniu i uniemożliwiać przeprowadzenie dezinstalacji. Administrator powinien rozwiązać problem w określonej liczbie prób dezinstalacji, a następnie uruchomić zadanie ponownie (ręcznie lub zgodnie z terminarzem).

Jeśli dezinstalacja się nie powiedzie, problem jest uznawany za nierozwiązalny i wszelkie dalsze uruchomienia zadania są postrzegane jako niepotrzebne zużywanie zasobów i ruchu sieciowego.

Po utworzeniu zadania, licznik prób jest ustawiony na `0`. Każde uruchomienie instalatora, które zwraca błąd na urządzeniu, zwiększa wartość licznika o jeden.

Jeśli liczba prób określonych w parametrze została przekroczona, a urządzenie jest gotowe do odinstalowania aplikacji, możesz zwiększyć wartość parametru **Maksymalna liczba prób dezinstalacji** i uruchomić zadanie do odinstalowania aplikacji. W razie czego możesz utworzyć nowe zadanie *Zdalna dezinstalacja aplikacji*.

- **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**

  Przed przesłaniem plików na urządzenia klienckie program Kaspersky Security Center sprawdza, czy ustawienia narzędzia do instalacji są stosowane do systemu operacyjnego urządzenia klienckiego. Jeśli ustawienia nie są stosowane, Kaspersky Security Center nie przesyła plików i nie próbuje zainstalować aplikacji. Na przykład, aby zainstalować aplikację Windows na urządzenia grupy administracyjnej, która zawiera urządzenia działające pod kontrolą różnych systemów operacyjnych, możesz przypisać zadanie instalacji do grupy administracyjnej, a następnie włączyć tę opcję, aby pominąć urządzenia, na których jest uruchomiony system operacyjny inny niż Windows.

  Podczas zdalnej instalacji Agenta sieciowego na nieprzypisanych urządzeniach, Kaspersky Security Center lub punkt dystrybucji automatycznie ustala typ systemu operacyjnego urządzenia, niezależnie od ustawienia **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**.

- **Użyj hasła dezinstalacyjnego**

  Ten parametr jest wyświetlany, jeśli w poprzednim kroku wybrano opcję **Odinstaluj zarządzaną aplikację**, a następnie w polu **Aplikacja do odinstalowania** określono Agenta sieciowego Kaspersky Security Center.

  Jeżeli wcześniej ustawiłeś hasło do zdalnej dezinstalacji Agenta sieciowego w ustawieniach zasady Agenta sieciowego, zaznacz pole wyboru **Użyj hasła dezinstalacyjnego**, a następnie wprowadź hasło dezinstalacyjne w polu **Hasło**. Jeśli nie ustawiłeś hasła do zdalnej dezinstalacji Agenta sieciowego, nie zaznaczaj tego pola wyboru.

8. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

  Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

  Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

9. Jeśli to konieczne, dodaj konta, które będą używane do uruchamiania zadania zdalnej dezinstalacji:

- **Konto nie jest wymagane (Agent sieciowy jest zainstalowany)**

  Jeśli ta opcja jest zaznaczona, nie musisz określić konta, z poziomu którego zostanie uruchomiony instalator aplikacji. Zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

  Jeśli Agent sieciowy nie został zainstalowany na urządzeniach klienckich, ta opcja nie będzie dostępna.

- **Konto wymagane (Agent sieciowy nie jest używany)**

  Wybierz tę opcję, jeśli Agent sieciowy nie jest zainstalowany na urządzeniach, do których przypisujesz zadanie *Zdalna dezinstalacja aplikacji*. W takim przypadku możesz określić konto użytkownika lub certyfikat SSH, aby zainstalować aplikację.

  - **Konto lokalne**. Jeśli ta opcja jest zaznaczona, określ konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji. Kliknij przycisk **Dodaj**, wybierz **Konto lokalne**, a następnie określ poświadczenia konta użytkownika.

    Możesz określić wiele kont użytkowników, jeśli na przykład żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, do których przypisujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

  - **Certyfikat SSH**. Jeśli chcesz zainstalować aplikację na urządzeniu klienckim opartym na systemie Linux, możesz określić certyfikat SSH zamiast konta użytkownika. Kliknij przycisk **Dodaj**, wybierz **Certyfikat SSH**, a następnie określ klucze prywatny i publiczny certyfikatu.

    Aby wygenerować klucz prywatny, możesz użyć narzędzia ssh-keygen. Należy zauważyć, że Kaspersky Security Center obsługuje format PEM kluczy prywatnych, ale narzędzie ssh-keygen domyślnie generuje klucze SSH w formacie OPENSSH. Format OPENSSH nie jest obsługiwany przez Kaspersky Security Center. Aby utworzyć klucz prywatny w obsługiwanym formacie PEM, dodaj opcję -m PEM w poleceniu ssh-keygen.

    Na przykład:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< adres e-mail użytkownika >"
    ```

10. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

11. Kliknij przycisk **Zakończ**.

    Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

12. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

13. W oknie właściwości zadania określ ogólne ustawienia zadania.

14. Kliknij przycisk **Zapisz**.

15. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej dezinstalacji, wybrana aplikacja zostanie usunięta z wybranych urządzeń.

Problemy związane ze zdalną instalacją

Czasami podczas zdalnego usuwania aplikacji innych firm można napotkać ostrzeżenie: „Zdalna dezinstalacja została zakończona na tym urządzeniu z ostrzeżeniami: Aplikacja do usunięcia nie jest zainstalowana". Problem ten występuje, gdy aplikacja przeznaczona do odinstalowania została już odinstalowana lub została zainstalowana wyłącznie dla pojedynczego użytkownika. Aplikacje zainstalowane dla pojedynczego użytkownika (nazywane również aplikacjami dla konkretnego użytkownika) stają się niewidoczne i nie mogą być odinstalowanie zdalnie, jeśli użytkownik nie jest zalogowany.

Takie zachowanie różni się od z zachowania aplikacji przeznaczonych do użytku przez wielu użytkowników na tym samym urządzeniu (nazywanych także aplikacjami na urządzenie). Aplikacje na urządzenie są widoczne i dostępne dla wszystkich użytkowników urządzenia.

W związku z tym aplikacje dla konkretnego użytkownika należy odinstalowywać tylko wtedy, gdy użytkownik jest zalogowany.

Źródła informacji o zainstalowanych aplikacjach

Agent sieciowy pobiera informacje o oprogramowaniu zainstalowanym na urządzeniach z systemem Windows z następujących kluczy rejestru:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla wszystkich użytkowników.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla wszystkich użytkowników.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla bieżącego użytkownika.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Zawiera informacje o aplikacjach zainstalowanych dla konkretnych użytkowników.

Zadania

Ta sekcja opisuje zadania używane przez Kaspersky Security Center.

Informacje o zadaniach

Kaspersky Security Center zarządza aplikacjami zabezpieczającymi Kaspersky, zainstalowanymi na urządzeniach poprzez tworzenie i uruchamianie *zadań*. Zadania są potrzebne do instalowania, uruchamiania i zatrzymywania działania aplikacji, skanowania plików, aktualizowania baz danych i modułów aplikacji, a także wykonywania innych działań na aplikacjach.

Zadania dla określonej aplikacji można utworzyć przy użyciu Kaspersky Security Center Web Console tylko wtedy, gdy wtyczka administracyjna dla tej aplikacji jest zainstalowana na serwerze Kaspersky Security Center Web Console Server.

Zadania mogą być wykonywane na Serwerze administracyjnym i na urządzeniach.

Zadania, które są wykonywane na Serwerze administracyjnym, obejmują:

- Automatyczne rozsyłanie raportów
- Pobieranie uaktualnień do repozytorium
- Tworzenie kopii zapasowych danych Serwera administracyjnego
- Obsługa baz danych

Na urządzeniach wykonywane są następujące typy zadań:

- *Zadania lokalne*—zadania wykonywane na określonym urządzeniu

  Zadania lokalne mogą zostać zmodyfikowane przez administratora przy użyciu narzędzi Konsoli administracyjnej lub przez użytkownika zdalnego urządzenia (na przykład, z poziomu interfejsu aplikacji zabezpieczającej). Jeśli zadanie lokalne zostało zmodyfikowane jednocześnie przez administratora i użytkownika zarządzanego urządzenia, zostaną zastosowane zmiany wprowadzone przez administratora, ponieważ mają wyższy priorytet.

- *Zadania grupowe*—zadania wykonywane na wszystkich urządzeniach określonej grupy

  Dopóki nie określono inaczej we właściwościach zadania, zadanie grupowe także wpływa na wszystkie podgrupy wybranej grupy. Zadanie grupowe także może wpływać (opcjonalnie) na urządzenia, które zostały podłączone do podrzędnych i wirtualnych Serwerów administracyjnych zainstalowanych w grupie lub w jej dowolnej podgrupie.

- *Zadania globalne*—zadania wykonywane na zbiorze urządzeń, niezależnie od tego, czy znajdują się w jakiejkolwiek grupie.

Dla każdej aplikacji można utworzyć dowolną liczbę zadań grupowych, zadań globalnych lub zadań lokalnych.

Możesz wprowadzać zmiany w ustawieniach zadań, przeglądać postęp ich wykonywania, a także kopiować, eksportować, importować i usuwać zadania.

Zadanie jest uruchamiane na urządzeniu tylko wtedy, gdy uruchomiona jest aplikacja, dla której utworzono zadanie.

Wyniki wykonania zadań są zapisywane w dzienniku zdarzeń systemu operacyjnego na każdym urządzeniu, w dzienniku zdarzeń systemu operacyjnego na Serwerze administracyjnym, a także w bazie danych Serwera administracyjnego.

Nie używaj prywatnych danych w ustawieniach zadania. Na przykład, unikaj określania hasła administratora domeny.

Informacje o obszarze zadania

Obszar zadania to zestaw urządzeń, na których wykonywane jest zadanie. Typy obszaru to:

- Dla *zadania lokalnego* obszarem jest samo urządzenie.
- Dla *zadania Serwera administracyjnego* obszarem jest Serwer administracyjny.
- Dla *zadania grupowego* obszarem jest lista urządzeń znajdujących się w grupie.

Podczas tworzenia *zadania globalnego* możesz użyć następujących metod do określenia jego obszaru:

- Ręcznie określ pewne urządzenia.

  Jako adresu urządzenia możesz użyć adresu IP (lub zakresu adresów IP), nazwy NetBIOS lub nazwy DNS.

- Zaimportuj listę urządzeń z pliku TXT zawierającego adresy dodawanych urządzeń (każdy adres powinien znajdować się w pojedynczej linii).

  Jeśli lista urządzeń jest importowana z pliku lub jest tworzona ręcznie, a urządzenia są identyfikowane po nazwie, lista może zawierać tylko urządzenia, o których informacje zostały już dodane do bazy danych Serwera administracyjnego. Co więcej, informacje musiały zostać wprowadzone, gdy te urządzenia były podłączone lub podczas wyszukiwania urządzeń.

- Utwórz wybór urządzeń.

  Obszar zadania zmienia się, gdy zmienia się zbiór urządzeń zawartych w wyborze. Wybór urządzeń można utworzyć w oparciu o atrybuty urządzeń, włączając w to oprogramowanie zainstalowane na urządzeniach, a także w oparciu o znaczniki przydzielone do urządzeń. Wybór urządzeń to najbardziej elastyczny sposób określania obszaru zadania.

  Zadania dla wyborów urządzeń są zawsze uruchamiane przez Serwer administracyjny zgodnie z terminarzem. Te zadania nie mogą zostać uruchomione na urządzeniach, które nie są połączone z Serwerem administracyjnym. Zadania, których obszar jest określony przy użyciu innych metod, są uruchamiane bezpośrednio na urządzeniach i dlatego nie zależą od połączenia urządzenia z Serwerem administracyjnym.

Zadania dla wyborów urządzeń nie są uruchamiane zgodnie z czasem lokalnym urządzenia tylko z czasem lokalnym Serwera administracyjnego. Zadania, których obszar jest określony przy użyciu innych metod, są uruchamiane zgodnie z czasem lokalnym urządzenia.

Tworzenie zadania

W celu utworzenia zadania:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z jego instrukcjami.
3. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
4. Kliknij przycisk **Zakończ**.

Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

Aby utworzyć nowe zadanie przypisane do wybranych urządzeń:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.
2. Aby uruchomić zadanie dla danych urządzeń, zaznacz znajdujące się obok nich pola wyboru na liście zarządzanych urządzeń. Aby znaleźć urządzenia, których szukasz, możesz skorzystać z funkcji wyszukiwania i filtrowania.

3. Kliknij przycisk **Uruchom zadanie**, a następnie wybierz opcję **Dodaj nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.

   W pierwszym kroku kreatora możesz usunąć wybrane urządzenia, które chcesz uwzględnić w zakresie zadania. Postępuj zgodnie z instrukcjami kreatora.

4. Kliknij przycisk **Zakończ**.

Zadanie zostanie utworzone dla wybranych urządzeń.

Ręczne uruchamianie zadania

Aplikacja jest uruchamiana zgodnie z ustawieniami terminarza, określonymi we właściwościach każdego zadania. Możesz ręcznie uruchomić zadanie w dowolnym momencie poziomu listy zadań. Alternatywnie możesz wybrać urządzenia na liście **Zarządzane urządzenia**, a następnie rozpocząć dla nich istniejące zadanie.

W celu ręcznego uruchomienia zadania:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.

2. Na liście zadań zaznacz pole obok zadania, które chcesz uruchomić.

3. Kliknij przycisk **Uruchom**.

Zadanie zostanie uruchomione. Możesz sprawdzić stan zadania w kolumnie **Stan** lub klikając przycisk **Wynik**.

Przeglądanie listy zadań

Możesz przejrzeć listę zadań, które zostały utworzone w Kaspersky Security Center.

W celu przejrzenia listy zadań,

W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.

Zostanie wyświetlona lista zadań. Zadania są grupowane według nazw aplikacji, których dotyczą. Na przykład, zadanie *Zdalna dezinstalacja aplikacji* dotyczy Serwera administracyjnego, a zadanie *Wyszukiwanie luk i wymaganych aktualizacji* odnosi się do Agenta sieciowego.

W celu przejrzenia właściwości zadania:

Kliknij nazwę zadania.

Okno właściwości zadania zostanie wyświetlone z kilkoma nazwanymi zakładkami. Na przykład, **Typ zadania** jest wyświetlany na zakładce **Ogólne**, a terminarz zadania na zakładce **Terminarz**.

Ogólne ustawienia zadania

Ta sekcja zawiera ustawienia, które możesz przeglądać i konfigurować dla większości swoich zadań. Lista dostępnych ustawień zależy od konfigurowanego zadania.

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- Ustawienia ponownego uruchamiania systemu operacyjnego:

  - **Nie uruchamiaj ponownie urządzenia**

    Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

  - **Uruchom urządzenie ponownie**

    Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

  - **Pytaj użytkownika o akcję**

    Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

    Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

  - **Uruchom ponownie po (min)**

    Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

    Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

- Ustawienia terminarza zadania:

  Rodzaje harmonogramów mogą się różnić w zależności od zadania.

  - **Ustawienie Uruchom zadanie:**

    - **Co N godzin**

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

      Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

    - **Co N dni**

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

      Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

    - **Co N minut**

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

      Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

    - **Według dni tygodnia**

      Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

      Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

    - **Co miesiąc**

      Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

      W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

      Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

    - **Ręcznie**

      Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

Domyślnie opcja ta jest zaznaczona.

- **Raz**

  Zadanie zostanie uruchomione raz, w określonym dniu i o określonej godzinie (domyślnie w dniu utworzenia zadania).

- **Natychmiast**

  Zadanie uruchamia się natychmiast po zapisaniu ustawień.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po pobraniu nowych aktualizacji do repozytorium**

  Zadanie jest uruchamiane po pobraniu uaktualnień do repozytorium. Na przykład, możesz użyć tego terminarza dla zadania wyszukiwania luk i wymaganych aktualizacji.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

- Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
- Kliknij ikonę sortowania, aby posortować zadania według nazwy.

  Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
- Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj automatycznego losowego opóźnienia dla zadań uruchamianych w przedziale**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

- Urządzenia, do których zadanie zostanie przypisane:

  - **Wybierz urządzenia sieciowe wykryte przez Serwer administracyjny**

    Zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

    Na przykład, możesz chcieć użyć tej opcji w zadaniu instalowania Agenta sieciowego na nieprzypisanych urządzeniach.

- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

  Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

  Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

- **Przypisz zadanie do wyboru urządzeń**

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

- **Przypisz zadanie do grupy administracyjnej**

  Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

  Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

- Ustawienia konta:

  - **Konto domyślne**

    Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

    Domyślnie opcja ta jest zaznaczona.

  - **Określ konto**

    Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

  - **Konto**

    Konto, z poziomu którego zadanie jest uruchamiane.

  - **Hasło**

    Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

Ustawienia określone po utworzeniu zadania

Następujące ustawienia możesz określić tylko po utworzeniu zadania.

- Ustawienia zadań grupowych:

  - **Roześlij do podgrup**

    Ta opcja jest dostępna tylko w ustawieniach zadań grupowych.

Kiedy ta opcja jest włączona, zakres zadania obejmuje:

- Grupa administracyjna, którą wybrano podczas tworzenia zadania.
- Grupy administracyjne podporządkowane wybranej grupie administracyjnej na dowolnym poziomie niżej w hierarchii grup.

Gdy ta opcja jest wyłączona, zakres zadania obejmuje tylko grupę administracyjną wybraną podczas tworzenia zadania.

Domyślnie opcja ta jest włączona.

- **Wyślij do podrzędnych i wirtualnych Serwerów administracyjnych**

  Gdy ta opcja jest włączona, zadanie działające na głównym serwerze administracyjnym jest również stosowane na drugorzędnych serwerach administracyjnych (w tym wirtualnych). Jeżeli zadanie tego samego typu już istnieje na drugorzędnym serwerze administracyjnym, oba zadania są stosowane na drugorzędnym serwerze administracyjnym — istniejące i odziedziczone z głównego serwera administracyjnego.

  Ta opcja jest dostępna tylko wtedy, gdy włączona jest opcja **Roześlij do podgrup**.

  Domyślnie opcja ta jest wyłączona.

- Zaawansowane ustawienia terminarza:

  - **Włącz urządzenia przed uruchomieniem zadania przy użyciu funkcji Wake-on-LAN**

    System operacyjny na urządzeniu zostanie uruchomiony o określonym czasie przed uruchomieniem zadania. Domyślnie czas ten wynosi pięć minut.

    Włącz tę opcję, jeśli chcesz, aby zadanie było uruchamiane na wszystkich urządzeniach klienckich z obszaru zadania, w tym tych urządzeniach, które są wyłączone, gdy zadanie ma zostać uruchomione.

    Jeśli chcesz, żeby urządzenie było automatycznie wyłączane po zakończeniu zadania, włącz opcję **Wyłącz urządzenia po zakończeniu zadania**. Ta opcja znajduje się w tym samym oknie.

    Domyślnie opcja ta jest wyłączona.

  - **Wyłącz urządzenia po zakończeniu zadania**

    Na przykład, możesz chcieć włączyć tę opcję dla zadania instalacji aktualizacji, które instaluje uaktualnienia na urządzeniach klienckich w każdy piątek w godzinach pracy, a następnie wyłącza te urządzenia w weekend.

    Domyślnie opcja ta jest wyłączona.

  - **Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż**

    Po minięciu określonego czasu, zadanie jest zatrzymywane automatycznie, niezależnie od tego, czy zostało zakończone.

    Włącz tę opcję, jeśli chcesz przerwać (lub zatrzymać) zadania, których wykonanie zajmuje zbyt dużo czasu.

    Domyślnie opcja ta jest wyłączona. Domyślny czas wykonania zadania to 120 minut.

- Ustawienia powiadomień:
  - Sekcja **Przechowywanie historii zadania**:
    - **Przechowuj w bazie danych Serwera administracyjnego przez (dni)**

      Zdarzenia aplikacji związane z wykonaniem zadania na wszystkich urządzeniach klienckich z obszaru zadania są przechowywane na Serwerze administracyjnym przez określoną liczbę dni. Po upłynięciu tego okresu, informacje są usuwane z Serwera administracyjnego.

      Domyślnie opcja ta jest włączona.

    - **Przechowuj w systemowym dzienniku zdarzeń urządzenia**

      Zdarzenia aplikacji związane z wykonaniem zadania są przechowywane lokalnie w dzienniku zdarzeń systemu Windows każdego urządzenia klienckiego.

      Domyślnie opcja ta jest wyłączona.

    - **Przechowuj w systemowym dzienniku zdarzeń Serwera administracyjnego**

      Zdarzenia aplikacji związane z wykonaniem zadania na wszystkich urządzeniach klienckich z obszaru zadania są przechowywane w sposób scentralizowany w dzienniku zdarzeń Windows systemu operacyjnego Serwera administracyjnego.

      Domyślnie opcja ta jest wyłączona.

    - **Zapisz wszystkie zdarzenia**

      Jeśli ta opcja jest zaznaczona, wszystkie zdarzenia dotyczące zadania zostaną zapisane w dziennikach zdarzeń.

    - **Zapisz zdarzenia dotyczące postępu zadania**

      Jeśli ta opcja jest zaznaczona, tylko zdarzenia dotyczące wykonania zadania zostaną zapisane w dziennikach zdarzeń.

    - **Zapisz jedynie wyniki wykonywania zadania**

      Jeśli ta opcja jest zaznaczona, tylko zdarzenia dotyczące wyników zadania zostaną zapisane w dziennikach zdarzeń.

  - **Powiadom administratora o wynikach wykonywania zadania**

    Możesz wybrać metody, przy użyciu których administratorzy otrzymają powiadomienia o wynikach wykonania zadań: za pośrednictwem poczty elektronicznej, przez SMS oraz poprzez uruchomienie pliku wykonywalnego. Aby skonfigurować powiadomienie, kliknij odnośnik **Ustawienia**.

    Domyślnie, wszystkie metody powiadamiania są wyłączone.

  - **Powiadom tylko o błędach**

    Jeśli ta opcja jest włączona, administratorzy są powiadamiani tylko wtedy, gdy wykonanie zadania zakończy się błędem.

    Jeśli ta opcja jest wyłączona, administratorzy są powiadamiania po każdym zakończeniu wykonywania zadania.

Domyślnie opcja ta jest włączona.

- Ustawienia zabezpieczeń.
- Ustawienia obszaru zadania.

  W zależności od sposobu określenia obszaru zadania, dostępne są następujące ustawienia:

  - **Urządzenia**

    Jeśli obszar zadania jest określany przez grupę administracyjną, możesz przejrzeć tę grupę. Nie ma tutaj dostępnych zmian. Jednakże możesz ustawić **Wykluczenia z zakresu zadania**.

    Jeśli obszar zadania jest określany przez listę urządzeń, możesz zmodyfikować tę listę poprzez dodanie i usunięcie urządzeń.

  - **Wybór urządzeń**

    Możesz zmienić wybór urządzeń, do którego zadanie jest stosowane.

  - **Wykluczenia z zakresu zadania**

    Możesz określić grupę urządzeń, do których zadanie nie jest stosowane. Grupy, które mają zostać wykluczone, mogą być tylko podgrupami grupami administracyjnej, do której zadanie jest stosowane.

- **Historia rewizji**.

Eksportowanie zadania

Kaspersky Security Center umożliwia zapisanie zadania i jego ustawień w pliku KLT. Możesz użyć tego pliku KLT do zaimportowania zapisanego zadania zarówno do Kaspersky Security Center Windows, jak i Kaspersky Security Center Linux.

W celu wyeksportowania zadania:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Zaznacz pole obok zadania, które chcesz wyeliminować.

   Nie można jednocześnie eksportować wielu zadań. Jeśli wybierzesz więcej niż jedno zadanie, przycisk **Eksportuj** będzie nieaktywny. Zadania Serwera administracyjnego są również niedostępne do eksportu.
3. Kliknij przycisk **Eksportuj**.
4. W otwartym oknie **Zapisz jako** określ nazwę i ścieżkę pliku zadania. Kliknij przycisk **Zapisz**.

   Okno **Zapisz jako** jest wyświetlane tylko wtedy, gdy korzystasz z przeglądarki Google Chrome, Microsoft Edge lub Opera. Jeśli używasz innej przeglądarki, plik zadania jest automatycznie zapisywany w folderze **Pobrane**.

Importowanie zadania

Kaspersky Security Center umożliwia import zadania z pliku KLT. Plik KLT zawiera wyeksportowane zadanie i jego ustawienia.

W celu zaimportowania zadania:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij przycisk **Importuj**.
3. Kliknij przycisk **Przeglądaj**, aby wybrać plik zadania, który chcesz zaimportować.
4. W otwartym oknie określ ścieżkę do pliku zadania KLT, a następnie kliknij przycisk **Otwórz**. Pamiętaj, że możesz wybrać tylko jeden plik zadania.

   Zadanie zostanie uruchomione.
5. Po pomyślnym przetworzeniu zadania wybierz urządzenia, do których chcesz przypisać zadanie. W tym celu wykonaj jedną z następujących czynności:

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

     Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

   - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

     Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

     Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

   - **Przypisz zadanie do wyboru urządzeń**

     Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.
6. Wybierz obszar zadania.
7. Kliknij przycisk **Zakończone**, aby zakończyć import zadania.

Pojawi się powiadomienie z wynikami importu. Jeśli zadanie zostało pomyślnie zaimportowane, możesz kliknąć łącze **Szczegóły**, aby wyświetlić właściwości zadania.

Po pomyślnym imporcie zadanie zostanie wyświetlone na liście zadań. Importowane są również ustawienia zadania i harmonogram. Zadanie zostanie uruchomione zgodnie z harmonogramem.

Jeśli nowo importowane zadanie ma identyczną nazwę jak istniejące zadanie, nazwa importowanego zadania jest rozszerzana o indeks **(<następny numer porządkowy>)**, na przykład: **(1)**, **(2)**.

Uruchamianie kreatora zmiany haseł w zadaniach

Dla zadania, które nie jest lokalne, możesz określić konto, z poziomu którego zadanie musi być uruchomione. Konto może zostać określone podczas tworzenia zadania lub we właściwościach istniejącego zadania. Jeśli określone konto jest używane zgodnie z instrukcjami bezpieczeństwa organizacji, te instrukcje mogą wymagać zmiany hasła do konta od czasu do czasu. Jeśli hasło do konta wygaśnie i ustawisz nowe, nie powiedzie się uruchomienie zadań, aż do momentu, gdy określisz nowe ważne hasło we właściwościach zadania.

Kreator zmiany haseł w zadaniach umożliwia automatyczne zastąpienie starego hasła nowym we wszystkich zadaniach, w których konto jest określone. Alternatywnie, możesz ręcznie zmienić to hasło we właściwościach każdego zadania.

W celu uruchomienia kreatora zmiany haseł w zadaniach:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Zarządzaj poświadczeniami kont do uruchamiania zadań**.

Postępuj zgodnie z instrukcjami kreatora.

Krok 1. Określanie danych uwierzytelniających

Określ nowe dane uwierzytelniające, które aktualnie są ważne w Twoim systemie (na przykład, w Active Directory). Jeśli przejdziesz do następnego kroku kreatora, Kaspersky Security Center sprawdzi, czy nazwa określonego konta odpowiada nazwie konta we właściwościach każdego zadania, które nie jest lokalne. Jeśli nazwy kont pasują do siebie, hasło we właściwościach zadania zostanie automatycznie zastąpione nowym.

W celu określenia nowego konta, wybierz opcję:

- **Użyj bieżącego konta**

  Kreator używa nazwy konta, na którym aktualnie zalogowano się do Kaspersky Security Center Web Console. Następnie ręcznie podaj hasło do konta w polu **Aktualne hasło do użycia w zadaniach**.

- **Określ inne konto**

  Określ nazwę konta, z poziomu którego zadania muszą być uruchamiane. Następnie określ hasło do konta w polu **Aktualne hasło do użycia w zadaniach**.

Jeśli uzupełnisz pole **Poprzednie hasło (opcjonalnie; jeśli chcesz zastąpić je obecnym)**, Kaspersky Security Center zastępuje hasło tylko dla tych zadań, w których zostanie wykryta nazwa konta oraz stare hasło. Zastępowanie odbywa się automatycznie. We wszystkich pozostałych przypadkach musisz wybrać działanie, jakie ma zostać podjęte w kolejnym kroku kreatora.

Krok 2. Wybieranie działania, jakie ma zostać podjęte

Jeśli nie określiłeś poprzedniego hasła w pierwszym kroku kreatora lub jeśli stare hasło nie odpowiada hasłom we właściwościach zadań, powinieneś wybrać działanie, jakie ma zostać wykonane na wykrytych zadaniach.

W celu wybrania akcji dla zadania:

1. Zaznacz pole obok zadania, dla której chcesz wybrać działanie.
2. Wykonaj jedną z następujących czynności:
   - Aby usunąć hasło we właściwościach zadania, kliknij **Usuń poświadczenia**.

     Zadanie zostanie przełączone do działania na koncie domyślnym.
   - Aby zastąpić hasło nowym, kliknij **Wymuszaj zmianę hasła, nawet jeśli stare hasło jest niepoprawne lub nie zostało podane**.
   - Aby anulować zmianę hasła, kliknij **Nie wybrano akcji**.

Wybrane akcje zostaną zastosowane po przejściu do następnego kroku kreatora.

Krok 3. Sprawdzanie wyników

W ostatnim kroku kreatora przejrzyj wyniki dla każdego wykrytego zadania. Aby zakończyć działanie kreatora, kliknij przycisk **Zakończ**.

Tworzenie zadania zdalnego wykonywania skryptów

Możesz utworzyć zadanie *Zdalne wykonywanie skryptów* aby wykonać pakiet instalacyjny na urządzeniu klienckim i zdalnie zainstalować aplikację.

Pakiet instalacyjny zawiera archiwum ZIP z zestawem skryptów do wykonania na urządzeniach klienckich oraz plik manifest.json. Więcej informacji na temat tworzenia tego typu pakietu instalacyjnego znajdziesz w tym artykule.

To zadanie należy uruchomić tylko na urządzeniach z Agentem sieciowym dla systemu Linux.

Aby uruchomić zadanie Zdalne wykonywanie skryptów:

1. Przejdź do **Kreator tworzenia nowego zadania** i wybierz typ zadania **Zdalne wykonywanie skryptów**.
2. Wpisz nazwę zadania i wybierz urządzenia, do których zostanie przypisane zadanie. Kliknij przycisk **Dalej**.
3. Wybierz pakiet instalacyjny oparty na archiwum ZIP z plikiem manifest.json do zdalnego wykonania.

   Jeśli nie chcesz ponownie uruchamiać zadania na urządzeniach, na których zostało już zakończone, włącz opcję **Nie uruchamiaj tego zadania na urządzeniach, na których zostało ono już ukończone**.
4. Wybierz konto, aby uruchomić zadanie.

   Jeżeli wybierzesz konto domyślne, zadanie wykona Agent sieciowy (konto root).

   Po uruchomieniu zadania *Zdalne wykonywanie skryptów* nie można zmienić konta, do którego jest ono przypisane. Aby zmienić konto, do którego przypisane jest zadanie, zatrzymaj zadanie w ustawieniach zadania i utwórz je ponownie z prawidłowymi szczegółami konta.

5. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

6. Kliknij przycisk **Zakończ**.

   Zadanie *Zdalne wykonywanie skryptów* zostanie utworzone i będzie wyświetlane na liście zadań.

Po odebraniu danych z zadania *Zdalne wykonywanie skryptów* Agent sieciowy ogranicza dostęp do otrzymanych danych wszystkim użytkownikom z wyjątkiem administratora i użytkownika określonego w ustawieniach zadania.

Zdalne instalowanie aplikacji na urządzeniach za pomocą zadania Zdalne wykonywanie skryptów

Zadanie *Zdalne wykonywanie skryptów* umożliwia zdalną instalację aplikacji na urządzeniu klienckim poprzez utworzenie niestandardowego pakietu instalacyjnego.

Z tego artykułu dowiesz się, jak przygotować archiwum do tego zadania.

Aby utworzyć pakiet instalacyjny do zdalnej instalacji aplikacji na urządzeniu klienckim, w archiwum, które chcesz załadować w ramach tego zadania, muszą znajdować się następujące pliki:

- `<nazwa pakietu>.deb`
- **install.sh**

  ```
  sudo apt-get install <nazwa pakietu>.deb
  ```

- **manifest.json**

  Schemat JSON do zdalnej instalacji aplikacji

  ```
  {
    "version": 1,
    "actions": [
      {
        "type": "execute",
        "path": "install.sh",
        "args": "<wprowadź argumenty w razie konieczności>",
        "results": [
          {
            "code": 0,
            "next": "continue"
          }
        ],
        "default_next": "break"
      }
    ]
  }
  ```

Opis tablic

1. `version`—wersja pliku manifestu i zadania.

   Obecnie jedyną akceptowalną wartością jest 1.

2. Elementy tablicy `actions` określają skład i kolejność skryptów wykonywanych w zadaniu.

   Kolejność wykonywania skryptu odpowiada indeksowi (miejscu) elementu w tablicy.

3. Dla każdego elementu tablicy `actions` definiowane są następujące elementy.

   a. `type`—typ wykonywalnego polecenia ze skryptów. Obecnie wartość jest zawsze `execute`.

   b. `path`—ścieżka do pliku skryptu w archiwum.

   c. `args`—argumenty przekazywane do skryptu jako część wykonywalnego polecenia.

   d. `results`—tablica określająca dalsze działania w zależności od wyniku zadania.

      1. `code`—wartość zwracająca skrypt.

      2. `next`—czynność do wykonania w następnej kolejności. Akcja `continue` powoduje wykonanie następnego skryptu (element w tablicy `actions`); akcja `break` zatrzymuje zadanie.

   e. `default_next`—akcja, jeśli skrypt zwróci wartość, która nie jest zawarta w `results`.

Po uruchomieniu zadania *Zdalne wykonywanie skryptów* Agent sieciowy prześle pakiet instalacyjny z aplikacją na urządzenie klienckie. Gdy urządzenie klienckie odbierze pakiet instalacyjny, Agent sieciowy na tym urządzeniu analizuje plik manifest.json i w zależności od wyniku określa kolejność wykonywania skryptów i akcji, a następnie rozpoczyna wykonywanie.

Po zakończeniu zadania *Zdalne wykonywanie skryptów* aplikacja zostanie zainstalowana na urządzeniu klienckim.

Konfigurowanie powiadomień i monitorowania dla zadania Zdalne wykonywanie skryptów

Możesz skonfigurować monitorowanie, zachowanie zapisywania zdarzeń i powiadomienia dla zadania *Zdalne wykonywanie skryptów*.

Aby Zdalne wykonywanie skryptów:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.

   Zostanie wyświetlona lista zadań.

2. Wybierz zadanie i kliknij **Historia urządzenia**.

   Wyświetlany jest postęp zadania.

Aby skonfigurować zachowanie zapisywania zdarzeń:

1. Na liście zadań kliknij zadanie i przejdź do zakładki **Ustawienia**.

2. W sekcji **Powiadomienia** kliknij przycisk **Ustawienia**.

3. Wybierz jedną z poniższych opcji zachowania aplikacji po zakończeniu zadania:

   - **Zapisz wszystkie zdarzenia**.
   - **Zapisz zdarzenia dotyczące postępu zadania**.
   - **Zapisz jedynie wyniki wykonywania zadania**.

     Zdarzenia zapisywane są w **Historia urządzenia** i **Repozytorium zdarzeń**.

     Domyślnie zapisywane są tylko wyniki wykonania zadania.

     > Jeśli wybierzesz opcję **Zapisz wszystkie zdarzenia**, zapisane zostaną jedynie wyniki wykonania zadania.

4. Jeśli chcesz zapisywać zdarzenia w bazie danych Serwera administracyjnego, w dzienniku zdarzeń na Serwerze administracyjnym lub na urządzeniu, włącz odpowiednią opcję.

Więcej o konfigurowaniu powiadomień dowiesz się z tego artykułu.

Przygotowanie archiwum dla zadania Zdalne wykonywanie skryptów

Archiwum dla zadania *Zdalne wykonywanie skryptów* w oparciu o plik manifest.json musi spełniać następujące wymagania:

- Format archiwum: ZIP.
- Całkowity rozmiar: nie więcej niż 1 GB.
- Liczba plików i folderów w archiwum jest nieograniczona.
- Plik manifestu archiwum musi być zgodny ze schematem poniżej i mieć nazwę manifest.json. Schemat jest sprawdzany tylko podczas wykonywania zadania na urządzeniu.

  Schemat JSON pliku manifestu i opis macierzy

  Schemat JSON

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
```

```
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Przykład pliku manifestu

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
```

```
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- Archiwum musi mieć następującą strukturę:

  `manifest.json`

  `<file1>`

  `<file2>`

  `<folder1>/<file3>`

  `<folder2>/<folder3>/<file4>`

  `...`

  `<fileX>`

  manifest.json to plik manifestu zadania.

  `<file1>, ...., <fileX>` to zestaw plików ze skryptami do wykonania.

Tworzenie pakietu instalacyjnego na podstawie pliku manifestu

Aby utworzyć pakiet instalacyjny na podstawie pliku manifestu:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym przejdź do **Wykrywanie i wdrażanie → Wdrażanie i przypisywanie → Pakiety instalacyjne**.
   - W menu głównym przejdź do **Operacje → Repozytoria → Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Wybierz opcję **Utwórz pakiet instalacyjny dla zadania Zdalne wykonanie skryptu na podstawie archiwum ZIP z plikiem manifest.json**.

4. Podaj nazwę pakietu i kliknij przycisk **Przeglądaj**.

   Zostanie otwarte standardowe okno Windows **Otwórz** w przeglądarce, abyś mógł wybrać plik do utworzenia pakietu instalacyjnego.

5. Wybierz plik archiwum znajdujący się na dostępnych dyskach. Z tego artykułu dowiesz się, jak przygotować archiwum do tego zadania.

   Rozpocznie się przesyłanie pliku na Serwer administracyjny Kaspersky Security Center.

   Zostanie uruchomiony proces tworzenia pakietu instalacyjnego.

   Kreator informuje, gdy proces zostanie zakończony.

   Jeśli pakiet instalacyjny nie zostanie utworzony, zostanie wyświetlona odpowiednia wiadomość.

6. W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

Pakiet instalacyjny, który utworzyłeś, zostanie pobrany do podfolderu Packages folderu współdzielonego Serwera administracyjnego. Po pobraniu, pakiet instalacyjny pojawi się na liście pakietów instalacyjnych.

Na liście pakietów instalacyjnych dostępnych na Serwerze administracyjnym możesz kliknąć odnośnik z nazwą niestandardowego pakietu instalacyjnego:

- Wyświetl następujące właściwości pakietu instalacyjnego:
  - **Nazwa.** Nazwa niestandardowego pakietu instalacyjnego.
  - **Źródło.** Nazwa producenta aplikacji.
  - **Wersja.** Wersja aplikacji.
  - **Utworzono.** Data utworzenia pakietu instalacyjnego.
  - **Zmodyfikowano.** Data modyfikacji pakietu instalacyjnego.
  - **Ścieżka dostępu.** Ścieżka do niestandardowego pakietu instalacyjnego na Serwerze administracyjnym.
- Zmień nazwę pakietu instalacyjnego i parametry wiersza poleceń. Ta funkcja jest dostępna tylko dla pakietów, które nie są tworzone na podstawie aplikacji Kaspersky.

Zarządzanie urządzeniami klienckimi

Kaspersky Security Center umożliwia zarządzanie urządzeniami klienckimi:

- Przeglądaj ustawienia i stany zarządzanych urządzeń, w tym klastrów i macierzy serwerów.
- Konfiguruj punkty dystrybucji.
- Zarządzaj zadaniami.

Za pomocą grup administracyjnych można łączyć urządzenia klienckie w zestaw, którym można zarządzać jak pojedynczą jednostką. Urządzenie klienckie może należeć tylko do jednej grupy administracyjnej. Urządzenia mogą być automatycznie przydzielane do grupy na podstawie **Warunki reguły**:

- Tworzenie reguł przenoszenia urządzeń.
- Kopiowanie reguł przenoszenia urządzeń.
- Warunki dla reguły przenoszenia urządzeń.

Możesz użyć opcji wyboru urządzeń, aby filtrować urządzenia na podstawie określonego warunku. Można również oznaczać urządzenia znacznikami w celu tworzenia selekcji, wyszukiwania urządzeń i przydzielania urządzeń grupom administracyjnym.

Ustawienia zarządzanego urządzenia

W celu sprawdzenia ustawień zarządzanego urządzenia:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń, kliknij odnośnik z nazwą żądanego urządzenia.

Zostanie wyświetlone okno właściwości wybranego urządzenia.

W górnej części okna właściwości wyświetlane są następujące zakładki reprezentujące główne grupy ustawień:

- **Ogólne**

  Ta zakładka zawiera następujące sekcje:

  - Sekcja **Ogólne** wyświetla ogólne informacje o urządzeniu klienckim. Informacje są dostarczane w oparciu o dane otrzymane podczas ostatniej synchronizacji urządzenia klienckiego z Serwerem administracyjnym:

    - **Nazwa**

      W tym polu możesz wyświetlić i zmodyfikować nazwę urządzenia klienckiego w grupie administracyjnej.

    - **Opis**

      W tym polu możesz wprowadzić dodatkowy opis urządzenia klienckiego.

    - **Stan urządzenia**

      Stan urządzenia klienckiego przypisany w oparciu o kryteria zdefiniowane przez administratora dla stanu ochrony antywirusowej na urządzeniu i aktywności urządzenia w sieci.

    - **Pełna nazwa grupy**

      Grupa administracyjna zawierająca urządzenie klienckie.

    - **Ostatnia aktualizacja antywirusowych baz danych**

      Data ostatniej aktualizacji antywirusowych baz danych lub aplikacji na urządzeniu.

    - **Połączono z Serwerem administracyjnym**

Data i godzina ostatniego połączenia Agenta sieciowego, zainstalowanego na urządzeniu klienckim, z Serwerem administracyjnym.

- **Ostatnio dostępny**

  Data i godzina, gdy urządzenie było ostatnio widoczne w sieci.

- **Wersja Agenta sieciowego**

  Wersja zainstalowanego Agenta sieciowego.

- **Utworzono**

  Data utworzenia urządzenia w Kaspersky Security Center.

- **Właściciel urządzenia**

  Nazwa właściciela urządzenia. Możesz przypisać lub usunąć użytkownika jako właściciela urządzenia, klikając łącze **Zarządzaj właścicielem urządzenia**.

- **Nie odłączaj od Serwera administracyjnego**

  Jeśli ta opcja jest włączona, utrzymywana jest ciągła łączność pomiędzy zarządzanym urządzeniem a Serwerem administracyjnym. Możesz użyć tej opcji, jeśli nie używasz serwerów push, które zapewniają taką łączność.

  Jeśli ta opcja jest wyłączona, a serwery push nie są używane, zarządzane urządzenie będzie nawiązywało połączenie z Serwerem administracyjnym jedynie w celu synchronizacji danych lub przesłania informacji.

  Maksymalna całkowita liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego** to 300.

  Ta opcja jest wyłączona domyślnie na zarządzanych urządzeniach. Ta opcja jest włączona domyślnie na urządzeniu, na którym jest zainstalowany Serwer administracyjny i pozostaje włączona nawet w przypadku próby jej wyłączenia.

- Sekcja **Sieć** wyświetla następujące informacje o właściwościach sieci urządzenia klienckiego:

  - **Adres IP**

    Adres IP urządzenia.

  - **Domena Windows**

    Domena lub grupa robocza Windows, która zawiera urządzenie.

  - **Nazwa DNS**

    Nazwa domeny DNS urządzenia klienckiego.

  - **Nazwa NetBIOS**

    Nazwa urządzenia klienckiego w sieci Windows.

  - **Adres IPv6**

- Sekcja **System** zawiera informacje o systemie operacyjnym zainstalowanym na urządzeniu klienckim:
  - **System operacyjny**
  - **Architektura procesora**
  - **Nazwa urządzenia**
  - **Typ maszyny wirtualnej**

    Producent maszyny wirtualnej.
  - **Dynamiczna maszyna wirtualna jako część VDI**

    Ten wiersz pokazuje, czy urządzenie klienckie jest dynamiczną maszyną wirtualną w ramach VDI.
- Sekcja **Ochrona** zawiera informacje o bieżącym stanie ochrony antywirusowej na urządzeniu klienckim:
  - **Widoczny**

    Stan widoczności urządzenia klienckiego.
  - **Stan urządzenia**

    Stan urządzenia klienckiego przypisany w oparciu o kryteria zdefiniowane przez administratora dla stanu ochrony antywirusowej na urządzeniu i aktywności urządzenia w sieci.
  - **Opis stanu**

    Stan ochrony urządzenia klienckiego i połączenia z Serwerem administracyjnym.
  - **Stan ochrony**

    To pole wyświetla bieżący stan ochrony urządzenia klienckiego w czasie rzeczywistym.

    Jeśli stan zmieni się na urządzeniu, nowy stan zostanie wyświetlony w oknie właściwości urządzenia dopiero po zsynchronizowaniu urządzenia klienckiego z Serwerem administracyjnym.
  - **Ostatnie pełne skanowanie**

    Data i godzina ostatniego skanowania w poszukiwaniu szkodliwego oprogramowania przeprowadzonego na urządzeniu klienckim.
  - **Wykryto wirusa**

    Całkowita liczba zagrożeń wykrytych na urządzeniu klienckim od momentu zainstalowania aplikacji zabezpieczającej (pierwsze skanowanie) lub od momentu ostatniego zresetowania licznika zagrożeń.
  - **Obiekty, których leczenie nie powiodło się**

    Liczba nieprzetworzonych plików na urządzeniu klienckim.

    To pole ignoruje liczbę nieprzetworzonych plików na urządzeniach mobilnych.
  - **Stan szyfrowania dysku**

Bieżący stan szyfrowania plików na lokalnych dyskach urządzenia. Opis statusów znajduje się w pomocy Kaspersky Endpoint Security for Windows.

- Sekcja **Stan urządzenia zdefiniowany przez aplikację** zawiera informacje o stanie urządzenia zdefiniowanym przez zarządzaną aplikację zainstalowaną na urządzeniu. Ten stan urządzenia może różnić się od stanu zdefiniowanego przez Kaspersky Security Center.

- **Aplikacje**

  Na tej karcie znajdują się wszystkie aplikacje Kaspersky zainstalowane na urządzeniu klienckim. Ta karta zawiera przyciski **Uruchom** i **Zatrzymaj** umożliwiające uruchomienie i zatrzymanie wybranej aplikacji Kaspersky (z wyłączeniem Agenta sieciowego). Można użyć tych przycisków, jeśli na zarządzanym urządzeniu dostępny jest port UDP o numerze 15000 do odbierania powiadomień push z Serwera administracyjnego. Jeśli zarządzane urządzenie nie jest dostępne dla powiadomień push, ale włączony jest tryb ciągłego połączenia z Serwerem administracyjnym (włączona jest opcja **Nie odłączaj od Serwera administracyjnego** w sekcji **Ogólne**), dostępne są również przyciski **Uruchom** i **Zatrzymaj**. W przeciwnym wypadku podczas próby uruchomienia lub zatrzymania aplikacji wyświetlany jest komunikat o błędzie. Możesz kliknąć nazwę aplikacji, aby wyświetlić ogólne informacje o aplikacji, listę zdarzeń, które wystąpiły na urządzeniu oraz ustawienia aplikacji.

- **Aktywne zasady i profile zasad**

  Ta karta zawiera listę zasad i profili zasad, które są aktualnie przypisane do zarządzanego urządzeniu.

- **Zadania**

  W zakładce **Zadania** możesz zarządzać zadaniami urządzenia klienckiego: przeglądać listę istniejących zadań, tworzyć nowe zadania, usuwać, uruchamiać i zatrzymywać zadania, a także modyfikować ustawienia zadań i przeglądać wyniki ich wykonania. Lista zadań jest tworzona w oparciu o dane otrzymane w czasie ostatniej synchronizacji komputera klienckiego z Serwerem administracyjnym. Serwer administracyjny żąda od urządzenia klienckiego szczegółów dotyczących stanu zadania. Jeżeli na zarządzanym urządzeniu dostępny jest port UDP o numerze 15000 do odbierania powiadomień push o otrzymaniu danych z Serwera administracyjnego, wyświetlany jest status zadania i włączane są przyciski umożliwiające zarządzanie zadaniem. Jeśli serwer push nie może uzyskać dostępu do zarządzanego urządzenia, ale włączony jest tryb ciągłego połączenia z Serwerem administracyjnym (włączona jest opcja **Nie odłączaj od Serwera administracyjnego** w sekcji **Ogólne**), dostępne są również akcje z zadaniami.

  Jeśli połączenie nie zostanie nawiązane, stan nie będzie wyświetlany.

- **Zdarzenia**

  Zakładka **Zdarzenia** wyświetla zdarzenia zarejestrowane na Serwerze administracyjnym dla wybranego urządzenia klienckiego.

  Możesz eksportować, kopiować i usuwać zdarzenia urządzenia.

- **Incydenty związane z bezpieczeństwem**

  Na zakładce **Incydenty związane z bezpieczeństwem** możesz przejrzeć, zmodyfikować i utworzyć incydenty związane z bezpieczeństwem dla urządzenia klienckiego. Problemy bezpieczeństwa mogą być tworzone automatycznie poprzez zarządzane aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim, a także ręcznie przez administratora. Na przykład, jeśli niektórzy użytkownicy regularnie przenoszą szkodliwe oprogramowanie ze swoich nośników wymiennych na urządzenia, administrator może utworzyć problem bezpieczeństwa. W treści problemu bezpieczeństwa administrator może dostarczyć krótki opis przypadku oraz zalecane działania (na przykład działania dyscyplinarne wobec użytkownika), a także dodać odsyłacz.

  Problem bezpieczeństwa, dla którego zostały wykonane wszystkie wymagane działania, nazywane jest *przetworzonym*. Obecność nieprzetworzonych problemów bezpieczeństwa może zostać wybrana jako warunek zmiany stanu urządzenia na *Krytyczny* lub *Ostrzeżenie*.

Ta sekcja zawiera listę problemów bezpieczeństwa, które zostały utworzone dla urządzenia. Problemy bezpieczeństwa są klasyfikowane według priorytetu i typu. Typ incydentu związanego z bezpieczeństwem jest definiowany przez aplikację Kaspersky, która utworzyła incydent związany z bezpieczeństwem. Możesz podświetlić przetworzone zdarzenia na liście, zaznaczając pole w kolumnie **Przetworzone**.

- **Znaczniki**

  W zakładce **Znaczniki** możesz zarządzać listą słów kluczowych, które są używane podczas wyszukiwania urządzeń klienckich: przejrzeć listę istniejących znaczników, przypisać znaczniki z listy, skonfigurować reguły automatycznego oznaczania oraz dodać nowe znaczniki i zmienić nazwy starszych znaczników, a także usunąć znaczniki.

- **Zaawansowane**

  Ta zakładka zawiera następujące sekcje:

  - **Rejestr aplikacji**. W tej sekcji możesz przejrzeć rejestr aplikacji zainstalowanych na urządzeniu klienckim i ich uaktualnień, a także możesz skonfigurować wyświetlanie rejestru aplikacji.

    Informacje o zainstalowanych aplikacjach są dostępne, jeśli Agent sieciowy zainstalowany na urządzeniu klienckim prześle żądane informacje do Serwera administracyjnego. Możesz skonfigurować przesyłanie informacji do Serwera administracyjnego w oknie właściwości Agenta sieciowego lub jego zasady, w sekcji **Repozytoria**.

    Kliknięcie nazwy aplikacji powoduje otwarcie okna zawierającego szczegółowe informacje o aplikacji oraz listę pakietów aktualizacji zainstalowanych dla aplikacji.

  - **Pliki wykonywalne**. Ta sekcja wyświetla pliki wykonywalne wykryte na urządzeniu klienckim.

  - **Punkty dystrybucji**. Ta sekcja zawiera listę punktów dystrybucji, z którymi urządzenie komunikuje się.

    - **Eksportuj do pliku**

      Kliknij przycisk **Eksportuj do pliku**, aby zapisać do pliku listę punktów dystrybucji, z którymi urządzenie komunikuje się. Domyślnie aplikacja eksportuje listę urządzeń do pliku CSV.

    - **Właściwości**

      Kliknij przycisk **Właściwości**, aby przejrzeć i skonfigurować punkt dystrybucji, z którym urządzenie komunikuje się.

  - **Rejestr sprzętu**. W tej sekcji możesz wyświetlić informacje o sprzęcie zainstalowanym na urządzeniu klienckim.

    Jeżeli Agent sieciowy jest zainstalowany na urządzeniu z systemem Windows, wysyła on do Serwera administracyjnego następujące informacje o sprzęcie urządzenia:

    - Pamięć RAM
    - Urządzenia pamięci masowej
    - Płyta główna
    - Procesor
    - Karty sieciowe
    - Monitory

- Karta graficzna
- Karta dźwiękowa

Jeżeli Agent sieciowy jest zainstalowany na urządzeniu z systemem Linux lub macOS, wysyła on do Serwera administracyjnego następujące informacje o sprzęcie urządzenia, jeżeli informacje te są dostarczane przez system operacyjny:

- Całkowita ilość pamięci RAM
- Całkowita pojemność urządzeń pamięci masowej
- Płyta główna
- Procesor
- Karty sieciowe

- **Dostępne aktualizacje**. Sekcja ta wyświetla listę aktualizacji oprogramowania znajdujących się na tym urządzeniu, ale jeszcze nie zainstalowanych.

- **Luki w oprogramowaniu**. Ta sekcja zawiera informacje o lukach w aplikacjach firm trzecich zainstalowanych na urządzeniach klienckich.

  Aby zapisać luki w pliku, zaznacz pola wyboru obok luk, które chcesz zapisać, a następnie kliknij przycisk **Eksportuj do pliku CSV** lub przycisk **Eksportuj do pliku TXT**.

  Ta sekcja zawiera następujące ustawienia:

  - **Pokaż tylko luki, które można naprawić**

    Jeśli ta opcja jest włączona, sekcja wyświetla luki, które można naprawić przy użyciu poprawki.

    Jeśli ta opcja jest wyłączona, sekcja wyświetla luki, które można wyeliminować przy użyciu poprawki, oraz luki, dla których nie opublikowano poprawki.

    Domyślnie opcja ta jest włączona.

  - **Właściwości luki**

    Na liście kliknij nazwę luki w oprogramowaniu, aby przejrzeć właściwości wybranej luki w oprogramowaniu w oddzielnym oknie. W oknie możesz wykonać następujące czynności:

    - Zignoruj lukę w oprogramowaniu na tym zarządzanym urządzeniu (w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console).
    - Przejrzyj listę zalecanych poprawek dla luki.
    - Ręcznie określ aktualizacje oprogramowania, aby naprawić lukę (w Konsoli administracyjnej lub w Kaspersky Security Center Web Console).
    - Przejrzyj instancje luki.
    - Przejrzyj listę istniejących zadań, aby naprawić lukę i utworzyć nowe zadania w celu wyeliminowania luki.

- **Zdalna diagnostyka** W tej sekcji możesz przeprowadzić zdalną diagnostykę urządzeń klienckich.

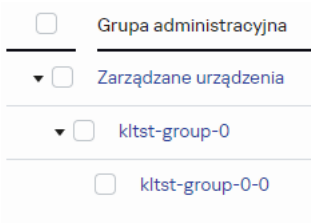
Jeśli używasz systemu PostgreSQL, MariaDB lub MySQL DBMS, karta **Zdarzenia** może wyświetlać niekompletną listę zdarzeń dla wybranego urządzenia klienckiego. Dzieje się tak, gdy system DBMS przechowuje bardzo dużą liczbę zdarzeń. Liczbę wyświetlanych zdarzeń można zwiększyć, wykonując jedną z następujących czynności:

- Usuwanie niepotrzebnych zdarzeń.
- Skrócenie okresu przechowywania niepotrzebnych zdarzeń.

Aby zobaczyć pełną listę zdarzeń zarejestrowanych na Serwerze administracyjnym dla danego urządzenia, należy użyć opcji Raporty.

Tworzenie grup administracyjnych

Od razu po zainstalowaniu Kaspersky Security Center, hierarchia grup administracyjnych zawiera tylko jedną grupę administracyjną, która nosi nazwę **Zarządzane urządzenia**. Podczas tworzenia hierarchii grup administracyjnych możesz dodać urządzenia, w tym maszyny wirtualne, do folderu **Zarządzane urządzenia**, a także możesz dodać zagnieżdżone grupy (patrz rysunek poniżej).



Wyświetlanie hierarchii grup administracyjnych

W celu utworzenia grupy administracyjnej:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Hierarchia grup**.
2. W strukturze grupy administracyjnej wybierz grupę administracyjną, aby uwzględnić nową grupę administracyjną.
3. Kliknij przycisk **Dodaj**.
4. W oknie **Nazwa nowej grupy administracyjnej**, które zostanie otwarte, wprowadź nazwę grupy, a następnie kliknij przycisk **Dodaj**.

W nowej grupie administracyjnej z określoną nazwą pojawi się w hierarchii grup administracyjnych.

Aplikacja umożliwia tworzenie hierarchii grup administracyjnych opartej na strukturze Active Directory lub na strukturze sieci domeny. Strukturę grup możesz również utworzyć z pliku tekstowego.

W celu utworzenia struktury grup administracyjnych:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Hierarchia grup**.
2. Kliknij przycisk **Importuj**.

Zostanie uruchomiony Kreator struktury nowej grupy administracyjnej. Postępuj zgodnie z instrukcjami kreatora.

Ręczne dodawanie urządzeń do grupy administracyjnej

Możesz automatycznie przenieść urządzenia do grup administracyjnych, tworząc reguły przenoszenia urządzeń, lub ręcznie, przenosząc urządzenia z jednej grupy administracyjnej do innej lub dodając urządzenia do wybranej grupy administracyjnej. Ta sekcja opisuje sposób ręcznego dodawania urządzeń do grupy administracyjnej.

W celu ręcznego dodania jednego lub kilku urządzeń do wybranej grupy administracyjnej:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
2. Kliknij odnośnik **Obecna ścieżka:** `<obecna ścieżka>` nad listą.
3. W otwartym oknie wybierz grupę administracyjną, do której chcesz dodać urządzenia.
4. Kliknij przycisk **Dodaj urządzenia**.

   Zostanie uruchomiony Kreator przenoszenia urządzeń.
5. Utwórz listę urządzeń, które chcesz dodać do grupy administracyjnej.

   > Możesz dodać tylko urządzenia, dla których informacje zostały już dodane do bazy danych Serwera administracyjnego przy podłączeniu urządzenia lub po wykrywaniu urządzeń.

   Wybierz sposób dodawania urządzeń do listy:

   - Kliknij przycisk **Dodaj urządzenia**, a następnie określ urządzenia w jeden z następujących sposobów:
     - Wybierz urządzenia z listy urządzeń wykrytych przez Serwer administracyjny.
     - Określ adres IP urządzenia lub zakres IP.

       > Zakres adresów IP nie może zawierać więcej niż 1 048 576 adresów.

     - Określ nazwę NetBIOS lub nazwę DNS urządzenia.

       > Pole nazwy urządzenia nie może zawierać spacji lub następujących zakazanych znaków: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %
   - Kliknij przycisk **Zaimportuj urządzenia z pliku**, aby zaimportować listę urządzeń z pliku .txt. Adres lub nazwa każdego urządzenia musi znajdować się w oddzielnym wierszu.

     > Plik nie może zawierać spacji lub następujących zakazanych znaków: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

6. Przejrzyj listę urządzeń, które mają zostać dodane do grupy administracyjnej. Możesz edytować listę, dodając lub usuwając urządzenia.

7. Jeśli upewnisz się, że lista jest poprawna, kliknij przycisk **Dalej**.

Kreator przetwarza listę urządzeń i wyświetla wynik. Pomyślnie przetworzone urządzenia zostaną dodane do grupy administracyjnej i będą wyświetlane na liście urządzeń pod nazwami wygenerowanymi przez Serwer administracyjny.

Ręczne przenoszenie urządzeń lub klastrów do grupy administracyjnej

Możesz przenieść urządzenia z jednej grupy administracyjnej do innej lub z grupy nieprzypisanych urządzeń do grupy administracyjnej.

Możesz także przenosić klastry lub macierze serwerowe z jednej grupy administracyjnej do drugiej. Kiedy przenosisz klaster lub macierz serwerową do innej grupy, wszystkie jego węzły są przenoszone razem z nim, ponieważ klaster i dowolny z jego węzłów zawsze należą do tej samej grupy administracyjnej. Po wybraniu pojedynczego węzła klastra na karcie **Urządzenia** przycisk **Przenieś do grupy** staje się niedostępny.

W celu przeniesienia jednego lub kilku urządzeń lub klastrów do wybranej grupy administracyjnej:

1. Otwórz grupę administracyjną, z której chcesz przenieść urządzenia. W tym celu wykonaj jedną z następujących czynności:

   - Aby otworzyć grupę administracyjną, przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**, kliknij odnośnik ścieżki w polu **Bieżąca ścieżka** i wybierz grupę administracyjną w otwartym okienku po lewej stronie.

   - Aby otworzyć grupę **Urządzenia nieprzypisane**, w menu głównym przejdź do **Wykrywanie i wdrażanie** → **Urządzenia nieprzypisane**.

2. Jeżeli grupa administracyjna zawiera klastry lub macierze serwerowe, sekcja **Zarządzane urządzenia** jest podzielona na dwie karty — kartę **Urządzenia** oraz kartę **Klastry i grupy serwerów**. Otwórz kartę obiektu, który chcesz przenieść.

3. Zaznacz pola obok urządzeń lub klastrów, które chcesz przenieść do innej grupy.

4. Kliknij przycisk **Przenieś do grupy**.

5. W hierarchii grup administracyjnych zaznacz pole obok grupy administracyjnej, do której chcesz przenieść wybrane urządzenia lub klastry.

6. Kliknij przycisk **Przenieś**.

Wybrane urządzenia lub klastry są przenoszone do wybranej grupy administracyjnej.

Tworzenie reguł przenoszenia urządzeń

Możesz skonfigurować reguły przenoszenia urządzeń, czyli reguły, które automatycznie przypisują urządzenia do grup administracyjnych.

W celu utworzenia reguły przenoszenia:

1. W menu głównym przejdź na **Zasoby (urządzenia)** → **Reguły przenoszenia**.
2. Kliknij **Dodaj**.
3. W otwartym oknie, na zakładce **Ogólne** określ następujące informacje:
   - **Nazwa reguły**

     Wprowadź nazwę nowej reguły.

     Jeśli kopiujesz regułę, nowa reguła otrzyma tę samą nazwę co reguła źródłowa, ale do nazwy zostanie dodany indeks w formacie (), na przykład: (1).
   - **Grupa administracyjna**

     Wybierz grupę administracyjną, do której urządzenia są przenoszone automatycznie.
   - **Aktywna reguła**

     Jeśli ta opcja jest włączona, reguła jest włączona i zaczyna działać po jej zapisaniu.

     Jeśli ta opcja jest wyłączona, reguła zostaje utworzona, ale nie jest włączona. Nie będzie działać, dopóki nie włączysz tej opcji.
   - **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**

     Jeśli ta opcja jest włączona, do wybranej grupy zostaną przeniesione tylko urządzenia nieprzypisane.

     Jeśli ta opcja jest wyłączona, urządzenia, które już należą do innych grup administracyjnych, a także urządzenia nieprzypisane, zostaną przeniesione do wybranej grupy.
   - **Zastosuj regułę**

     Możesz wybrać jedną z następujących opcji:
     - **Uruchom raz na każdym urządzeniu**

       Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom.
     - **Uruchom raz na każdym urządzeniu, a następnie po każdej instalacji Agenta sieciowego**

       Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom, a następnie tylko wtedy, gdy Agent sieciowy jest ponownie instalowany na tych urządzeniach.
     - **Stosuj regułę w sposób ciągły**

       Reguła jest stosowana zgodnie z terminarzem, który Serwer administracyjny konfiguruje automatycznie (zazwyczaj co kilka godzin).
4. Na karcie **Warunki reguły** określ co najmniej jedno kryterium, według którego urządzenia są przenoszone do grupy administracyjnej.
5. Kliknij **Zapisz**.

Reguła przenoszenia została utworzona. Jest wyświetlana na liście reguł przenoszenia.

Im wyższa pozycja na liście, tym wyższy priorytet reguły. Aby zwiększyć lub zmniejszyć priorytet reguły przenoszenia, przesuń regułę odpowiednio w górę lub w dół na liście za pomocą myszy.

Jeśli zaznaczona jest opcja **Stosuj regułę w sposób ciągły**, reguła przenoszenia zostanie zastosowana niezależnie od ustawień priorytetu. Reguły takie są stosowane zgodnie z harmonogramem, który Serwer administracyjny konfiguruje automatycznie.

Jeśli atrybuty urządzenia spełniają warunki kilku reguł, urządzenie zostanie przeniesione do grupy docelowej reguły z najwyższym priorytetem (czyli tej, która znajduje się najwyżej na liście).

Kopiowanie reguł przenoszenia urządzeń

Możesz kopiować reguły przenoszenia, na przykład, jeśli chcesz mieć kilka identycznych reguł dla różnych docelowych grup administracyjnych.

W celu skopiowania istniejącej reguły przenoszenia:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym przejdź na **Zasoby (urządzenia)** → **Reguły przenoszenia**.
   - W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Reguły przenoszenia**.

   Zostanie wyświetlona lista reguł przenoszenia.

2. Zaznacz pole obok reguły, którą chcesz skopiować.
3. Kliknij **Kopiuj**.
4. W otwartym oknie zmień następujące informacje na zakładce **Ogólne** lub nie wprowadzaj żadnych zmian, jeśli chcesz tylko skopiować regułę bez zmiany jej ustawień:

   - **Nazwa reguły**

     Wprowadź nazwę nowej reguły.

     Jeśli kopiujesz regułę, nowa reguła otrzyma tę samą nazwę co reguła źródłowa, ale do nazwy zostanie dodany indeks w formacie (), na przykład: (1).

   - **Grupa administracyjna**

     Wybierz grupę administracyjną, do której urządzenia są przenoszone automatycznie.

   - **Aktywna reguła**

     Jeśli ta opcja jest włączona, reguła jest włączona i zaczyna działać po jej zapisaniu.

     Jeśli ta opcja jest wyłączona, reguła zostaje utworzona, ale nie jest włączona. Nie będzie działać, dopóki nie włączysz tej opcji.

   - **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**

     Jeśli ta opcja jest włączona, do wybranej grupy zostaną przeniesione tylko urządzenia nieprzypisane.

     Jeśli ta opcja jest wyłączona, urządzenia, które już należą do innych grup administracyjnych, a także urządzenia nieprzypisane, zostaną przeniesione do wybranej grupy.

- **Zastosuj regułę**

  Możesz wybrać jedną z następujących opcji:

  - **Uruchom raz na każdym urządzeniu**

    Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom.

  - **Uruchom raz na każdym urządzeniu, a następnie po każdej instalacji Agenta sieciowego**

    Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom, a następnie tylko wtedy, gdy Agent sieciowy jest ponownie instalowany na tych urządzeniach.

  - **Stosuj regułę w sposób ciągły**

    Reguła jest stosowana zgodnie z terminarzem, który Serwer administracyjny konfiguruje automatycznie (zazwyczaj co kilka godzin).

5. Na karcie **Warunki reguły** określ co najmniej jedno kryterium dla urządzeń, które mają być przenoszone automatycznie.

6. Kliknij **Zapisz**.

Nowa reguła przenoszenia została utworzona. Jest wyświetlana na liście reguł przenoszenia.

Warunki dla reguły przenoszenia urządzenia

Gdy tworzysz lub kopiujesz regułę przenoszenia urządzeń klienckich do grup administracyjnych, na karcie **Warunki reguły** ustawiasz warunki przenoszenia urządzeń. Aby określić, które urządzenia przenieść, możesz skorzystać z następujących kryteriów:

- Tagi przypisane do urządzeń klienckich.
- Parametry sieciowe. Na przykład możesz przenieść urządzenia z adresami IP z określonego zakresu.
- Aplikacje zarządzane zainstalowane na urządzeniach klienckich, na przykład Agent sieciowy lub Serwer administracyjny.
- Maszyny wirtualne, które są urządzeniami klienckimi.
- Informacje o jednostce organizacyjnej Active Directory (OU) z urządzeniami klienckimi.
- Informacje o segmencie chmury z urządzeniami klienckimi.

Poniżej znajdziesz opis, jak określić te informacje w regule przenoszenia urządzeń.

Jeśli określisz kilka warunków w regule, operator logiczny AND działa i wszystkie warunki mają zastosowanie w tym samym czasie. Jeśli nie zaznaczysz żadnych opcji lub pozostawisz niektóre pola puste, takie warunki nie mają zastosowania.

Zakładka Znaczniki

Na tej zakładce można skonfigurować regułę przenoszenia urządzeń na podstawie znaczników urządzenia, które zostały wcześniej dodane do opisów urządzeń klienckich. Aby to zrobić, wybierz wymagane tagi. Możesz także włączyć następujące opcje:

- **Zastosuj do urządzeń bez określonych znaczników**

  Jeśli ta opcja jest włączona, wszystkie urządzenia z określonymi tagami są wykluczane z reguły przenoszenia urządzeń. Jeśli ta opcja jest wyłączona, reguła przenoszenia urządzeń dotyczy urządzeń ze wszystkimi wybranymi tagami.

  Domyślnie opcja ta jest wyłączona.

- **Zastosuj, jeśli co najmniej jeden określony znacznik jest zgodny**

  Jeśli ta opcja jest włączona, reguła przenoszenia urządzeń dotyczy urządzeń klienckich z co najmniej jednym z wybranych tagów. Jeśli ta opcja jest wyłączona, reguła przenoszenia urządzeń dotyczy urządzeń ze wszystkimi wybranymi tagami.

  Domyślnie opcja ta jest wyłączona.

Karta Sieć

Na tej karcie możesz określić dane sieciowe urządzeń, które uwzględnia reguła przenoszenia urządzeń:

- **Nazwa urządzenia w sieci Windows**

  Nazwa sieciowa systemu Windows (nazwa NetBIOS) urządzenia lub adres IPv4 lub IPv6.

- **Domena Windows**

  Reguła przenoszenia urządzeń dotyczy wszystkich urządzeń znajdujących się w określonej domenie Windows.

- **Nazwa DNS urządzenia**

  Nazwa domeny DNS urządzenia klienckiego, które chcesz przenieść. Wypełnij to pole, jeśli Twoja sieć zawiera serwer DNS.

  > Jeśli dla bazy danych używanej przez Kaspersky Security Center ustawione jest sortowanie z rozróżnianiem wielkości liter, zachowaj wielkość liter podczas określania nazwy DNS urządzenia. W przeciwnym razie reguła przenoszenia urządzenia nie będzie działać.

- **Domena DNS**

  Reguła przenoszenia urządzeń dotyczy wszystkich urządzeń zawartych w określonym głównym sufiksie DNS. Wypełnij to pole, jeśli Twoja sieć zawiera serwer DNS.

- **Zakres IP**

  Jeśli ta opcja jest włączona, możesz wprowadzić początkowy i końcowy adres IP z zakresu adresów IP, do którego muszą zostać włączone odpowiednie urządzenia.

  Domyślnie opcja ta jest wyłączona.

- **Adres IP do łączenia z Serwerem administracyjnym**

  Jeżeli ta opcja jest włączona, możesz ustawić adresy IP, za pomocą których urządzenia klienckie będą połączone z Serwerem administracyjnym. W tym celu określ zakres adresów IP, który zawiera wszystkie niezbędne adresy IP.

  Domyślnie opcja ta jest wyłączona.

- **Urządzenie znajduje się w zakresie IP**

  Jeżeli ta opcja jest włączona, możesz wybrać zakres adresów IP, który wcześniej dodałeś w sekcji **Zakresy IP**. Odpowiednie urządzenia muszą znajdować się w wybranym zakresie adresów IP.

  Domyślnie opcja ta jest wyłączona.

- **Zmieniono profil połączenia**

  Wybierz jedną z następujących wartości:

  - **Tak**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich ze zmienionym profilem połączenia.
  - **Nie**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich, których profil połączenia nie uległ zmianie.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

- **Zarządzane przez inny Serwer administracyjny**

  Wybierz jedną z następujących wartości:

  - **Tak**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich zarządzanych przez inne Serwery administracyjne. Te serwery różnią się od serwera, na którym konfigurujesz regułę przenoszenia urządzeń.
  - **Nie**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich zarządzanych przez bieżący Serwer administracyjny.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

Karta Aplikacje

Na tej karcie możesz skonfigurować regułę przenoszenia urządzeń na podstawie zarządzanych aplikacji i systemów operacyjnych zainstalowanych na urządzeniach klienckich:

- **Agent sieciowy jest zainstalowany**

  Wybierz jedną z następujących wartości:

  - **Tak**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich z zainstalowanym Agentem sieciowym.
  - **Nie**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich, na których nie jest zainstalowany Agent sieciowy.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

- **Aplikacje**

  Określ, jakie zarządzane aplikacje powinny być zainstalowane na urządzeniach klienckich, aby reguła przenoszenia urządzeń miała zastosowanie do tych urządzeń. Na przykład możesz wybrać **Agent sieciowy Kaspersky Security Center 15.1** lub **Serwer administracyjny Kaspersky Security Center 15.1**.

  Jeśli nie wybierzesz żadnej zarządzanej aplikacji, warunek nie ma zastosowania.

- **Wersja systemu operacyjnego**

  Urządzenia klienckie można usuwać na podstawie wersji systemu operacyjnego. W tym celu określ systemy operacyjne, które powinny być zainstalowane na urządzeniach klienckich. W rezultacie reguła przenoszenia urządzeń dotyczy urządzeń klienckich z wybranymi systemami operacyjnymi.

  Jeśli nie włączysz tej opcji, warunek nie ma zastosowania. Domyślnie opcja ta jest wyłączona.

- **Typ systemu operacyjnego (bity)**

  Urządzenia klienckie można usuwać według rozmiarów bitowych systemu operacyjnego. W polu **Typ systemu operacyjnego (bity)** możesz wybrać jedną z następujących wartości:

  - **Nieznany**
  - **x86**
  - **AMD64**
  - **IA64**

  Aby sprawdzić architekturę systemu operacyjnego urządzeń klienckich:

  1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
  2. Kliknij przycisk **Ustawienia kolumn** (⚙) po prawej stronie.
  3. Wybierz opcję **Typ systemu operacyjnego (bity)**, a następnie kliknij przycisk **Zapisz**.

     Następnie dla każdego zarządzanego urządzenia zostanie wyświetlona architektura systemu operacyjnego.

- **Wersja dodatku Service Pack systemu operacyjnego**

  W tym polu możesz określić wersję pakietu systemu operacyjnego (w formacie *X.Y*), która będzie określać sposób stosowania reguły przenoszenia do urządzenia. Domyślnie nie jest zdefiniowana żadna wartość.

- **Certyfikat użytkownika**

  Wybierz jedną z następujących wartości:

  - **Zainstalowano**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń mobilnych z certyfikatem mobilnym.
  - **Nie zainstalowano**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń mobilnych bez certyfikatu mobilnego.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

- **Kompilacja systemu operacyjnego**

  To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować regułę przenoszenia urządzeń dla wszystkich numerów kompilacji z wyjątkiem określonego.

- **Numer wersji systemu operacyjnego**

  > To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer wydania. Możesz także skonfigurować regułę przenoszenia urządzeń dla wszystkich numerów wersji z wyjątkiem określonego.

Karta Maszyny wirtualne

Na tej karcie możesz skonfigurować regułę przenoszenia urządzeń w zależności od tego, czy urządzenia klienckie są maszynami wirtualnymi, czy częścią Virtual Desktop Infrastructure (VDI):

- **Jest maszyną wirtualną**

  Z listy rozwijalnej możesz wybrać jedną z następujących opcji:
  - **N/D**. Warunek nie ma zastosowania.
  - **Nie**. Przenosi urządzenia, które nie są maszynami wirtualnymi.
  - **Tak**. Przenosi urządzenia, które są maszynami wirtualnymi.

- **Typ maszyny wirtualnej**

- **Część Virtual Desktop Infrastructure**

  Z listy rozwijalnej możesz wybrać jedną z następujących opcji:
  - **N/D**. Warunek nie ma zastosowania.
  - **Nie**. Przenieś urządzenia, które nie są częścią VDI.
  - **Tak**. Przenieś urządzenia, które są częścią VDI.

Karta Sterownik domeny

Na tej karcie możesz określić, że konieczne jest przeniesienie urządzeń znajdujących się w jednostce organizacyjnej domeny. Możesz także przenieść urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej domeny:

- **Urządzenie wchodzi w skład następującej jednostki organizacyjnej**

  Jeśli ta opcja jest włączona, reguła przenoszenia urządzeń dotyczy urządzeń z jednostki organizacyjnej domeny określonej na liście pod opcją.

  Domyślnie opcja ta jest wyłączona.

- **Uwzględnij podrzędne jednostki organizacyjne**

  Jeśli ta opcja jest włączona, wybór zawiera urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej domeny.

  Domyślnie opcja ta jest wyłączona.

- **Przenieś urządzenia z podrzędnych jednostek do odpowiednich podgrup**

- **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń**

- **Usuń podgrupy, które nie są obecne w domenie**

- **Urządzenie należy do następującej grupy zabezpieczeń domeny**

  Jeśli ta opcja jest włączona, reguła przenoszenia urządzeń dotyczy urządzeń z grupy bezpieczeństwa domeny określonej na liście pod opcją.

  Domyślnie opcja ta jest wyłączona.

Zakładka Segmenty chmury

Na tej zakładce możesz określić, że konieczne jest przeniesienie urządzeń należących do określonych segmentów chmury:

- **Urządzenie znajduje się w segmencie chmury**

  Jeśli wybierzesz tę opcję, reguła przenoszenia urządzeń zostanie zastosowana do urządzeń klienckich należących do segmentu chmury. Możesz wybrać żądany segment chmury aż do podsieci na liście pod opcją.

  Domyślnie opcja ta jest wyłączona.

- **Włączając obiekty potomne**

  W przypadku wybrania tej opcji reguła przenoszenia urządzeń dotyczy nie tylko wybranego segmentu chmury, ale także obiektów podrzędnych tego segmentu.

  Domyślnie opcja ta jest wyłączona.

- **Przenieś urządzenia z obiektów zagnieżdżonych do odpowiednich podgrup**

- **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń**

- **Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury**

- **Urządzenie wykryte przy pomocy API**

  Z listy rozwijalnej możesz wybrać, czy urządzenie jest wykrywane przez narzędzia API:

  - **AWS**. Urządzenie jest wykrywane przy pomocy AWS API, co oznacza, że urządzenie znajduje się w środowisku chmury AWS.

  - **Azure**. Urządzenie jest wykrywane przy pomocy Azure API, co oznacza, że urządzenie znajduje się w środowisku chmury Azure.

  - **Google Cloud.** Urządzenie jest wykrywane przy pomocy Google API, co oznacza, że urządzenie znajduje się w środowisku Google Cloud.

- **Nie**. Urządzenie nie może zostać wykryte przy użyciu AWS, Azure lub Google API, co oznacza, że znajduje się poza środowiskiem chmury lub znajduje się w środowisku chmury, ale nie może zostać wykryte przy użyciu API.

- **Brak wartości**. Ten warunek nie ma zastosowania.

Informacje o klastrach i macierzach serwerowych

Kaspersky Security Center Linux obsługuje technologię klastra. Jeśli Agent sieciowy wyśle na Serwer administracyjny informacje potwierdzające, że aplikacja zainstalowana na urządzeniu klienckim jest częścią grupy serwerów, to urządzenie klienckie staje się węzłem klastra.

Jeśli grupa administracyjna zawiera klastry lub macierze serwerowe, na stronie **Zarządzane urządzenia** są wyświetlane dwie zakładki — jedna dla poszczególnych urządzeń, a druga dla klastrów i macierzy serwerowych. Po wykryciu zarządzanych urządzeń jako węzłów klastra, klaster jest dodawany jako pojedynczy obiekt na karcie **Klastry i grupy serwerów**.

Węzły klastra lub macierzy serwerowej są wymienione na karcie **Urządzenia** wraz z innymi zarządzanymi urządzeniami. Możesz przeglądać właściwości węzłów jako pojedynczych urządzeń i wykonywać inne operacje, ale nie możesz usunąć węzła klastra ani przenieść go do innej grupy administracyjnej niezależnie od jego klastra. Możesz usunąć lub przenieść tylko cały klaster.

Na klastrach lub macierzach serwerowych można wykonywać następujące operacje:

- Wyświetl właściwości

- Przenieś klaster lub macierz serwerową do innej grupy administracyjnej

  Kiedy przenosisz klaster lub macierz serwerową do innej grupy, wszystkie jego węzły są przenoszone razem z nim, ponieważ klaster i dowolny z jego węzłów zawsze należą do tej samej grupy administracyjnej.

- Delete

  Usunięcie klastra lub macierzy serwerowej jest zasadne tylko wtedy, gdy klaster lub macierz serwerowa nie istnieją już w sieci organizacji. Jeśli klaster jest nadal widoczny w Twojej sieci, a Agent sieciowy i aplikacja zabezpieczająca Kaspersky są nadal zainstalowane na węzłach klastra, Kaspersky Security Center automatycznie przywraca usunięty klaster i jego węzły z powrotem na listę zarządzanych urządzeń.

Właściwości klastra lub macierzy serwerowej

Aby wyświetlić ustawienia klastra lub macierzy serwerów:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia** → **Klastry i grupy serwerów**.

   Zostanie wyświetlona lista klastrów i macierzy serwerowych.

2. Kliknij nazwę wymaganego klastra lub macierzy serwerowej.

Zostanie wyświetlone okno właściwości wybranego klastra lub macierzy serwerowej.

Ogólne

W sekcji **Ogólne** wyświetlane są ogólne informacje dotyczące klastra lub macierzy serwerowej. Informacje są dostarczane w oparciu o dane otrzymane podczas ostatniej synchronizacji węzłów klastra z Serwerem administracyjnym:

- **Nazwa**
- **Opis**
- **Domena Windows**

  Domena lub grupa robocza systemu Windows, która zawiera klaster lub macierz serwerową.

- **Nazwa NetBIOS**

  Nazwa sieciowa systemu Windows klastra lub macierzy serwerowej.

- **Nazwa DNS**

  Nazwa domeny DNS klastra lub macierzy serwerowej.

Zadania

Na karcie **Zadania** możesz zarządzać zadaniami przydzielonymi do klastra lub macierzy serwerowej: przeglądać listę istniejących zadań; tworzyć nowe zadania; usuwać, uruchamiać i zatrzymywać zadania; modyfikować ustawienia zadań; oraz przeglądać wyniki ich wykonania. Wymienione zadania dotyczą aplikacji zabezpieczającej Kaspersky zainstalowanej na węzłach klastra. Kaspersky Security Center otrzymuje listę zadań i szczegóły stanu zadań z węzłów klastra. Jeśli połączenie nie jest nawiązane, stan nie jest wyświetlany.

Węzły

Na tej karcie wyświetlana jest lista węzłów wchodzących w skład klastra lub macierzy serwerowej. Możesz kliknąć nazwę węzła, aby wyświetlić okno właściwości urządzenia.

Aplikacja Kaspersky

Okno właściwości może również zawierać dodatkowe karty z informacjami i ustawieniami związanymi z aplikacją zabezpieczającą Kaspersky zainstalowaną na węzłach klastra.

Przeglądanie i konfigurowanie działań, gdy urządzenia wykazują brak aktywności

Jeśli urządzenia klienckie w grupie są nieaktywne, możesz otrzymać informacje na ten temat. Możesz także automatycznie usuwać takie urządzenia.

W celu przejrzenia lub skonfigurowania działań, gdy urządzenia w grupie wykazują brak aktywności:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Hierarchia grup**.
2. Kliknij nazwę żądanej grupy administracyjnej.

   Zostanie otwarte okno właściwości grupy administracyjnej.
3. W oknie właściwości przejdź na zakładkę **Ustawienia**.
4. W sekcji **Dziedziczenie** włącz lub wyłącz następujące opcje:

   - **Dziedzicz z grupy nadrzędnej**

     Ustawienia z tej sekcji są dziedziczone od grupy nadrzędnej, w której znajduje się urządzenie klienckie. Jeśli ta opcja jest włączona, ustawienia w sekcji **Aktywność urządzenia w sieci** nie mogą być modyfikowane.

     Ta opcja jest dostępna tylko wtedy, gdy grupa administracyjna posiada grupę nadrzędną.

     Domyślnie opcja ta jest włączona.

   - **Wymuś dziedziczenie ustawień w grupach podrzędnych**

     Wartości ustawień zostaną rozesłane do grup podrzędnych ale we właściwościach grup podrzędnych te ustawienia są zablokowane.

     Domyślnie opcja ta jest wyłączona.
5. W sekcji **Aktywność urządzenia** włącz lub wyłącz następujące opcje:

   - **Powiadom administratora, jeżeli urządzenie jest nieaktywne dłużej niż (dni)**

     Jeśli ta opcja jest włączona, administrator otrzyma powiadomienie o nieaktywnych urządzeniach. Możesz określić przedział czasu, po upływie którego tworzone jest zdarzenie **Urządzenie było nieaktywne w sieci od bardzo dawna**. Domyślny przedział czasu wynosi 7 dni.

     Domyślnie opcja ta jest włączona.

   - **Usuń urządzenie z grupy, jeżeli było nieaktywne dłużej niż (dni)**

     Jeśli ta opcja jest włączona, możesz określić przedział czasu, po upływie którego urządzenie zostanie automatycznie usunięte z grupy. Domyślny przedział czasu wynosi 60 dni.

     Domyślnie opcja ta jest włączona.
6. Kliknij **Zapisz**.

Twoje zmiany zostaną zapisane i zastosowane.

Informacje o stanach urządzeń

Kaspersky Security Center przypisze stan do każdego zarządzanego urządzenia. Określony stan zależy od tego, czy spełnione są warunki zdefiniowane przez użytkownika. W niektórych przypadkach, podczas przypisywania stanu do urządzenia, Kaspersky Security Center bierze pod uwagę flagę widoczności urządzenia w sieci (patrz tabela poniżej). Na przykład, jeśli do zarządzanego urządzenia został przypisany stan *Krytyczny*, ponieważ spełniony był warunek *Bazy danych są nieaktualne*, a później flaga widoczności została ustawiona dla urządzenia, wówczas do urządzenia zostanie przypisany stan *OK*. Jeśli Kaspersky Security Center nie znajdzie urządzenia w sieci w ciągu dwóch godzin, flaga widoczności urządzenia zostanie ustawiona na *Nie jest widoczne*.

Stany są następujące:

- *Krytyczny* lub *Krytyczny / Widoczne*
- *Ostrzeżenie* lub *Ostrzeżenie / Widoczne*
- *OK* lub *OK / Widoczne*

Poniższa tabela wyświetla domyślne warunki, które muszą być spełnione, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia, wraz ze wszystkimi możliwymi wartościami.

Warunki przypisania stanu do urządzenia

Warunek	Opis warunku	Dostępne wartości
Aplikacja zabezpieczająca nie jest zainstalowana	Agent sieciowy jest zainstalowany na urządzeniu, ale aplikacja zabezpieczająca nie jest zainstalowana.	• Przycisk przełącznika jest ustawiony w pozycji włączenia. • Przycisk przełącznika jest ustawiony w pozycji wyłączenia.
Wykryto zbyt wiele wirusów	Niektóre wirusy zostały wykryte na urządzeniu przez zadanie wykrywania wirusów, na przykład, zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* oraz liczba wykrytych wirusów przekraczają określoną wartość.	Większe niż 0.
Poziom ochrony w czasie rzeczywistym jest inny niż poziom zdefiniowany przez administratora	Urządzenie jest widoczne w sieci, ale poziom ochrony w czasie rzeczywistym różni się od poziomu ustawionego (w warunku) przez administratora dla stanu urządzenia.	• Zatrzymane. • Wstrzymane. • Uruchomione.
Skanowanie w poszukiwaniu złośliwego oprogramowania nie było wykonywane od dłuższego czasu	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale zadanie *Skanowanie w poszukiwaniu szkodliwego oprogramowania* ani zadanie lokalnego skanowania nie było uruchamiane w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego 7 dni temu lub wcześniej.	Więcej niż 1 dzień.
Bazy danych są nieaktualne	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale antywirusowe bazy danych nie były aktualizowane na tym urządzeniu w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego dzień wcześniej lub jeszcze wcześniej.	Więcej niż 1 dzień.
Niepołączony od dłuższego czasu	Agent sieciowy jest zainstalowany na urządzeniu, ale urządzenie nie było połączone z Serwerem administracyjnym w określonym przedziale czasu, ponieważ urządzenie było wyłączone.	Więcej niż 1 dzień.
Wykryto aktywne zagrożenia	Liczba nieprzetworzonych obiektów w folderze **Aktywne zagrożenia** przekracza określoną wartość.	Więcej niż 0 elementów.

Warunek	Opis warunku	Dostępne wartości
Wymagane jest ponowne uruchomienie	Urządzenie jest widoczne w sieci, ale aplikacja wymaga ponownego uruchomienia urządzenia dłużej niż określony przedział czasu i z jednego z wybranych powodów.	Więcej niż 0 minut.
Zainstalowane są niekompatybilne aplikacje	Urządzenie jest widoczne w sieci, ale inwentaryzacja oprogramowania wykonywana poprzez Agenta sieciowego wykryła niekompatybilne aplikacje zainstalowane na urządzeniu.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto luki w oprogramowaniu	Urządzenie jest widoczne w sieci, a Agent sieciowy jest zainstalowany na urządzeniu, ale zadanie *Wyszukiwania luk i wymaganych aktualizacji* wykryło luki z określonym priorytetem w aplikacjach zainstalowanych na urządzeniu.	• Krytyczny. • Wysoki. • Średni. • Ignoruj, jeśli luka nie może być naprawiona. • Ignoruj, jeśli aktualizacja jest przypisana do instalacji.
Licencja utraciła ważność	Urządzenie jest widoczne w sieci, ale licencja utraciła ważność.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Licencja wkrótce utraci ważność	Urządzenie jest widoczne w sieci, ale licencja utraci ważność na urządzeniu za mniej niż określona liczba dni.	Mniej niż 0 dni.

Warunek	Opis warunku	Dostępne wartości
Wyszukiwanie aktualizacji Windows Update nie było przeprowadzane od dłuższego czasu	Urządzenie jest widoczne w sieci, ale zadanie *Wyszukiwania luk i wymaganych aktualizacji* nie było uruchamiane w zdefiniowanym przedziale czasu.	Więcej niż 1 dzień.
Nieprawidłowy stan szyfrowania	Agent sieciowy jest zainstalowany na urządzeniu, ale wynik szyfrowania urządzenia jest równy określonej wartości.	• Nie zgadza się z zasadą w wyniku odmowy użytkownika (tylko dla urządzeń zewnętrznych). • Nie zgadza się z zasadą w wyniku błędu. • Po zastosowaniu zasady wymagane jest ponowne uruchomienie. • Nie określono zasady szyfrowania. • Nieobsługiwany. • Po zastosowaniu zasady.
Ustawienia urządzenia mobilnego nie są zgodne z zasadą	Ustawienia urządzenia mobilnego są inne niż ustawienia, które zostały określone w zasadzie Kaspersky Endpoint Security for Android podczas sprawdzania reguł zgodności.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto nieprzetworzone incydenty związane z bezpieczeństwem	Na urządzeniu zostały wykryte pewne nieprzetworzone problemy bezpieczeństwa. Problemy bezpieczeństwa mogą być tworzone automatycznie poprzez zarządzane aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim, a także ręcznie przez administratora.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Stan urządzenia zdefiniowany przez aplikację	Stan urządzenia jest definiowany przez zarządzaną aplikację. Zarządzane urządzenia mogą mieć stan zdefiniowany przez zarządzane aplikacje, niezależnie od ustawień Kaspersky Security Center. Po zwróceniu przez ten stan jednego ze stanów zdefiniowanych przez Kaspersky Security Center, Serwer administracyjny przypisuje zarządzanemu urządzeniu najbardziej krytyczny stan spośród stanów zwróconych przez zarządzaną aplikację i przypisanych przez Serwer administracyjny. Stany zdefiniowane przez zarządzane aplikacje mają opisy przekazane przez zarządzane aplikacje. Możesz wyświetlić opisy na liście zarządzanych urządzeń, w kolumnie **Opis stanu**.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Brakuje miejsca na dysku urządzenia	Wolnego miejsca na dysku jest mniej niż określona wartość lub urządzenie nie mogło zostać zsynchronizowane z Serwerem administracyjnym. Stan *Krytyczny* lub *Ostrzeżenie* zmieniło się na stan *OK*, gdy urządzenie zostało pomyślnie zsynchronizowane z Serwerem administracyjnym, a wolna przestrzeń na urządzeniu jest większa niż lub równa określonej wartości.	Więcej niż 0 MB.
Zarządzanie urządzeniem nie jest możliwe	Podczas wykrywania urządzeń, urządzenie zostało rozpoznane jako widoczne w sieci, ale więcej niż trzy próby synchronizacji z Serwerem administracyjnym nie powiodły się.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Ochrona jest wyłączona	Urządzenie jest widoczne w sieci, ale aplikacja zabezpieczająca na urządzeniu została wyłączona na dłużej niż określony przedział czasu. W tym przypadku stan aplikacji zabezpieczającej to *zatrzymany* lub *błąd* i różni się od następujących: *uruchamianie*, *uruchomiony* lub *zawieszony*.	Więcej niż 0 minut.
Aplikacja zabezpieczająca nie jest uruchomiona	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale nie jest uruchomiona.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.

Kaspersky Security Center umożliwia skonfigurowanie automatycznego przełączania stanu urządzenia w grupie administracyjnej, gdy spełnione są określone warunki. Jeśli określone warunki są spełnione, do urządzenia klienckiego zostanie przypisany jeden z następujących stanów: *Krytyczny* lub *Ostrzeżenie*. Jeśli określone warunki zostaną spełnione, urządzeniu klienckiemu zostanie przypisany stan *OK*.

Różne stany mogą odpowiadać różnym wartościom jednego warunku. Na przykład, domyślnie, jeśli warunek **Bazy danych są nieaktualne** posiada wartość **Ponad 3 dni**, do urządzenia klienckiego zostaje przypisany stan *Ostrzeżenie*; jeśli wartość to **Ponad 7 dni**, wówczas zostanie przypisany stan *Krytyczny*.

Jeśli aktualizujesz Kaspersky Security Center z poprzedniej wersji, wartości warunku **Bazy danych są nieaktualne** dla przypisania stanu do *Krytyczne* lub *Ostrzeżenie* nie zmienią się.

Konfigurowanie przełączania stanów urządzeń

Możesz zmienić warunki, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia.

W celu włączenia zmiany stanu urządzenia na Krytyczny:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Hierarchia grup**.
2. Na otwartej liście grup kliknij odnośnik z nazwą grupy, dla której chcesz zmienić przełączanie stanów urządzeń.
3. W otwartym oknie właściwości wybierz zakładkę **Stan urządzenia**.
4. W lewej części okna wybierz **Krytyczny**.
5. W prawej części okna, w sekcji **Ustaw stan Krytyczny, jeśli** włącz warunek, aby przełączyć urządzenie do stanu *Krytyczny*.

   Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

6. Wybierz przycisk radiowy obok warunku na liście.
7. W lewym górnym rogu listy kliknij przycisk **Edytuj**.
8. Dla wybranego warunku ustaw żądaną wartość.
   Nie dla każdego warunku można ustawić wartości.
9. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Krytyczne*.

W celu włączenia zmiany stanu urządzenia na Ostrzeżenie:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Hierarchia grup**.
2. Na otwartej liście grup kliknij odnośnik z nazwą grupy, dla której chcesz zmienić przełączanie stanów urządzeń.
3. W otwartym oknie właściwości wybierz zakładkę **Stan urządzenia**.
4. W lewej części okna wybierz **Ostrzeżenie**.

5. W prawej części okna, w sekcji **Ustaw stan Ostrzeżenie, jeśli** włącz warunek, aby przełączyć urządzenie do stanu *Ostrzeżenie*.

   Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

6. Wybierz przycisk radiowy obok warunku na liście.
7. W lewym górnym rogu listy kliknij przycisk **Edytuj**.
8. Dla wybranego warunku ustaw żądaną wartość.

   Nie dla każdego warunku można ustawić wartości.

9. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Ostrzeżenie*.

Zdalne połączenie z pulpitem urządzenia klienckiego

Administrator może uzyskać zdalny dostęp do pulpitu urządzenia klienckiego poprzez Agenta sieciowego zainstalowanego na urządzeniu klienckim. Zdalne połączenie z urządzeniem poprzez Agenta sieciowego jest możliwe nawet wtedy, gdy porty TCP i UDP urządzenia klienckiego są zamknięte.

Po nawiązaniu połączenia z urządzeniem, administrator uzyskuje pełny dostęp do informacji przechowywanych na tym urządzeniu, dzięki czemu może zarządzać aplikacjami, które są na nim zainstalowane.

Zdalne połączenie musi być dozwolone w ustawieniach systemu operacyjnego docelowego zarządzanego urządzenia. Na przykład, w systemie Windows 10 ta opcja nazywa się **Zezwalaj na połączenia Pomocy zdalnej z tym komputerem** (tę opcję można znaleźć w **Panel sterowania** → **System i zabezpieczenia** → **System** → **Ustawienia zdalne**). Jeśli posiadasz licencję dla funkcji Zarządzanie lukami i poprawkami, możesz wymusić włączenie tej funkcji podczas nawiązywania połączenia z zarządzanym urządzeniem. Jeśli nie masz licencji, włącz tę opcję lokalnie na docelowym zarządzanym urządzeniu. Jeśli ta opcja jest wyłączona, nawiązanie zdalnego połączenia nie jest możliwe.

W celu nawiązania zdalnego połączenia z urządzeniem, musisz posiadać dwa narzędzia:

- Narzędzie Kaspersky o nazwie klsctunnel. To narzędzie musi być przechowywane na stacji roboczej administratora. Tego narzędzia używasz do tunelowania połączenia między urządzeniem klienckim a Serwerem administracyjnym.

  Kaspersky Security Center umożliwia tunelowanie połączeń TCP z Konsoli administracyjnej poprzez Serwer administracyjny, a następnie poprzez Agenta sieciowego do określonego portu na zarządzanym urządzeniu. Tunelowanie połączeń jest przeznaczone dla połączenia aplikacji klienckiej na urządzeniu z zainstalowaną Konsolą administracyjną z portem TCP na zarządzanym urządzeniu—jeśli nie jest możliwe bezpośrednie połączenie między Konsolą administracyjną a urządzeniem docelowym.

  Tunelowanie połączenia pomiędzy zdalnym urządzeniem klienckim a Serwerem administracyjnym jest wymagane, gdy port używany do nawiązania połączenia z Serwerem administracyjnym nie jest dostępny na urządzeniu. Port może być niedostępny na urządzeniu w następujących przypadkach:

  - Zdalne urządzenie jest podłączone do sieci lokalnej, która wykorzystuje mechanizm NAT.
  - Zdalne urządzenie jest częścią sieci lokalnej Serwera administracyjnego, ale jego port jest zamknięty przez zaporę sieciową.

- Standardowy składnik systemu Microsoft Windows o nazwie Podłączanie pulpitu zdalnego. Połączenie ze zdalnym pulpitem jest nawiązywane przy użyciu standardowego narzędzia Windows o nazwie mstsc.exe zgodnie z ustawieniami narzędzia.

  Połączenie z bieżącą sesją zdalnego pulpitu użytkownika jest nawiązywane bez zgody użytkownika. Po nawiązaniu przez administratora połączenia z sesją, użytkownik urządzenia zostaje odłączony od sesji bez wcześniejszego powiadomienia.

W celu zdalnego połączenia z pulpitem urządzenia klienckiego:

1. W Konsoli administracyjnej opartej na MMC, w menu kontekstowym Serwera administracyjnego wybierz **Właściwości**.
2. W otwartym oknie właściwości Serwera administracyjnego przejdź do **Ustawienia połączenia z Serwerem administracyjnym** → **Porty połączenia**.
3. Upewnij się, że opcja **Otwórz port RDP dla Kaspersky Security Center Web Console** jest włączona.
4. W Kaspersky Security Center Web Console przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
5. W polu **Bieżąca ścieżka** nad listą zarządzanych urządzeń kliknij łącze ścieżki.
6. W otwartym okienku po lewej stronie wybierz grupę administracyjną zawierającą urządzenie, do którego chcesz uzyskać dostęp.
7. Zaznacz pole obok nazwy urządzenia, do którego chcesz uzyskać dostęp.
8. Kliknij przycisk **Połącz przez Pulpit zdalny**.

   Zostanie otwarte okno Pulpit zdalny (tylko Windows).
9. Włącz opcję **Zezwól na połączenie ze zdalnym pulpitem na zarządzanym urządzeniu**. W tym przypadku połączenie zostanie nawiązane nawet wtedy, gdy zdalne połączenia są aktualnie zabronione w ustawieniach systemu operacyjnego na zarządzanym urządzeniu.

   Ta opcja jest dostępna tylko wtedy, gdy posiadasz licencję dla funkcji Zarządzanie lukami i poprawkami.
10. Kliknij przycisk **Pobierz**, aby pobrać narzędzie klsctunnel.
11. Kliknij przycisk **Kopiuj do schowka**, aby skopiować tekst z pola tekstowego. Ten tekst to Duży obiekt binarny (BLOB), który zawiera ustawienia wymagane do nawiązania połączenia między Serwerem administracyjnym a zarządzanym urządzeniem.

    BLOB jest ważny przez 3 minuty. Jeśli wygasł, otwórz ponownie okno Pulpit zdalny (tylko Windows), aby wygenerować nowy BLOB.
12. Uruchom narzędzie klsctunnel.

    Zostanie otwarte okno narzędzia.
13. Wklej skopiowany tekst do pola tekstowego.
14. Jeśli korzystasz z serwera proxy, zaznacz pole **Użyj serwera proxy**, a następnie określ ustawienia połączenia z serwerem proxy.

15. Kliknij przycisk **Otwórz port**.

    Zostanie otwarte okno logowania Podłączanie pulpitu zdalnego.

16. Podaj dane uwierzytelniające konta, na którym jesteś aktualnie zalogowany do konsoli Kaspersky Security Center Web Console.

17. Kliknij przycisk **Połącz**.

Po nawiązaniu połączenia z urządzeniem, pulpit jest dostępny w oknie Podłączanie pulpitu zdalnego systemu Microsoft Windows.

Nawiązywanie połączenia z urządzeniami poprzez udostępnianie pulpitu Windows

Administrator może uzyskać zdalny dostęp do pulpitu urządzenia klienckiego poprzez Agenta sieciowego zainstalowanego na urządzeniu klienckim. Zdalne połączenie z urządzeniem poprzez Agenta sieciowego jest możliwe nawet wtedy, gdy porty TCP i UDP urządzenia klienckiego są zamknięte.

Administrator może połączyć się z istniejącą sesją na urządzeniu klienckim bez rozłączania użytkownika w tej sesji. W tym przypadku administrator i użytkownik sesji na urządzeniu klienckim współdzielą dostęp do pulpitu.

W celu nawiązania zdalnego połączenia z urządzeniem, musisz posiadać dwa narzędzia:

- Narzędzie Kaspersky o nazwie klsctunnel. To narzędzie musi być przechowywane na stacji roboczej administratora. Tego narzędzia używasz do tunelowania połączenia między urządzeniem klienckim a Serwerem administracyjnym.

  Kaspersky Security Center umożliwia tunelowanie połączeń TCP z Konsoli administracyjnej poprzez Serwer administracyjny, a następnie poprzez Agenta sieciowego do określonego portu na zarządzanym urządzeniu. Tunelowanie połączeń jest przeznaczone dla połączenia aplikacji klienckiej na urządzeniu z zainstalowaną Konsolą administracyjną z portem TCP na zarządzanym urządzeniu—jeśli nie jest możliwe bezpośrednie połączenie między Konsolą administracyjną a urządzeniem docelowym.

  Tunelowanie połączenia pomiędzy zdalnym urządzeniem klienckim a Serwerem administracyjnym jest wymagane, gdy port używany do nawiązania połączenia z Serwerem administracyjnym nie jest dostępny na urządzeniu. Port może być niedostępny na urządzeniu w następujących przypadkach:

  - Zdalne urządzenie jest podłączone do sieci lokalnej, która wykorzystuje mechanizm NAT.
  - Zdalne urządzenie jest częścią sieci lokalnej Serwera administracyjnego, ale jego port jest zamknięty przez zaporę sieciową.

- Udostępnianie pulpitu Windows. Podczas łączenia się z istniejącą sesją zdalnego pulpitu użytkownik sesji na urządzeniu otrzymuje od administratora żądanie dotyczące połączenia. W raportach utworzonych przez Kaspersky Security Center nie są zapisywane żadne informacje dotyczące zdalnych działań wykonywanych na urządzeniu ani wyniki tych działań.

  Administrator może skonfigurować audyt aktywności użytkownika na zdalnym urządzeniu klienckim. W trakcie audytu aplikacja zapisuje informacje o plikach na urządzeniu klienckim, który został otwarty i/lub zmodyfikowany przez administratora.

W celu nawiązania połączenia z pulpitem urządzenia klienckiego poprzez udostępnianie pulpitu Windows muszą być spełnione następujące warunki:

- Na stacji roboczej administratora powinien być zainstalowany system operacyjny Microsoft Windows Vista lub nowszy. Typ systemu operacyjnego urządzenia, na którym znajduje się Serwer administracyjny nie nakłada żadnych ograniczeń na łączenie poprzez udostępnianie pulpitu Windows.

  Aby sprawdzić, czy funkcja udostępniania pulpitu Windows znajduje się w posiadanej przez Ciebie edycji systemu Windows, upewnij się, że klucz CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} znajduje się w rejestrze systemu Windows.

- System Microsoft Windows Vista lub nowszy jest zainstalowany na urządzeniu klienckim.

- Kaspersky Security Center korzysta z licencji dla Zarządzania lukami i poprawkami.

W celu nawiązania połączenia z pulpitem urządzenia klienckiego poprzez udostępnianie pulpitu Windows:

1. W Konsoli administracyjnej opartej na MMC, w menu kontekstowym Serwera administracyjnego wybierz **Właściwości**.

2. W otwartym oknie właściwości Serwera administracyjnego przejdź do **Ustawienia połączenia z Serwerem administracyjnym** → **Porty połączenia**.

3. Upewnij się, że opcja **Otwórz port RDP dla Kaspersky Security Center Web Console** jest włączona.

4. W Kaspersky Security Center Web Console przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.

5. W polu **Bieżąca ścieżka** nad listą zarządzanych urządzeń kliknij łącze ścieżki.

6. W otwartym okienku po lewej stronie wybierz grupę administracyjną zawierającą urządzenie, do którego chcesz uzyskać dostęp.

7. Zaznacz pole obok nazwy urządzenia, do którego chcesz uzyskać dostęp.

8. Kliknij przycisk **Udostępnianie pulpitu Windows**.

   Zostanie otwarty Kreator Udostępnianie pulpitu Windows.

9. Kliknij przycisk **Pobierz**, aby pobrać narzędzie klsctunnel i zaczekaj, aż proces pobierania zostanie zakończony.

   Jeśli już posiadasz narzędzie klsctunnel, pomiń ten krok.

10. Kliknij przycisk **Dalej**.

11. Wybierz sesję na urządzeniu, z którym chcesz nawiązać połączenie, a następnie kliknij przycisk **Dalej**.

12. Na urządzeniu docelowym, w otwartym oknie dialogowym użytkownik musi zezwolić na sesję udostępniania pulpitu. W przeciwnym razie sesja nie będzie możliwa.

    Po potwierdzeniu przez użytkownika urządzenia sesji udostępniania pulpitu zostanie otwarta następna strona kreatora.

13. Kliknij przycisk **Kopiuj do schowka**, aby skopiować tekst z pola tekstowego. Ten tekst to Duży obiekt binarny (BLOB), który zawiera ustawienia wymagane do nawiązania połączenia między Serwerem administracyjnym a zarządzanym urządzeniem.

    BLOB jest ważny przez 3 minuty. Jeśli wygasł, wygeneruj nowy BLOB.

14. Uruchom narzędzie klsctunnel.

    Zostanie otwarte okno narzędzia.

15. Wklej skopiowany tekst do pola tekstowego.

16. Jeśli korzystasz z serwera proxy, zaznacz pole **Użyj serwera proxy**, a następnie określ ustawienia połączenia z serwerem proxy.

17. Kliknij przycisk **Otwórz port**.

    Udostępnianie pulpitu rozpocznie się w nowym oknie. Jeśli chcesz wejść w interakcję z urządzeniem, kliknij ikonę menu () w lewym górnym rogu okna, a następnie wybierz **Tryb interaktywny**.

Wybory urządzeń

Wybory urządzeń to narzędzie do filtrowania urządzeń zgodnie z określonymi warunkami. Możesz użyć wyborów urządzeń do zarządzania kilkoma urządzeniami: na przykład, aby przejrzeć raport dotyczący tylko tych urządzeń lub żeby przenieść wszystkie te urządzenia do innej grupy.

Kaspersky Security Center oferuje szeroki zakres *predefiniowanych wyborów* (na przykład: **Urządzenia ze stanem Krytyczny**, **Ochrona jest wyłączona**, **Wykryto aktywne zagrożenia**). Predefiniowanych wyborów nie można usunąć. Możesz także utworzyć i skonfigurować dodatkowe *wybory zdefiniowane przez użytkownika*.

W wyborach zdefiniowanych przez użytkownika możesz określić obszar wyszukiwania i wybrać wszystkie urządzenia, zarządzane urządzenia lub urządzenia nieprzypisane. Parametry wyszukiwania są określone w warunkach. W wyborze urządzeń możesz utworzyć kilka warunków z różnymi parametrami wyszukiwania. Na przykład, możesz utworzyć dwa warunki i określić różne zakresy IP w każdym z nich. Jeśli określono kilka warunków, wybór wyświetli urządzenia, które spełniają jakikolwiek warunek. Natomiast parametry wyszukiwania w obrębie warunku nakładają się na siebie. Jeśli zakres IP oraz nazwa zainstalowanej aplikacji są określone w warunku, wyświetlane będą tylko te urządzenia, na których jest zainstalowana aplikacja, a adres IP należy do określonego zakresu.

Przeglądanie listy urządzeń z wyboru urządzeń

Kaspersky Security Center umożliwia przeglądanie listy urządzeń z poziomu wyboru urządzenia.

Aby wyświetlić listę urządzeń z poziomu wyboru urządzenia:

1. W menu głównym przejdź do sekcji **Zasoby (urządzenia)** → **Wybory urządzeń** lub **Wykrywanie i wdrażanie** → **Wybory urządzeń**.

2. Na liście wyboru kliknij nazwę wybranego urządzenia.

   Na stronie wyświetlana jest tabela z informacjami o urządzeniach uwzględnionych w wyborze.

3. Dane tabeli urządzeń można grupować i filtrować w następujący sposób:

   - Kliknij ikonę ustawień (⚙), a następnie wybierz kolumny, które mają być wyświetlane w tabeli.
   - Kliknij ikonę filtrowania (▽), a następnie określ i zastosuj kryterium filtrowania w wywołanym menu.

     Zostanie wyświetlona przefiltrowana tabela urządzeń.

Można wybrać jedno lub kilka urządzeń i kliknąć przycisk **Nowe zadanie**, aby utworzyć odpowiednie zadanie, które zostanie zastosowane do tychże urządzeń.

Aby przenieść wybrane urządzenia do innej grupy administracyjnej, kliknij przycisk **Przenieś do grupy**, a następnie wybierz docelową grupę administracyjną.

Tworzenie kryteriów wyboru urządzeń

W celu utworzenia kryterium wyboru urządzeń:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Wybory urządzeń**.

   Zostanie wyświetlona lista wyborów urządzeń.

2. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Ustawienia wyboru urządzeń**.

3. Wprowadź nazwę nowego wyboru.

4. Określ grupę obejmującą urządzenia, które mają zostać uwzględnione w wyborze urządzeń:

   - **Wyszukaj dowolne urządzenia**— Wyszukiwanie urządzeń spełniających kryteria wyboru i uwzględnionych w grupach **Zarządzane urządzenia** lub **Urządzenia nieprzypisane**.
   - **Wyszukaj zarządzane urządzenia**— Wyszukiwanie urządzeń spełniających kryteria wyboru i uwzględnionych w grupie **Zarządzane urządzenia**.
   - **Wyszukaj nieprzypisane urządzenia**— Wyszukiwanie urządzeń spełniających kryteria wyboru i uwzględnionych w grupie **Urządzenia nieprzypisane**.

   Można włączyć pole wyboru **Uwzględnij dane z podrzędnych Serwerów administracyjnych**, aby umożliwić wyszukiwanie urządzeń spełniających kryteria wyboru i zarządzanych przez podrzędne Serwery administracyjne.

5. Kliknij przycisk **Dodaj**.

6. W oknie, które zostanie otwarte, określ warunki, które muszą być spełnione, aby uwzględnić urządzenia w tym wyborze, a następnie kliknij przycisk **OK**.

7. Kliknij przycisk **Zapisz**.

Wybór urządzeń zostanie utworzony i dodany do listy wyborów urządzeń.

Konfigurowanie kryteriów wyboru urządzeń

W celu skonfigurowania kryteriów wyboru urządzeń:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Wybory urządzeń**.

   Zostanie wyświetlona lista wyborów urządzeń.

2. Wybierz odpowiednie urządzenie zdefiniowane przez użytkownika i kliknij przycisk **Właściwości**.

   Zostanie otwarte okno **Ustawienia wyboru urządzeń**.

3. Na karcie **Ogólne** kliknij łącze **Nowy warunek**.

4. Określ warunki, jakie muszą zostać spełnione do uwzględnienia urządzeń w tym wyborze.

5. Kliknij przycisk **Zapisz**.

   Ustawienia zostaną zastosowane i zapisane.

Poniżej znajdują się opisy warunków przydzielania urządzeń do wyboru. Warunki są łączone przy użyciu operatora logicznego LUB: Wybór będzie zawierał urządzenia odpowiadające przynajmniej jednemu z wymienionych warunków.

Ogólne

W sekcji **Ogólne** możesz zmienić nazwę warunku wyboru oraz określić, czy ten warunek ma być odwrócony:

Odwróć warunek wyboru

Domyślnie opcja ta jest wyłączona.

Jeśli ta opcja jest włączona, określony warunek wyboru zostanie odwrócony. Wybór będzie zawierał wszystkie urządzenia, które nie spełniają warunku.

Poniższy przykład pokazuje logikę działania inwersji:

- **Warunek**: Na Twoim urządzeniu znajduje się system operacyjny z typem Linux i numerem kompilacji 00.0.000.
- **Warunek odwrócony**: Na urządzeniu znajduje się system operacyjny NIE z (typ Linux i numer kompilacji 00.0.000), co jest równoważne z następującym:

  Istnieje system operacyjny z typem NIE Linux LUB numerem kompilacji NIE 00.0.000.

W związku z tym wybór obejmie urządzenia z systemem operacyjnym, na przykład typu Windows i numerem kompilacji 00.0.000 lub typu Linux i dowolnym numerem kompilacji innym niż 00.0.000.

Infrastruktura sieci

W sekcji **Sieć** możesz określić kryteria, które będą wykorzystywane do uwzględniania urządzeń w wyborze zgodnie z ich danymi sieciowymi:

- **Nazwa urządzenia**

  Nazwa sieciowa systemu Windows (nazwa NetBIOS) urządzenia lub adres IPv4 lub IPv6.

- **Domena**

  Wyświetla wszystkie urządzenia znajdujące się w określonej domenie Windows.

- **Grupa administracyjna**

  Wyświetla urządzenia znajdujące się w określonej grupie administracyjnej.

- **Opis**

  Tekst wyświetlany w oknie właściwości urządzenia: pole **Opis** sekcji **Ogólne**.

W celu opisania tekstu w polu **Opis** możesz użyć następujących znaków:

- W słowie:
  - *****. Zastępuje dowolny wiersz dowolną liczbą znaków.

    Na przykład:

    Aby opisać słowa **Serwer** lub **Serwera**, możesz wpisać **Serwer***.

  - **?.** Zastępuje dowolny pojedynczy znak.

    Na przykład:

    Aby opisać słowa **Okno** lub **Okna**, możesz wpisać **Okn?**.

    Gwiazdka (*****) lub znak zapytania (**?**) nie mogą być używane jako pierwsze symbole wyszukiwanego słowa.

- W celu wyszukania kilku słów użyj:
  - Spacji. Wyświetla wszystkie urządzenia, których opisy zawierają dowolne z wymienionych słów.

    Na przykład:

    Aby odszukać frazę zawierającą słowa **Podrzędny** lub **Wirtualny**, wprowadź **Podrzędny Wirtualny** w tekście wyszukiwania.

  - **+**. Jeśli przed wyrazem wpisano znak „+”, wszystkie wyniki wyszukiwania będą zawierać ten wyraz.

    Na przykład:

    Aby odszukać frazę zawierającą zarówno **Podrzędny**, jak i **Wirtualny**, wprowadź **+Podrzędny+Wirtualny**.

  - **-**. Jeśli przed wyrazem wpisano znak „-”, żaden z wyników wyszukiwania nie będzie zawierać tego wyrazu.

    Na przykład:

    Aby odszukać frazę zawierającą **Podrzędny** i nie zawierającą **Wirtualny**, wprowadź **+Podrzędny-Wirtualny**.

  - **„<jakikolwiek tekst>”**. Tekst w cudzysłowach musi znajdować się w tekście.

    Na przykład:

    Aby odszukać frazę zawierającą kombinację słów **Podrzędny Serwer**, wprowadź **Podrzędny Serwer** w tekście wyszukiwania.

- **Zakres IP**

  Jeśli ta opcja jest włączona, możesz wprowadzić początkowy i końcowy adres IP z zakresu adresów IP, do którego muszą zostać włączone odpowiednie urządzenia.

  Domyślnie opcja ta jest wyłączona.

- **Zarządzane przez inny Serwer administracyjny**

  Wybierz jedną z następujących wartości:

  - **Tak**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich zarządzanych przez inne Serwery administracyjne. Te serwery różnią się od serwera, na którym konfigurujesz regułę przenoszenia urządzeń.
  - **Nie**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich zarządzanych przez bieżący Serwer administracyjny.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

W podsekcji **Sterownik domeny** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze na podstawie przynależności do domeny:

- **Urządzenie znajduje się w jednostce organizacyjnej domeny**

  Jeśli ta opcja jest włączona, wybór będzie zawierał urządzenia z jednostki organizacyjnej domeny określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

- **Urządzenie to należy do grupy zabezpieczeń domeny**

  Jeśli ta opcja jest włączona, wybór będzie zawierał urządzenia z grupy bezpieczeństwa domeny określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

W sekcji **Aktywność sieciowa** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich aktywnością sieciową:

- **Działa jako punkt dystrybucji**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Wybór zawiera urządzenia pełniące role punktów dystrybucji.
  - **Nie**. Urządzenia pełniące role punktów dystrybucji nie będą uwzględniane w wyborze.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Nie odłączaj od Serwera administracyjnego**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Włączona**. Wybór będzie zawierał urządzenia, na których zaznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Wyłączona**. Wybór będzie zawierał urządzenia, na których odznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Przełączanie profilu połączenia**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Wybór będzie zawierał urządzenia, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie**. Wybór nie będzie zawierał urządzeń, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Ostatnie połączenie z Serwerem administracyjnym**

  To pole ustawia kryterium wyszukiwania urządzeń według godziny ostatniego połączenia z Serwerem administracyjnym.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego zostało nawiązane ostatnie połączenie pomiędzy Agentem sieciowym zainstalowanym na urządzeniu klienckim a Serwerem administracyjnym. Wybór będzie zawierał urządzenia mieszczące się w określonym przedziale czasu.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- **Nowe urządzenia odnalezione podczas skanowania sieci**

  Wyszukiwanie nowych urządzeń, które zostały wykryte podczas przeszukiwania sieci w przeciągu kilku ostatnich dni.

  Jeśli ta opcja jest włączona, wybór będzie zawierał nowe urządzenia wykryte podczas wykrywania urządzeń w czasie określonym w polu **Okres wykrywania (dni)**.

  Jeśli ta opcja jest wyłączona, wybór będzie zawierał wszystkie urządzenia wykryte podczas wykrywania urządzeń.

  Domyślnie opcja ta jest wyłączona.

- **Dostępność urządzenia**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie widoczne w sieci.
  - **Nie**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie niewidoczne w sieci.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

W sekcji **Segmenty chmury** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o ich odpowiednie segmenty chmury:

- **Urządzenie znajduje się w segmencie chmury**

  Jeśli ta opcja jest włączona, można wybrać urządzenia z segmentów chmury AWS, Azure i Google.

  Jeśli włączono także opcję **Włączając obiekty potomne**, wyszukiwanie jest uruchamiane na wszystkich obiektach podrzędnych określonego segmentu.

  Wyniki wyszukiwania zawierają tylko urządzenia z wybranego segmentu.

- **Urządzenie wykryte przy pomocy API**

  Z listy rozwijalnej możesz wybrać, czy urządzenie jest wykrywane przez narzędzia API:

  - **Tak**. Urządzenie jest wykrywane za pomocą interfejsu API AWS, Azure lub Google.
  - **Nie**. Urządzenia nie można wykryć za pomocą interfejsu API AWS, Azure lub Google. Oznacza to, że urządzenie znajduje się poza środowiskiem chmury lub też w środowisku chmury, ale nie można go wykryć za pomocą interfejsu API.
  - Brak wartości. Ten warunek nie ma zastosowania.

Stany urządzenia

W sekcji **Stan zarządzanego urządzenia** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o opis stanu urządzeń z zarządzanej aplikacji:

- **Stan urządzenia**

  Lista rozwijalna, z której możesz wybrać jeden ze stanów urządzenia: *OK*, *Krytyczny*, or *Ostrzeżenie*.

- **Stan ochrony w czasie rzeczywistym**

  Lista rozwijalna, z której możesz wybrać stan ochrony w czasie rzeczywistym. Urządzenia z określonymi stanami ochrony w czasie rzeczywistym są uwzględniane w wyborze.

- **Opis stanu urządzenia**

  W tym polu możesz zaznaczyć pola obok warunków, które, jeśli są spełnione, spowodują przypisanie do urządzenia jednego z następujących stanów: *OK, Krytyczny* lub *Ostrzeżenie*.

W sekcji **Stan komponentów w zarządzanych aplikacjach** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o stan składników w zarządzanych aplikacjach:

- **Stan ochrony przed wyciekiem danych**

  Wyszukiwanie urządzeń według stanu Ochrona przed wyciekaniem danych (*Nieznana, Zatrzymano, Uruchamianie, Wstrzymana, Uruchamianie, Niepowodzenie*).

- **Stan ochrony serwerów współpracy**

  Wyszukiwanie urządzeń według stanu ochrony serwerów współpracy (*Nieznana*, *Zatrzymano*, *Uruchamianie, Wstrzymana*, *Uruchamianie*, *Niepowodzenie*).

- **Stan ochrony antywirusowej serwerów pocztowych**

  Wyszukiwanie urządzeń według stanu ochrony dla serwerów pocztowych (*Nieznana, Zatrzymano, Uruchamianie, Wstrzymana, Uruchamianie, Niepowodzenie*).

- **Stan czujnika Endpoint Sensor**

  Wyszukiwanie urządzeń według stanu komponentu Endpoint Sensor (*Nieznana, Zatrzymano, Uruchamianie, Wstrzymana, Uruchamianie, Niepowodzenie*).

W sekcji **Problemy mające wpływ na stan zarządzanych aplikacji** możesz określić kryteria, które będą używane do uwzględniania urządzeń do wyboru według listy możliwych problemów wykrytych przez zarządzaną aplikację. Jeśli przynajmniej jeden problem, który wybrałeś, istnieje na urządzeniu, urządzenie zostanie uwzględnione w wyborze. Jeśli wybierzesz problem wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego problemu na wszystkich listach.

Możesz zaznaczyć opcje dla opisów stanów z zarządzanej aplikacji. Po odebraniu tych stanów, urządzenia zostaną uwzględnione w wyborze. Jeśli wybierzesz stan wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego stanu na wszystkich listach.

Informacje o systemie

W sekcji **System operacyjny** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z typem systemu operacyjnego.

- **Typ platformy**

  Jeśli pole jest zaznaczone, możesz wybrać system operacyjny z listy. Urządzenia, na których zainstalowany jest określony system operacyjny, są uwzględniane w wynikach wyszukiwania.

- **Wersja dodatku Service Pack systemu operacyjnego**

  W tym polu możesz określić wersję pakietu systemu operacyjnego (w formacie *X.Y*), która będzie określać sposób stosowania reguły przenoszenia do urządzenia. Domyślnie nie jest zdefiniowana żadna wartość.

- **Typ systemu operacyjnego (bity)**

  Z listy rozwijalnej możesz wybrać architekturę swojego systemu operacyjnego, która określi sposób stosowania reguły przenoszenia do urządzenia (**Nieznany**, **x86**, **AMD64**, or **IA64**). Domyślnie, na liście nie wybrano żadnej opcji i tym samym nie zdefiniowano architektury systemu operacyjnego.

- **Kompilacja systemu operacyjnego**

  > To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Numer kompilacji systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować wyszukiwanie wszystkich numerów kompilacji, za wyjątkiem określonego.

- **Numer wersji systemu operacyjnego**

  > To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Identyfikator wydania systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy identyfikator wydania. Możesz także skonfigurować wyszukiwanie wszystkich numerów identyfikatorów wydania, za wyjątkiem określonego.

W sekcji **Maszyny wirtualne** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w zależności od tego, czy są to maszyny wirtualne lub czy są one częścią Virtual Desktop Infrastructure (VDI):

- **Jest maszyną wirtualną**

  Z listy rozwijalnej możesz wybrać następujące opcje:

  - **Nie zdefiniowano**.
  - **Nie**. Wyszukuje urządzenia, które nie są maszynami wirtualnymi.
  - **Tak**. Wyszukuje urządzenia, które są maszynami wirtualnymi.

- **Typ maszyny wirtualnej**

  Z listy rozwijalnej możesz wybrać producenta maszyny wirtualnej.

  Ta lista rozwijalna jest dostępna, jeśli wartość **Tak** lub **Nieważne** została wybrana na liście rozwijalnej **Jest maszyną wirtualną**.

- **Część Virtual Desktop Infrastructure**

  Z listy rozwijalnej możesz wybrać następujące opcje:

  - **Nie zdefiniowano**.
  - **Nie**. Wyszukuje urządzenia, które nie są częścią Virtual Desktop Infrastructure.
  - **Tak**. Wyszukuje urządzenia, które są częścią Virtual Desktop Infrastructure (VDI).

W sekcji **Rejestr sprzętu** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o sprzęt na nich zainstalowany:

Upewnij się, że narzędzie lshw jest zainstalowane na urządzeniach z systemem Linux, z których chcesz pobrać szczegółowe informacje o sprzęcie. Szczegóły dot. sprzętu przechwycone z maszyn wirtualnych mogą być niekompletne, w zależności od używanego hiperwizora.

- **Urządzenie**

  Z listy rozwijalnej możesz wybrać typ jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- **Producent**

  Z listy rozwijalnej możesz wybrać nazwę producenta jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- **Nazwa urządzenia**

  Nazwa urządzenia w sieci Windows. Urządzenie z określoną nazwą zostanie uwzględniony w wyborze.

- **Opis**

  Opis urządzenia lub sprzętu. Urządzenia z opisem określonym w tym polu zostaną uwzględnione w wyborze.

Opis urządzenia w dowolnym formacie może zostać wprowadzony w oknie właściwości tego urządzenia. Pole obsługuje wyszukiwanie pełnotekstowe.

- **Producent urządzenia**

  Nazwa producenta urządzenia. Urządzenia, które zostały wyprodukowane przez producenta określonego w tym polu, zostaną uwzględnione w wyborze.

  Nazwę producenta można wprowadzić w oknie właściwości urządzenia.

- **Numer seryjny**

  Cały sprzęt o numerze seryjnym określonym w tym polu zostanie uwzględniony w wyborze.

- **Numer ewidencyjny**

  Sprzęt o numerze inwentarzowym podanym w tym polu zostanie uwzględniony w wyborze.

- **Użytkownik**

  Cały sprzęt użytkownika określonego w tym polu zostanie uwzględniony w wyborze.

- **Lokalizacja**

  Lokalizacja urządzenia lub sprzętu (na przykład: w kwaterze głównej lub w oddziale firmy). Komputery lub inne urządzenia zainstalowane w lokalizacji określonej w tym polu zostaną uwzględnione w wyborze.

  Możesz opisać lokalizację urządzenia w dowolnym formacie w oknie właściwości tego urządzenia.

- **Częstotliwość taktowania procesora, w MHz, od**

  Minimalna częstotliwość taktowania procesora. Urządzenia z procesorem pasującym do zakresu częstotliwości taktowania określonego w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Częstotliwość taktowania procesora, w MHz, do**

  Maksymalna częstotliwość taktowania procesora. Urządzenia z procesorem pasującym do zakresu częstotliwości taktowania określonego w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Liczba rdzeni procesora wirtualnego, od**

  Minimalna liczba wirtualnych rdzeni CPU. Urządzenia z procesorem odpowiadającym zakresowi liczby wirtualnych rdzeni wg definicji w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Liczba rdzeni procesora wirtualnego, do**

  Maksymalna liczba wirtualnych rdzeni CPU. Urządzenia z procesorem odpowiadającym zakresowi liczby wirtualnych rdzeni wg definicji w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Pojemność dysku twardego, w GB, od**

  Minimalna pojemność dysku twardego w urządzeniu. Urządzenia z dyskami twardymi odpowiadającymi zakresowi określonemu w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Pojemność dysku twardego, w GB, do**

  Maksymalna pojemność dysku twardego w urządzeniu. Urządzenia z dyskami twardymi odpowiadającymi zakresowi określonemu w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Rozmiar pamięci RAM, w MB, od**

  Minimalny rozmiar pamięci RAM urządzenia. Urządzenia z pamięcią RAM o rozmiarze odpowiadającym zakresowi podanemu w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

- **Rozmiar pamięci RAM, w MB, do**

  Maksymalny rozmiar pamięci RAM urządzenia. Urządzenia z pamięcią RAM o rozmiarze odpowiadającym zakresowi podanemu w polach wejściowych (włącznie) zostaną uwzględnione w wyborze.

Informacje o oprogramowaniu innych firm

W sekcji **Rejestr aplikacji** możesz skonfigurować kryteria wyszukiwania urządzeń na podstawie aplikacji na nich zainstalowanych:

- **Nazwa aplikacji**

  Lista rozwijalna, z której możesz wybrać aplikację. Urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Wersja aplikacji**

  Pole, w którym możesz określić wersję wybranej aplikacji.

- **Producent**

  Lista rozwijalna, z której możesz wybrać producenta aplikacji zainstalowanej na urządzeniu.

- **Stan aplikacji**

  Lista rozwijalna, z której możesz wybrać stan aplikacji (*Zainstalowana*, *Nie zainstalowana*). Urządzenia, na których określona aplikacja została zainstalowana lub nie została zainstalowana, w zależności od wybranego stanu, zostaną uwzględnione w wyborze.

- **Wyszukaj według aktualizacji**

  Jeśli ta opcja jest włączona, wyszukiwanie będzie się odbywać z użyciem szczegółów aktualizacji dla aplikacji zainstalowanych na odpowiednich urządzeniach. Po zaznaczeniu pola, pola **Nazwa aplikacji**, **Wersja aplikacji** i **Stan aplikacji** zostaną zmienione na **Nazwa aktualizacji**, **Wersja aktualizacji** i **Stan**.

  Domyślnie opcja ta jest wyłączona.

- **Nazwa niekompatybilnej aplikacji zabezpieczającej**

  Lista rozwijalna, z której możesz wybrać aplikacje zabezpieczające firm trzecich. Podczas wyszukiwania, urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Znacznik aplikacji**

  Z listy rozwijalnej możesz wybrać znacznik aplikacji. Wszystkie urządzenia, na których są zainstalowane aplikacje z wybranym znacznikiem w opisie, zostają uwzględnione w wyborze urządzeń.

- **Zastosuj do urządzeń bez określonych znaczników**

  Jeśli ta opcja jest włączona, wybór obejmuje urządzenia z opisami, które nie zawierają żadnego z wybranych znaczników.

  Jeśli ta opcja jest wyłączona, kryterium nie zostanie zastosowane.

  Domyślnie opcja ta jest wyłączona.

W sekcji **Luki oraz aktualizacje** możesz określić kryteria, które będą wykorzystywane do uwzględniania urządzeń w wyborze zgodnie z ich źródłem Windows Update:

WUA został przełączony na Serwer administracyjny

Z listy rozwijalnej można wybrać jedną z następujących opcji wyszukiwania:

- **Tak**. Jeśli wybrano tę opcję, wyniki wyszukiwania będą uwzględniać urządzenia, które uzyskały aktualizacje poprzez Windows Update z Serwera administracyjnego.
- **Nie**. Jeśli wybrano tę opcję, wyniki będą uwzględniać urządzenia, które uzyskały aktualizacje za pośrednictwem Windows Update z innych źródeł.

Szczegóły aplikacji Kaspersky

W sekcji **Aplikacje Kaspersky** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o wybraną zarządzaną aplikację:

- **Nazwa aplikacji**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji Kaspersky.

  Lista zawiera tylko nazwy aplikacji z wtyczkami administracyjnymi zainstalowanych na stacji roboczej administratora.

  Jeśli żadna aplikacja nie została wybrana, kryterium nie będzie stosowane.

- **Wersja aplikacji**

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według numeru wersji aplikacji Kaspersky.

  Jeśli żaden numer wersji nie został określony, kryterium nie będzie stosowane.

- **Nazwa aktualizacji krytycznej**

  Lista rozwijalna, z której możesz wybrać stan aplikacji (*Zainstalowana*, *Nie zainstalowana*). Urządzenia, na których określona aplikacja została zainstalowana lub nie została zainstalowana, w zależności od wybranego stanu, zostaną uwzględnione w wyborze.

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji lub numeru pakietu aktualizacyjnego.

  Jeśli pole będzie puste, kryterium nie będzie stosowane.

- **Wybierz okres ostatniej aktualizacji modułów**

  Ta opcja może zostać użyta do ustawienia kryterium wyszukiwania urządzeń według godziny ostatniej aktualizacji modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego została wykonana ostatnia aktualizacja modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- **Urządzenie jest zarządzane przez Serwer administracyjny**

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić urządzenia zarządzane poprzez Kaspersky Security Center:

  - **Tak**. Aplikacja uwzględni w wyborze urządzenia zarządzane poprzez Kaspersky Security Center.
  - **Nie**. Aplikacja uwzględni w wyborze urządzenia, jeśli nie są one zarządzane przez Kaspersky Security Center.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- **Aplikacja zabezpieczająca jest zainstalowana**

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą:

  - **Tak**. Aplikacja uwzględni w wyborze wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą.
  - **Nie**. Aplikacja uwzględni w wyborze wszystkie urządzenia bez zainstalowanej aplikacji zabezpieczającej.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

W sekcji **Ochrona antywirusowa** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o ich stan ochrony:

- **Data opublikowania baz danych**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według daty opublikowania antywirusowej bazy danych. W polach do wprowadzania danych możesz określić przedział czasu, na podstawie którego wykonywane jest wyszukiwanie.

  Domyślnie opcja ta jest wyłączona.

- **Liczba wpisów w bazie danych**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według liczby wpisów w bazie danych. W polach wejściowych możesz określić niższe i wyższe wartości progowe wpisów w antywirusowej bazie danych.

  Domyślnie opcja ta jest wyłączona.

- **Ostatnie skanowanie**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według czasu ostatniego skanowania w poszukiwaniu złośliwego oprogramowania. W polach wejściowych możesz określić przedział czasu, w trakcie którego zostało wykonane ostatnie skanowanie w poszukiwaniu złośliwego oprogramowania.

  Domyślnie opcja ta jest wyłączona.

- **Wykryte zagrożenia**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według liczby wykrytych wirusów. W polach wejściowych możesz określić niższe i wyższe wartości progowe liczby wykrytych wirusów.

  Domyślnie opcja ta jest wyłączona.

W sekcji **Szyfrowanie** możesz skonfigurować kryteria uwzględniania urządzeń w oparciu o wybrany algorytm szyfrowania:

Algorytm szyfrowania

Algorytm blokowego szyfru symetrycznego AES (Advanced Encryption Standard). Z listy rozwijalnej możesz wybrać długość klucza szyfrowania (56-bitowy, 128-bitowy, 192-bitowy lub 256-bitowy).

Dostępne wartości: *AES56*, *AES128*, *AES192* i *AES256*.

Podsekcja **Składniki aplikacji** obejmuje listę składników tych aplikacji, które mają odpowiednie wtyczki administracyjne zainstalowane w Kaspersky Security Center Web Console.

W sekcji **Składniki aplikacji** możesz określić kryteria uwzględniania urządzeń – zgodnie ze statusami i numerami wersji komponentów, które odpowiadają wybieranej przez ciebie aplikacji:

- **Stan**

  Wyszukiwanie urządzeń zgodnie ze stanem komponentu wysłanym przez aplikację do Serwera administracyjnego. Możesz wybrać jeden z następujących stanów: *Nie dotyczy, Zatrzymane*, *Wstrzymane*, *Uruchamianie*, *Uruchomione, Niepowodzenie, Nie zainstalowane, Nie obsługiwane na podstawie licencji*. Jeśli wybrany komponent aplikacji zainstalowanej na zarządzanym urządzeniu posiada określony stan, urządzenie jest uwzględniane w wyborze urządzeń.

  Stany wysłane przez aplikacje:

  - *Zatrzymane*—komponent jest wyłączony i nie działa w tym momencie.
  - *Wstrzymane*—komponent został zawieszony, na przykład, po wstrzymaniu przez użytkownika ochrony w zarządzanej aplikacji.
  - *Uruchamianie*—komponent jest właśnie w procesie inicjalizacji.
  - *Uruchomione*—komponent jest włączony i działa poprawnie.
  - *Niepowodzenie* — Podczas działania składnika wystąpił błąd.
  - *Nie zainstalowano*—użytkownik nie wybrał komponentu do zainstalowania podczas konfigurowania niestandardowej instalacji aplikacji.
  - *Nie obsługiwany na podstawie licencji* — Licencja nie obejmuje wybranego składnika.

  W przeciwieństwie do pozostałych stanów, stan *Nie dotyczy* nie jest przekazywany poprzez aplikacje. Ta opcja pokazuje, że aplikacje nie posiadają informacji o wybranym stanie komponentu. Na przykład, to może mieć miejsce, gdy wybrany komponent nie należy do żadnej z aplikacji zainstalowanych na urządzeniu lub gdy urządzenie jest wyłączone.

- **Wersja**

  Wyszukiwanie urządzeń zgodnie z numerem wersji komponentu, który wybierasz na liście. Możesz wpisać numer wersji, na przykład `3.4.1.0`, a następnie określić, czy wybrany komponent musi posiadać równą, wcześniejszą lub nowszą wersję. Możesz także skonfigurować wyszukiwanie wszystkich wersji, za wyjątkiem określonej.

Znaczniki

W sekcji **Znaczniki** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o słowa kluczowe (znaczniki), które wcześniej zostały dodane do opisów zarządzanych urządzeń:

Zastosuj, jeśli co najmniej jeden określony znacznik jest zgodny

Jeśli ta opcja jest włączona, w wynikach wyszukiwania będą wyświetlane urządzenia z opisami, które zawierają przynajmniej jeden z wybranych znaczników.

Jeśli ta opcja jest wyłączona, w wynikach wyszukiwania będą wyświetlane tylko urządzeni z opisami, które zawierają wszystkie wybrane znaczniki.

Domyślnie opcja ta jest wyłączona.

Aby dodać tagi do kryterium, kliknij przycisk **Dodaj** i wybierz tagi, klikając pole wejściowe **Znacznik**. Określanie, czy urządzenia z wybranymi tagami mają być uwzględniane w wyborze urządzeń, czy też wykluczane.

- **Wszystkie urządzenia posiadające ten znacznik**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy zawierają wybrany znacznik. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

  Domyślnie opcja ta jest zaznaczona.

- **Wszystkie urządzenia nieposiadające tego znacznika**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy nie zawierają wybranego znacznika. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

Użytkownicy

W sekcji **Użytkownicy** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze według kont użytkowników, którzy logowali się do systemu operacyjnego.

- **Ostatni użytkownik zalogowany do systemu**

  Jeśli ta opcja jest włączona, można wybrać konto użytkownika do konfiguracji kryterium. Wyniki wyszukiwania obejmują urządzenia, na których określony użytkownik ostatnio logował się do systemu.

- **Użytkownik zalogowany do systemu co najmniej raz**

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik przynajmniej raz logował się do systemu.

Eksportowanie listy urządzeń z wyboru urządzeń

Kaspersky Security Center umożliwia zapisywanie informacji o urządzeniach z poziomu wyboru urządzenia i wyeksportowanie ich do pliku CSV lub TXT.

Aby wyeksportować listę urządzeń z poziomu wyboru urządzenia:

1. Otwórz tabelę z urządzeniami z wyboru urządzeń.
2. Użyj jednego z poniższych sposobów, aby wybrać urządzenia, które chcesz wyeksportować:
   - Aby wybrać określone urządzenia, zaznacz pola wyboru obok nich.
   - Aby wybrać wszystkie urządzenia z bieżącej strony tabeli, zaznacz pole wyboru w nagłówku tabeli urządzeń, a następnie zaznacz pole wyboru **Wybierz wszystko na bieżącej stronie**.
   - Aby wybrać wszystkie urządzenia z tabeli, zaznacz pole wyboru w nagłówku tabeli urządzeń, a następnie zaznacz pole wyboru **Wybierz wszystko**.
3. Kliknij przycisk **Eksportuj do pliku CSV** lub **Eksportuj do pliku TXT**. Wszystkie informacje o wybranych urządzeniach zawarte w tabeli zostaną wyeksportowane.

Należy pamiętać, że jeśli do tabeli urządzeń zastosowano kryterium filtrowania, zostaną wyeksportowane tylko przefiltrowane dane z wyświetlonych kolumn.

Usuwanie urządzeń z grup administracyjnych w wyborze

Podczas pracy z wyborami urządzeń możesz usunąć urządzenia z grup administracyjnych bezpośrednio w tym wyborze, bez przełączania do grup administracyjnych, z których te urządzenia mają być usunięte.

W celu usunięcia urządzeń z grup administracyjnych:

1. W menu głównym przejdź do sekcji **Zasoby (urządzenia)** → **Wybory urządzeń** lub **Wykrywanie i wdrażanie** → **Wybory urządzeń**.
2. Na liście wyboru kliknij nazwę wybranego urządzenia.

   Na stronie wyświetlana jest tabela z informacjami o urządzeniach uwzględnionych w wyborze.
3. Wybierz urządzenia, które chcesz usunąć, a następnie kliknij **Usuń**.

   Wybrane urządzenia zostaną usunięte z odpowiednich grup administracyjnych.

Znaczniki urządzeń

Kaspersky Security Center umożliwia *znakowanie* urządzeń. Znacznik to etykieta urządzenia i może zostać użyty do grupowania, opisywania lub wyszukiwania urządzeń. Znaczniki przydzielone do urządzeń mogą być użyte do tworzenia wyborów, wyszukiwania urządzeń i rozdzielania urządzeń pomiędzy grupami administracyjnymi.

Urządzenia można znakować ręcznie lub automatycznie. Jeśli chcesz oznakować pojedyncze urządzenie, możesz użyć oznaczania ręcznego. Automatyczne znakowanie jest wykonywane przez Kaspersky Security Center na jeden z następujących sposobów:

- Zgodnie z określonymi regułami znakowania.
- Przez aplikację.

Nie zalecamy używania różnych sposobów znakowania w celu przypisania tego samego znacznika. Przykładowo, jeśli znacznik jest przypisany przez regułę, nie zaleca się ręcznego przypisywania tego znacznika do urządzeń.

Jeśli znaczniki są przypisane przez reguły, urządzenia zostaną automatycznie oznakowane po spełnieniu określonych reguł. Każdemu znacznikowi odpowiada pojedyncza reguła. Reguły są stosowane do właściwości sieciowych urządzenia, systemu operacyjnego, aplikacji zainstalowanych na urządzeniu i innych właściwości urządzenia. Na przykład, jeśli posiadasz infrastrukturę hybrydową maszyn fizycznych, instancji Amazon EC2 oraz maszyn wirtualnych Microsoft Azure, możesz skonfigurować regułę, która przypisze znacznik `[Azure]` do wszystkich maszyn wirtualnych Microsoft Azure. Następnie możesz użyć tego znacznika podczas tworzenia wyboru urządzeń; pomoże to w sortowaniu wszystkich maszyn wirtualnych Microsoft Azure i przypisaniu do nich zadania.

Można dodać tylko jedną regułę automatycznego znakowania na znacznik. Jeśli utworzysz nową regułę dla tego samego znacznika, poprzednia zostanie zastąpiona.

Znacznik jest automatycznie usuwany z urządzenia w następujących przypadkach:

- Jeśli urządzenie przestanie spełniać warunki reguły, która przypisuje znacznik.
- Jeśli reguła, która przypisuje znacznik, jest wyłączona lub została usunięta.

Lista znaczników oraz lista reguł na każdym Serwerze administracyjnym są niezależne od wszystkich pozostałych Serwerów administracyjnych, w tym głównego Serwera administracyjnego lub podległych wirtualnych Serwerów administracyjnych. Reguła jest stosowana tylko do urządzeń z tego samego Serwera administracyjnego, na którym reguła jest tworzona.

Tworzenie znacznika urządzenia

W celu utworzenia znacznika urządzenia:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Znaczniki** → **Znaczniki urządzenia**.
2. Kliknij **Dodaj**.

   Zostanie otwarte okno nowego znacznika.
3. W polu **Znacznik** wprowadź nazwę znacznika.
4. Kliknij **Zapisz**, aby zachować zmiany.

Nowy znacznik pojawi się na liście znaczników urządzenia.

Zmienianie nazwy znacznika urządzenia

W celu zmiany nazwy znacznika urządzenia:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Znaczniki** → **Znaczniki urządzenia**.
2. Kliknij nazwę znacznika, którego nazwę chcesz zmienić.

   Zostanie otwarte okno właściwości znacznika.
3. W polu **Znacznik** zmień nazwę znacznika.
4. Kliknij **Zapisz**, aby zachować zmiany.

Zaktualizowany znacznik pojawi się na liście znaczników urządzenia.

Usuwanie znacznika urządzenia

W celu usunięcia znacznika urządzenia:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Znaczniki** → **Znaczniki urządzenia**.
2. Z listy wybierz znacznik urządzenia, który chcesz usunąć.
3. Kliknij przycisk **Usuń**.
4. W otwartym oknie kliknij **Tak**.

Znacznik urządzenia zostanie usunięty. Usunięty znacznik jest automatycznie usuwany ze wszystkich urządzeń, do których został przypisany.

Znacznik, który usunąłeś, nie zostanie usunięty automatycznie z reguł automatycznego znakowania. Po usunięciu znacznika, zostanie on przypisany do nowego urządzenia tylko wtedy, gdy urządzenie będzie spełniało wymagania reguły przypisującej znacznik.

Usunięty tag nie jest automatycznie usuwany z urządzenia, jeśli ten tag jest przypisany do urządzenia przez aplikację lub Agenta sieciowego. Aby zarządzać tymi znacznikami, użyj narzędzia klscflag.

Przeglądanie urządzeń, do których przypisano znacznik

W celu przejrzenia urządzeń, do których przypisywany jest znacznik:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Znaczniki** → **Znaczniki urządzenia**.
2. Kliknij odnośnik **Wyświetl urządzenia** obok znacznika, dla którego chcesz wyświetlić przypisane urządzenia.

   Zostaniesz przekierowany do sekcji **Zarządzane urządzenia** w menu głównym, gdzie urządzenia zostaną odfiltrowane według tagu, dla którego kliknąłeś odnośnik **Wyświetl urządzenia**.
3. Jeśli chcesz wrócić do listy znaczników urządzenia, kliknij przycisk **Wstecz** w swojej przeglądarce.

Po przejrzeniu urządzeń, do których przypisany jest znacznik, możesz utworzyć i przypisać nowy znacznik lub przypisać istniejący znacznik do innych urządzeń. W takim przypadku należy usunąć filtr według znacznika, wybrać urządzenia, a następnie przypisać znacznik.

Przeglądanie znaczników przydzielonych do urządzenia

W celu przejrzenia znaczników przydzielonych do urządzenia:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
2. Kliknij nazwę urządzenia, którego znaczniki chcesz przejrzeć.
3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Znaczniki**.

   Zostanie wyświetlona lista znaczników przypisanych do wybranego urządzenia. W kolumnie **Przypisany znacznik** możesz zobaczyć, w jaki sposób znacznik został przypisany.

W pasku narzędzi możesz wykonać następujące czynności:

- Przypisz inny znacznik do urządzenia.
- Usuń już przypisany znacznik.
- Wyświetl wszystkie znaczniki urządzenia, które znajdują się na Serwerze administracyjnym.

Nie można przeglądać przypisanych znaczników lokalnie na urządzeniu.

Ręczne oznaczanie urządzenia

W celu ręcznego przypisania znacznika do urządzenia:

1. Przejrzyj znaczniki przypisane do urządzenia, do którego chcesz przypisać inny znacznik.
2. Kliknij **Dodaj**.

3. W otwartym oknie wykonaj jedną z następujących czynności:

   - Aby utworzyć i przypisać nowy znacznik, wybierz **Utwórz nowy znacznik**, a następnie określ nazwę nowego znacznika.

   - Aby wybrać istniejący znacznik, wybierz **Przypisz istniejący znacznik**, a następnie, z listy rozwijalnej wybierz potrzebny znacznik.

4. Kliknij **OK**, aby zastosować zmiany.

5. Kliknij **Zapisz**, aby zachować zmiany.

Wybrany znacznik zostanie przypisany do urządzenia.

Usuwanie przydzielonego znacznika z urządzenia

W celu usunięcia znacznika z urządzenia:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.

2. Kliknij nazwę urządzenia, którego znaczniki chcesz przejrzeć.

3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Znaczniki**.

4. Zaznacz pole obok znacznika, który chcesz usunąć.

5. U góry listy kliknij przycisk **Wycofać przypisanie znacznika?**.

6. W otwartym oknie kliknij **Tak**.

Znacznik zostanie usunięty z urządzenia.

Znacznik urządzenia nieprzypisanego został usunięty. Jeśli chcesz, możesz usunąć go ręcznie.

Nie możesz ręcznie usunąć znaczników przypisanych do urządzenia przez aplikacje lub Agenta sieciowego. Aby zarządzać tymi znacznikami, użyj narzędzia klscflag.

Wyświetlanie reguł automatycznego oznaczania urządzeń

W celu wyświetlenia reguł automatycznego znakowania urządzeń:

Wykonaj jedną z poniższych czynności:

- W menu głównym przejdź do **Zasoby (urządzenia)** → **Znaczniki** → **Reguły automatycznego znakowania**.
- W menu głównym przejdź do **Zasoby (urządzenia)** → **Znaczniki** → **Znaczniki urządzenia**, and then click the **Ustaw reguły automatycznego znakowania**.
- Wyświetl znaczniki przypisane do urządzenia, a następnie kliknij przycisk **Ustaw reguły automatycznego znakowania**.

Zostanie wyświetlona lista reguł automatycznego znakowania urządzeń.

Edytowanie reguły automatycznego znakowania urządzeń

W celu edytowania reguły automatycznego znakowania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.
2. Kliknij nazwę reguły, którą chcesz edytować.

   Zostanie otwarte okno ustawień reguły.
3. Edytuj ogólne właściwości reguły:

   a. W polu **Nazwa reguły** zmień nazwę reguły.

   Nazwa nie może zawierać więcej niż 256 znaków.

   b. Wykonaj jedną z poniższych czynności:

   - Włącz regułę, ustawiając przełącznik w pozycji **Reguła włączona**.
   - Wyłącz regułę, ustawiając przełącznik w pozycji **Reguła wyłączona**.
4. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz dodać nowy warunek, kliknij przycisk **Dodaj** i w otwartym oknie określ ustawienia nowego warunku.
   - Jeśli chcesz edytować istniejący warunek, kliknij nazwę warunku, który chcesz edytować, a następnie edytuj ustawienia warunku.
   - Jeśli chcesz usunąć warunek, zaznacz pole obok nazwy warunku, który chcesz usunąć, a następnie kliknij **Usuń**.

5. Kliknij przycisk **OK** w oknie ustawień warunków.

6. Kliknij **Zapisz**, aby zachować zmiany.

Edytowana reguła zostanie wyświetlona na liście.

Tworzenie reguły automatycznego znakowania urządzeń

W celu utworzenia reguły automatycznego znakowania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.

2. Kliknij **Dodaj**.

   Zostanie otwarte okno ustawień nowej reguły.

3. Skonfiguruj ogólne właściwości reguły:

   a. W polu **Nazwa reguły** wprowadź nazwę reguły.

   Nazwa nie może zawierać więcej niż 256 znaków.

   b. Wykonaj jedną z poniższych czynności:

   - Włącz regułę, ustawiając przełącznik w pozycji **Reguła włączona**.
   - Wyłącz regułę, ustawiając przełącznik w pozycji **Reguła wyłączona**.

   c. W polu **Znacznik** wprowadź nazwę nowego znacznika urządzenia lub wybierz istniejące znaczniki urządzeń z listy.

   Nazwa nie może zawierać więcej niż 256 znaków.

4. W sekcji warunków kliknij przycisk **Dodaj**, aby dodać nowy warunek.

   Zostanie otwarte okno ustawień nowego warunku.

5. Wprowadź nazwę warunku.

   Nazwa nie może zawierać więcej niż 256 znaków. Nazwa musi być unikatowa w obrębie reguły.

6. Skonfiguruj wyzwalanie reguły zgodnie z następującymi warunkami. Możesz określić kilka warunków.

   - **Sieć**—właściwości sieci urządzenia, takie jak nazwa urządzenia w sieci Windows lub uwzględnienie urządzenia w domenie lub podsieci IP.

     > Jeśli dla bazy danych używanej z Kaspersky Security Center ustawione jest sortowanie z rozróżnianiem wielkości liter, zachowaj wielkość liter podczas określania nazwy DNS urządzenia. W przeciwnym razie reguła automatycznego tagowania nie będzie działać.

   - **Aplikacje**—obecność Agenta sieciowego na urządzeniu oraz typ, wersja i architektura systemu operacyjnego.
   - **Maszyny wirtualne**—urządzenie należy do określonego typu maszyny wirtualnej.

- **Sterownik domeny**—Obecność urządzenia w jednostce organizacyjnej Active Directory i członkostwo urządzenia w grupie Active Directory.
- **Rejestr aplikacji**—obecność aplikacji różnych producentów na urządzeniu.

7. Kliknij **OK**, aby zachować zmiany.

   Jeśli to konieczne, dla jednej reguły możesz ustawić kilka warunków. W tej sytuacji znacznik zostanie przypisany do urządzenia, jeśli spełnia przynajmniej jeden warunek.

8. Kliknij **Zapisz**, aby zachować zmiany.

Nowo utworzona reguła jest wymuszona na urządzeniach zarządzanych przez wybrany Serwer administracyjny. Jeśli ustawienia urządzenia spełniają warunki reguły, do urządzenia zostanie przydzielony znacznik.

Później reguła będzie stosowana w następujących przypadkach:

- Automatycznie i okresowo, w zależności od obciążenia na serwerze
- Po edytowaniu reguły
- Jeśli ręcznie uruchamiasz regułę
- Po wykryciu przez Serwer administracyjny zmian w ustawieniach urządzenia, które spełnia warunki reguły lub w ustawieniach grupy, która zawiera to urządzenie

Możesz utworzyć kilka reguł znakowania. Do jednego urządzenia może zostać przypisanych kilka znaczników, jeśli utworzyłeś kilka reguł znakowania i jeśli odpowiednie warunki tych reguł są spełnione w tym samym czasie. Listę wszystkich przydzielonych znaczników można przejrzeć we właściwościach urządzenia.

Uruchamianie reguł automatycznego znakowania urządzeń

Jeśli reguła jest uruchomiona, znacznik określony we właściwościach tej reguły zostanie przypisany do urządzeń, które spełniają warunki określone we właściwościach tej samej reguły. Możesz uruchamiać tylko aktywne reguły.

W celu uruchomienia reguł automatycznego znakowania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.
2. Zaznacz pola obok aktywnych reguł, które chcesz uruchomić.
3. Kliknij przycisk **Uruchom regułę**.

Wybrane reguły zostały uruchomione.

Usuwanie reguły automatycznego oznaczania urządzeń

W celu usunięcia reguły automatycznego oznaczania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.
2. Zaznacz pole obok reguły, którą chcesz usunąć.

3. Kliknij **Usuń**.

4. W otwartym oknie ponownie kliknij **Usuń**.

Wybrana reguła została usunięta. Znacznik, który został określony we właściwościach tej reguły, został wypisany ze wszystkich urządzeń, do których został przypisany.

Znacznik urządzenia nieprzypisanego został usunięty. Jeśli chcesz, możesz usunąć go ręcznie.

Zarządzanie znacznikami urządzeń za pomocą narzędzia klscflag

Aby przypisać zestaw znaczników do urządzenia, należy uruchomić narzędzie klscflag na urządzeniu klienta, do którego mają zostać przypisane znaczniki.

Narzędzie klscflag nadpisuje istniejące znaczniki przypisane do urządzenia. Oznacza to, że możesz dodawać lub usuwać znaczniki, określając w poleceniu żądany zestaw znaczników. Narzędzie nie posiada osobnych poleceń do dodawania lub usuwania poszczególnych znaczników. Zamiast tego modyfikujesz cały zestaw znaczników.

Podczas określania nazw znaczników w poleceniach typu klscflag zaleca się stosowanie spójnego podejścia polegającego na przykład na pisaniu wielkimi literami. Używanie samych wielkich liter może pomóc uniknąć potencjalnych problemów ze znacznikami, które różnią się jedynie wielkością liter, w zależności od konfiguracji systemu DBMS.

Aby przypisać znaczniki do swojego urządzenia za pomocą narzędzia klscflag:

1. Uruchom wiersz poleceń systemu Windows, korzystając z uprawnień administratora, a następnie zmień bieżący katalog na inny za pomocą narzędzia klscflag. Narzędzie klscflag znajduje się w folderze, w którym zainstalowany jest Agent sieciowy. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\NetworkAgent.

2. Uruchom jedno z następujących poleceń:

   - Aby przypisać zestaw znaczników:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NAZWA ZNACZNIKA 1\",\"NAZWA ZNACZNIKA 2\",\"NAZWA ZNACZNIKA 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     gdzie `[\"NAZWA ZNACZNIKA 1\",\"NAZWA ZNACZNIKA 2\",\"NAZWA ZNACZNIKA 3\"]` to lista znaczników, które chcesz przypisać do swojego urządzenia.

     Jeżeli pozostawisz nawiasy kwadratowe puste, spowoduje to usunięcie wszystkich znaczników z urządzenia:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

   - Aby przypisać nowy znacznik do istniejącego zestawu znaczników:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NOWA NAZWA ZNACZNIKA\",\"NAZWA ZNACZNIKA 1\",\"NAZWA ZNACZNIKA 2\",\"NAZWA ZNACZNIKA 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     gdzie `NAZWA NOWEGO ZNACZNIKA` to nazwa znacznika, który chcesz przypisać do swojego urządzenia, a `NAZWA ZNACZNIKA 1`, `NAZWA ZNACZNIKA 2`, `NAZWA ZNACZNIKA 3` to nazwy znaczników już przypisanych do urządzenia.

- Aby usunąć konkretny znacznik bez usuwania innych znaczników już przypisanych do urządzenia, uruchom polecenie ze zaktualizowanym zestawem znaczników.

  Na przykład, jeśli Twoje obecne znaczniki to `NAZWA ZNACZNIKA 1`, `NAZWA ZNACZNIKA 2`, `NAZWA ZNACZNIKA 3` i chcesz usunąć `NAZWA ZNACZNIKA 2`, uruchom następujące polecenie:

  ```
  klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NAZWA ZNACZNIKA 1\",\"NAZWA ZNACZNIKA 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
  ```

3. Uruchom ponownie usługę Agenta sieciowego.

   Narzędzie klscflag przypisuje określone znaczniki do Twojego urządzenia.

4. Aby mieć pewność, że narzędzie klscflag pomyślnie przypisało określone znaczniki, wyświetl znaczniki przypisane do urządzenia.

Alternatywnie możesz ręcznie przypisać znaczniki urządzeń.

Zasady i profile zasad

W Kaspersky Security Center Web Console możesz tworzyć zasady dla aplikacji Kaspersky. Ta sekcja opisuje zasady i profile zasad, a także zawiera instrukcje dotyczące ich tworzenia i modyfikowania.

Informacje o zasadach i profilach zasad

Zasada to zbiór ustawień aplikacji Kaspersky, które są stosowane do grupy administracyjnej i jej podgrup. Możesz zainstalować kilka aplikacji Kaspersky na urządzeniach należących do grupy administracyjnej. Kaspersky Security Center zapewnia jedną zasadę dla każdej aplikacji Kaspersky w grupie administracyjnej. Zasada ma jeden z następujących stanów (patrz poniższa tabela):

Stan zasady

Stan	Opis
Aktywny	Bieżąca zasada, która jest stosowana do urządzenia. W każdej grupie administracyjnej dla aplikacji Kaspersky może być aktywna tylko jedna zasada. Urządzenia stosują wartości ustawień aktywnej zasady aplikacji Kaspersky.
Nieaktywna	Zasada, która nie jest obecnie stosowana do urządzenia.
Profil użytkownika mobilnego	Jeżeli ta opcja jest zaznaczona, zasada stanie się aktywna, gdy urządzenie znajdzie się poza siecią korporacyjną.

Zasady działają zgodnie z następującymi regułami:

- Dla jednej aplikacji można skonfigurować kilka zasad z różnymi wartościami.
- Tylko jedna zasada może być aktywna dla bieżącej aplikacji.
- Możesz aktywować nieaktywną zasadę, gdy wystąpi określone zdarzenie. Na przykład możesz wymusić bardziej rygorystyczne ustawienia ochrony antywirusowej podczas epidemii wirusów.
- Zasada może mieć zasady podrzędne.

Zazwyczaj można używać zasad w celu przygotowania się na sytuacje awaryjne, takie jak atak wirusa. Na przykład, jeśli wystąpi atak za pośrednictwem dysków flash, można aktywować zasadę blokującą dostęp do dysków flash. W takim przypadku bieżąca aktywna zasada automatycznie stanie się nieaktywna.

Aby zapobiec utrzymywaniu wielu zasad, na przykład, gdy przy różnych okazjach zakłada się zmianę tylko kilku ustawień, można użyć profili zasad.

Profil zasad to nazwany podzbiór wartości ustawień zasad, który zastępuje wartości ustawień zasady. Profil zasad wpływa na efektywne tworzenie ustawień na zarządzanym urządzeniu. *Obowiązujące ustawienia* to zbiory ustawień zasad, ustawień profilu zasad i lokalnych ustawień aplikacji, które są aktualnie zastosowane do urządzenia.

Profile zasad działają zgodnie z następującymi regułami:

- Profil zasad zaczyna obowiązywać, gdy wystąpi określony warunek aktywacji.
- Profile zasad zawierają wartości ustawień, które różnią się od ustawień zasad.
- Aktywacja profilu zasad zmienia obowiązujące ustawienia zarządzanego urządzenia.
- Zasada może zawierać maksymalnie 100 profili zasad.

Informacje o blokadzie i zablokowanych ustawieniach

Każde ustawienie zasady ma ikonę przycisku blokady (). Poniższa tabela przedstawia stany przycisków blokady:

Stany przycisków blokady

Stan	Opis
Nie zdefiniowano	Jeśli obok ustawienia jest wyświetlana otwarta kłódka, a przycisk przełącznika jest wyłączony, ustawienie nie jest określone w zasadzie. Użytkownik może zmienić te ustawienia w interfejsie zarządzanej aplikacji. Tego typu ustawienia nazywane są *odblokowanymi*.
Wymuś	Jeśli obok ustawienia jest wyświetlana zamknięta kłódka, a przycisk przełącznika jest włączony, ustawienie jest stosowane do urządzeń, na których zasada jest wymuszana. Użytkownik nie może zmodyfikować wartości tych ustawień w interfejsie zarządzanej aplikacji. Tego typu ustawienia nazywane są *zablokowanymi*.

Zdecydowanie zalecamy zamknięcie blokad dla ustawień zasad, które chcesz zastosować na zarządzanych urządzeniach. Odblokowane ustawienia zasady można ponownie przypisać przez ustawienia aplikacji Kaspersky na zarządzanym urządzeniu.

Możesz użyć przycisku blokady, aby wykonać następujące czynności:

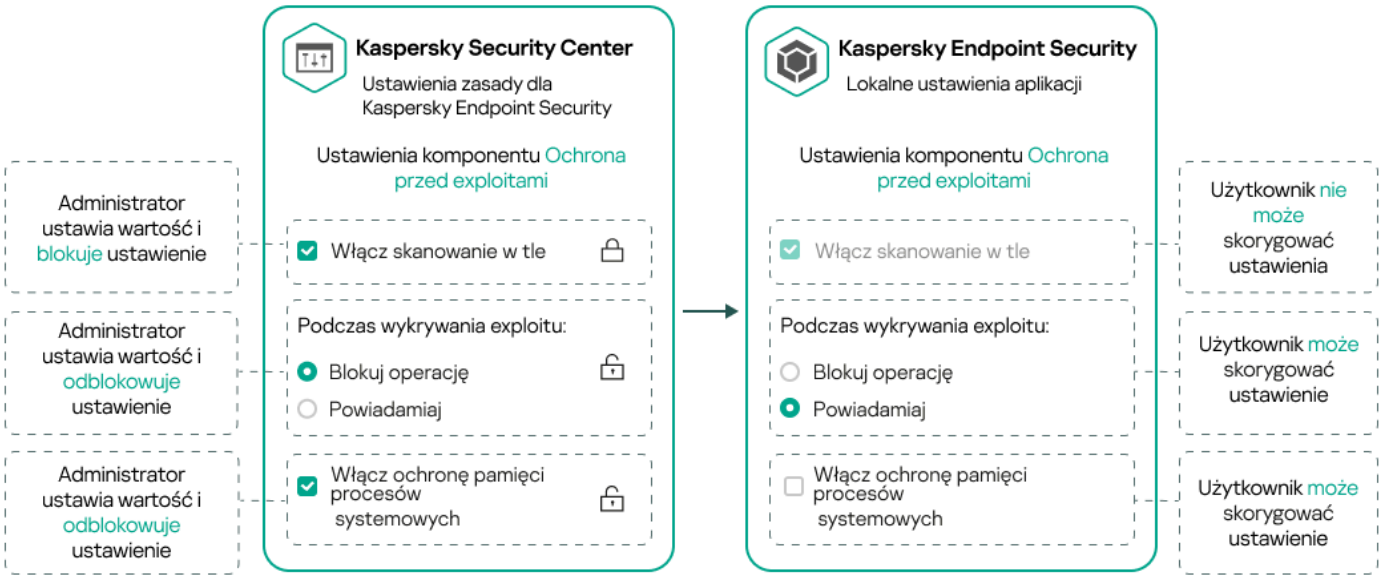
- Blokowanie ustawień dla zasady podgrupy administracyjnej
- Blokowanie ustawień aplikacji Kaspersky na zarządzanym urządzeniu

W ten sposób zablokowane ustawienie jest używane do implementacji obowiązujących ustawień na zarządzanym urządzeniu.

Proces skutecznego wdrażania ustawień obejmuje następujące działania:

- Zarządzane urządzenie stosuje wartości ustawień aplikacji Kaspersky.
- Zarządzane urządzenie stosuje zablokowane wartości ustawień zasady.

Zasada i zarządzana aplikacja Kaspersky zawierają ten sam zbiór ustawień. Po skonfigurowaniu ustawień zasady, wartości ustawień aplikacji Kaspersky ulegają zmianie na zarządzanym urządzeniu. Użytkownik nie może dostosować zablokowanych ustawień na zarządzanym urządzeniu (patrz rysunek poniżej):



Blokady i ustawienia aplikacji Kaspersky

Dziedziczenie zasad i profili zasad

Ta sekcja zawiera informacje o hierarchii i dziedziczeniu zasad oraz profilach zasad.

Hierarchia zasad

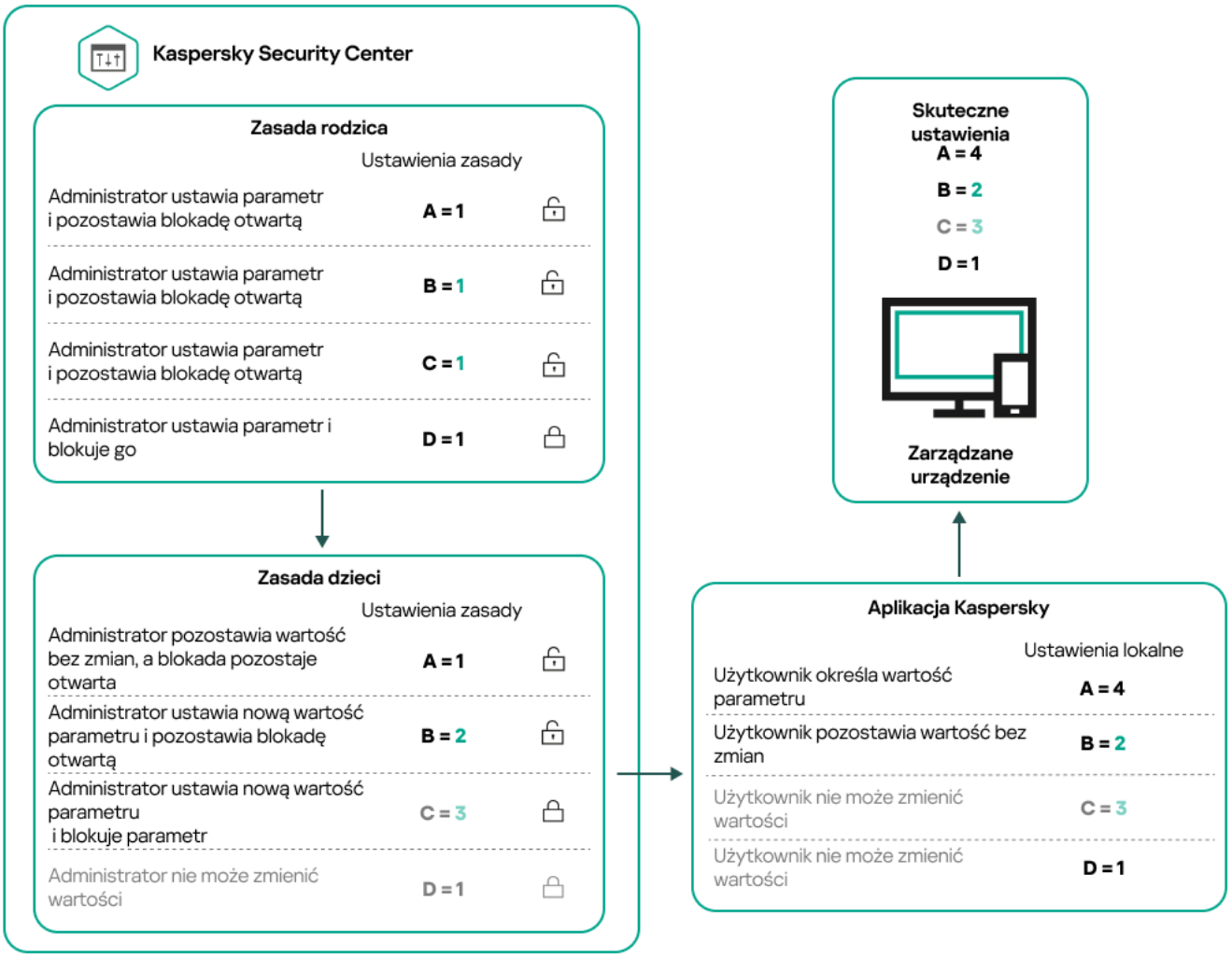
Jeśli różne urządzenia wymagają różnych ustawień, możesz zorganizować je w grupy administracyjne.

Możesz określić zasadę dla pojedynczej grupy administracyjnej. Ustawienia zasad mogą być *dziedziczone*. Dziedziczenie oznacza odbieranie wartości ustawień zasad w podgrupach (grupach podrzędnych) z zasady grupy administracyjnej wyższego poziomu (nadrzędnej).

Dalej zasada dla grupy nadrzędnej jest też zwana *zasadą nadrzędną*. Dalej zasada dla podgrupy (grupy podrzędnej) jest też zwana *zasadą podrzędną*.

Domyślnie co najmniej jedna grupa zarządzane urządzenia istnieje na Serwerze administracyjnym. Jeśli chcesz utworzyć grupy niestandardowe, są one tworzone jako podgrupy (grupy podrzędne) w ramach grupy zarządzane urządzenia.

Zasady tej samej aplikacji oddziałują na siebie zgodnie z hierarchią grup administracyjnych. Zablokowane ustawienia z zasady grupy administracyjnej wyższego poziomu (nadrzędnej) spowodują ponowne przypisanie wartości ustawień zasad podgrupy (patrz rysunek poniżej).



Hierarchia zasad

Profile zasad w hierarchii zasad

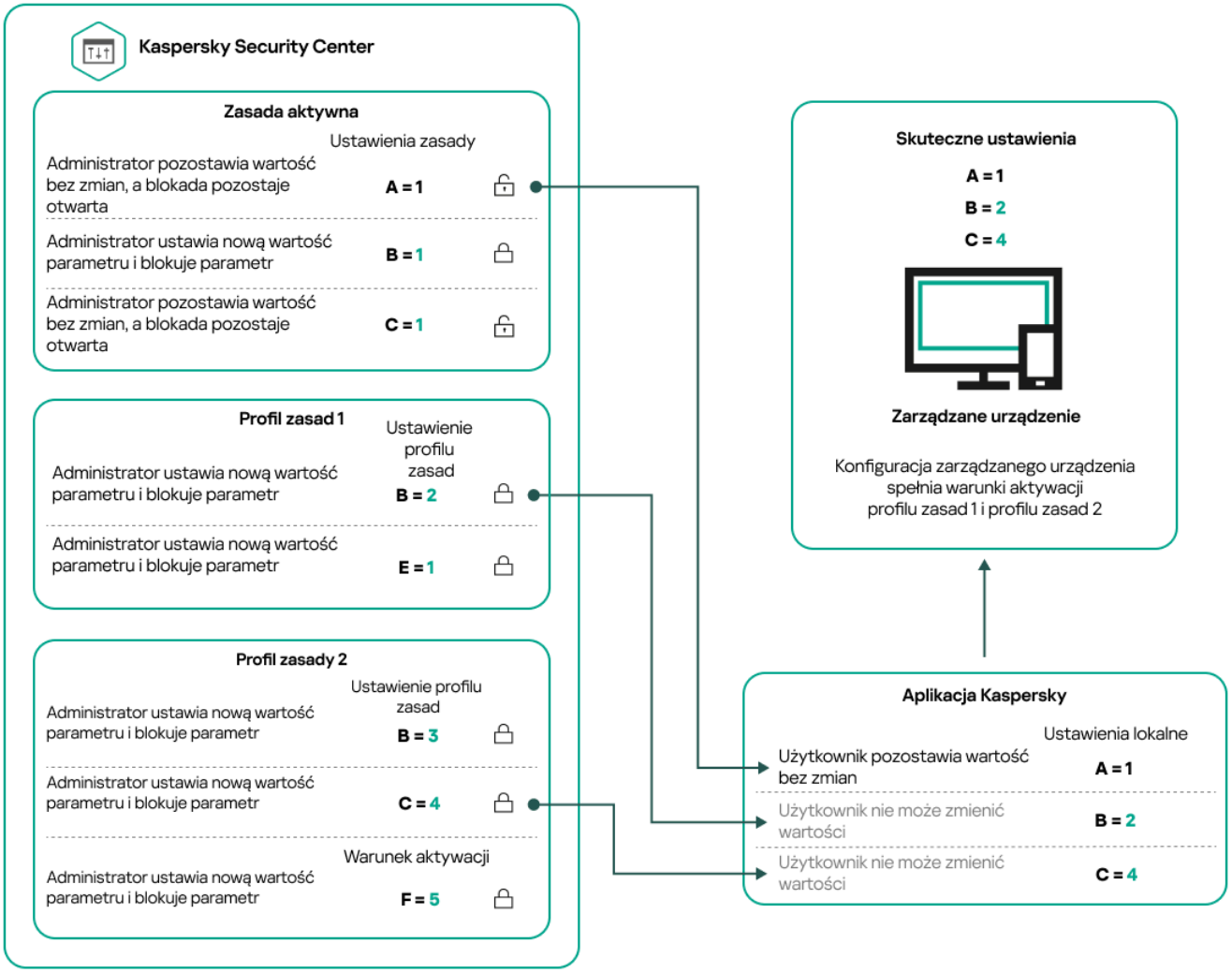
Profile zasad mają następujące warunki przypisywania priorytetów:

- Pozycja profilu na liście profili zasad wskazuje jego priorytet. Możesz zmienić priorytet profilu zasad. Najwyższa pozycja na liście oznacza najwyższy priorytet (patrz rysunek poniżej).



Definicja priorytetu profilu zasad

- Warunki aktywacji profili zasad nie są od siebie zależne. Jednocześnie można aktywować kilka profili zasad. Jeśli kilka profili zasad wpływa na to samo ustawienie, urządzenie przyjmuje wartość ustawienia z profilu zasad o najwyższym priorytecie (patrz rysunek poniżej).

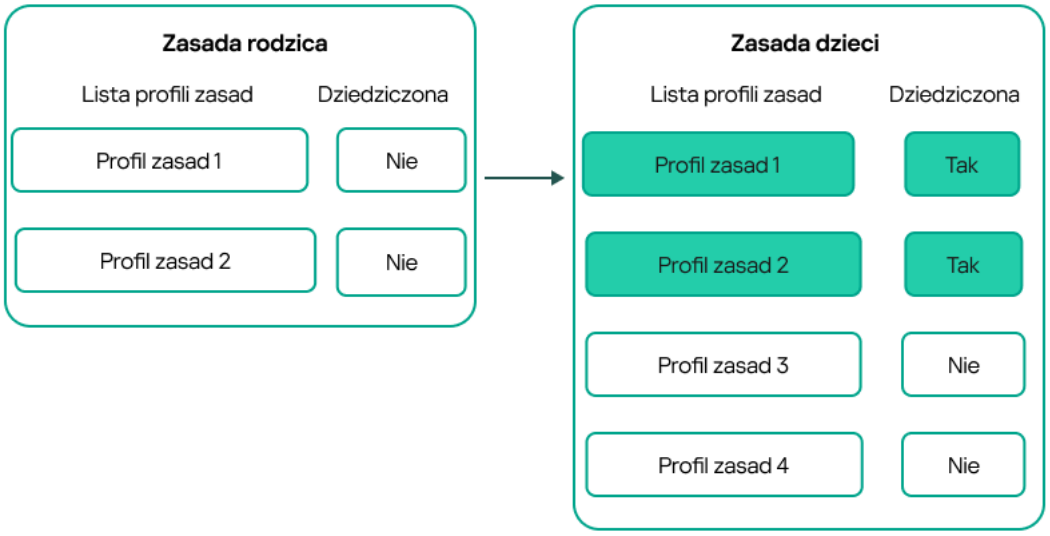


Konfiguracja zarządzanego urządzenia spełnia warunki aktywacji kilku profili zasad

Profile zasad w hierarchii dziedziczenia

Profile zasad z zasad różnych poziomów hierarchii spełniają następujące warunki:

- Zasada niższego poziomu dziedziczy profile zasad z zasady wyższego poziomu. Profil zasad odziedziczony z zasady wyższego poziomu uzyskuje wyższy priorytet niż poziom oryginalnego profilu zasad.
- Nie można zmienić priorytetu odziedziczonego profilu zasad (zobacz poniższy rysunek).



Dziedziczenie profili zasad

Profile zasad o tej samej nazwie

Jeśli istnieją dwie zasady o tych samych nazwach na różnych poziomach hierarchii, te zasady działają zgodnie z następującymi regułami:

- Ustawienia zablokowane i warunek aktywacji profilu zasad wyższego poziomu zmieniają ustawienia i warunek aktywacji profilu zasad niższego poziomu (patrz rysunek poniżej).



Profil podrzędny dziedziczy wartości ustawień z nadrzędnego profilu zasad

- Ustawienia odblokowane i warunek aktywacji profilu zasad wyższego poziomu nie zmieniają ustawień i warunku aktywacji profilu zasad niższego poziomu.

Implementacja ustawień na zarządzanym urządzeniu

Implementację obowiązujących ustawień na zarządzanym urządzeniu można opisać w następujący sposób:

- Wartości wszystkich ustawień, które nie zostały zablokowane, są pobierane z zasady.
- Następnie są nadpisywane wartościami ustawień zarządzanej aplikacji.
- Następnie stosowane są zablokowane wartości ustawień z obowiązującej zasady. Zablokowane wartości ustawień zmieniają wartości odblokowanych obowiązujących ustawień.

Zarządzanie zasadami

Ta sekcja opisuje zarządzanie zasadami i zawiera informacje o przeglądaniu listy zasad, tworzeniu zasady, modyfikowaniu zasady, kopiowaniu zasady, przenoszeniu zasady, wymuszonej synchronizacji, przeglądaniu wykresu stanu dystrybucji zasad i usuwaniu zasady.

Przeglądanie listy zasad

Możesz przejrzeć listy zasad utworzonych dla Serwera administracyjnego lub dla dowolnej grupy administracyjnej.

W celu wyświetlenia listy zasad:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Hierarchia grup**.
2. W strukturze grupy administracyjnej należy wybrać grupę administracyjną, dla której chcesz przejrzeć listę zasad.

Lista zasad zostanie wyświetlona w postaci tabeli. Jeśli nie ma zasad, tabela jest pusta. Możesz wyświetlać lub ukrywać kolumny tabeli, zmieniać ich kolejność, przeglądać tylko wiersze, które zawierają określoną przez Ciebie wartość, lub korzystać z wyszukiwania.

Tworzenie zasady

Możesz tworzyć zasady, a także modyfikować i usuwać istniejące zasady.

W celu utworzenia zasady:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Wybierz grupę administracyjną dla której chcesz utworzyć zasadę:
   - Dla grupy głównej.
     W takim przypadku możesz przejść do następnego kroku.
   - Dla grupy podrzędnej:
     a. Kliknij odnośnik bieżącej ścieżki znajdujący się u góry okna.
     b. W otwartym panelu kliknij odnośnik z nazwą żądanej grupy podrzędnej.

   Bieżąca ścieżka zmienia się, aby odzwierciedlić wybraną grupę podrzędną.
3. Kliknij **Dodaj**.
   Zostanie otwarte okno **Wybierz aplikację**.
4. Wybierz aplikację, dla której chcesz utworzyć zasadę.

5. Kliknij **Dalej**.

   Zostanie otwarte okno ustawień nowej zasady na zakładce **Ogólne**.

6. Jeśli chcesz, zmień domyślną nazwę, domyślny stan oraz domyślne ustawienia dziedziczenia zasady.

7. Wybierz zakładkę **Ustawienia aplikacji**.

   Lub kliknij **Zapisz** i zakończ działanie. Zasada pojawi się na liście zasad i będziesz mógł w późniejszym czasie edytować jego ustawienia.

8. Na zakładce **Ustawienia aplikacji**, w lewej części okna wybierz żądaną kategorię, a w prawej części okna zmień ustawienia zasady. Możesz edytować ustawienia zasady w każdej kategorii (sekcja).

   Zestaw ustawień zależy od aplikacji, dla której tworzysz zasadę. Więcej informacji można znaleźć w:

   - Konfiguracja Serwera administracyjnego
   - Ustawienia zasady Agenta sieciowego
   - Dokumentacja do Kaspersky Endpoint Security for Windows

   Szczegółowe informacje dotyczące ustawień innych aplikacji zabezpieczających można znaleźć w dokumentacji dla odpowiedniej aplikacji.

   Podczas edytowania ustawień możesz kliknąć **Anuluj**, aby anulować ostatnie działanie.

9. Kliknij **Zapisz**, aby zapisać zasadę.

Zasada zostanie wyświetlona na liście zasad.

Modyfikowanie zasady

W celu zmodyfikowania zasady:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.

2. Kliknij zasadę, którą chcesz zmodyfikować.

   Zostanie otwarte okno ustawień zasady.

3. Określ ustawienia główne oraz ustawienia aplikacji, dla której tworzysz zasadę. Więcej informacji można znaleźć w:

   - Konfiguracja Serwera administracyjnego
   - Ustawienia zasady Agenta sieciowego
   - Dokumentacja do Kaspersky Endpoint Security for Windows

   Szczegółowe informacje dotyczące ustawień innych aplikacji zabezpieczających można znaleźć w dokumentacji dla tej aplikacji.

4. Kliknij **Zapisz**.

Zmiany wprowadzone w zasadzie zostaną zapisane we właściwościach zasady i pojawią się w sekcji **Historia rewizji**.

Ogólne ustawienia zasady

Ogólne

Na zakładce **Ogólne** możesz zmodyfikować stan zasady oraz określić dziedziczenie ustawień zasady:

- W sekcji **Stan zasady** możesz wybrać jeden z trybów zasady:
  - **Aktywny**

    Jeśli wybrano tę opcję, zasada jest aktywna.

    Domyślnie opcja ta jest zaznaczona.
  - **Użytkownik mobilny**

    Jeżeli ta opcja jest zaznaczona, zasada stanie się aktywna, gdy urządzenie znajdzie się poza siecią korporacyjną.
  - **Nieaktywny**

    Jeśli ta opcja jest zaznaczona, zasada stanie się nieaktywna, ale wciąż będzie przechowywana w folderze **Zasady**. Jeśli jest to wymagane, zasadę można aktywować.
- W grupie ustawień **Dziedziczenie ustawień** możesz skonfigurować dziedziczenie zasady:
  - **Dziedzicz ustawienia z zasady nadrzędnej**

    Jeśli ta opcja jest włączona, wartości ustawień zasady są dziedziczone z zasady grupy najwyższego poziomu, są więc zablokowane.

    Domyślnie opcja ta jest włączona.
  - **Wymuś dziedziczenie ustawień w zasadach podrzędnych**

    Jeśli ta opcja jest włączona, po zastosowaniu zmian w zasadzie zostaną wykonane następujące czynności:
    - Wartości ustawień zasady zostaną rozesłane do zasad podgrup administracyjnych, czyli do zasad podrzędnych.
    - Opcja **Dziedzicz ustawienia z zasady nadrzędnej** będzie automatycznie włączona w podsekcji **Dziedziczenie ustawień** sekcji **Ogólne** okna właściwości każdej zasady podrzędnej.

    Jeśli ta opcja jest włączona, ustawienia zasad podrzędnych są zablokowane.

    Domyślnie opcja ta jest wyłączona.

Konfiguracja zdarzenia

Zakładka **Konfiguracja zdarzenia** umożliwia skonfigurowanie zapisywania zdarzeń oraz powiadamiania o zdarzeniach. Zdarzenia są grupowane według istotności na następujących zakładkach:

- **Krytyczny**

  Sekcja **Krytyczny** nie jest wyświetlana we właściwościach zasad Agenta sieciowego.
- **Błąd funkcjonalny**

- **Ostrzeżenie**
- **Informacja**

W każdej sekcji, lista wyświetla typy zdarzeń oraz domyślny czas przechowywania zdarzeń na Serwerze administracyjnym (w dniach). Kliknięcie typu zdarzenia umożliwia określenie następujących ustawień:

- **Rejestracja zdarzenia**

  Możesz określić ilość dni przechowywania zdarzenia oraz wybrać miejsce przechowywania zdarzenia:

  - **Eksportuj do systemu SIEM przez Dziennik systemu**
  - **Przechowuj w systemowym dzienniku zdarzeń urządzenia**
  - **Przechowuj w systemowym dzienniku zdarzeń Serwera administracyjnego**

- **Powiadomienia o zdarzeniu**

  Możesz wybrać, jeśli chcesz być powiadamiany o zdarzeniu w jeden z następujących sposobów:

  - **Powiadom przez e-mail**
  - **Powiadom przez SMS**
  - **Powiadom, uruchamiając plik wykonywalny lub skrypt**
  - **Powiadom przez SNMP**

  Domyślnie, używane są ustawienia powiadamiania, określone na zakładce Właściwości Serwera administracyjnego (takie, jak adres odbiorcy). Jeśli chcesz, możesz zmienić te ustawienia na zakładkach: **E-mail**, **SMS** i **Plik wykonywalny do uruchomienia**.

Historia rewizji

Zakładka **Historia rewizji** umożliwia przeglądanie listy rewizji zasady i wycofanie zmian wprowadzonych do zasady, jeśli to konieczne.

Włączanie i wyłączanie opcji dziedziczenia zasady

Aby włączyć lub wyłączyć opcję dziedziczenia w zasadzie:

1. Otwórz wymaganą zasadę.
2. Otwórz zakładkę **Ogólne**.

3. Włącz lub wyłącz dziedziczenie zasad:

   - Jeśli włączysz opcję **Dziedzicz ustawienia z zasady nadrzędnej** w zasadzie podrzędnej i administrator zablokuje niektóre ustawienia w zasadzie nadrzędnej, wówczas nie będzie można zmienić tych ustawień w zasadzie podrzędnej.

   - Jeśli wyłączysz opcję **Dziedzicz ustawienia z zasady nadrzędnej** w zasadzie podrzędnej, wówczas możesz zmienić wszystkie ustawienia w zasadzie podrzędnej nawet wtedy, gdy niektóre ustawienia są zablokowane w zasadzie nadrzędnej.

   - Jeśli włączysz opcję **Wymuś dziedziczenie ustawień w zasadach podrzędnych** w grupie nadrzędnej, spowoduje to włączenie opcji **Dziedzicz ustawienia z zasady nadrzędnej** dla każdej zasady podrzędnej. W tym przypadku nie możesz wyłączyć tej opcji dla żadnej zasady podrzędnej. Wszystkie ustawienia, które są zablokowane w zasadzie nadrzędnej, są dziedziczone w grupach podrzędnych w sposób wymuszony i nie możesz zmienić tych ustawień w grupach podrzędnych.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany, lub kliknij przycisk **Anuluj**, aby odrzucić zmiany.

Domyślnie, opcja **Dziedzicz ustawienia z zasady nadrzędnej** jest włączona dla nowej zasady.

Jeśli zasada zawiera profile, wszystkie zasady podrzędne dziedziczą te profile.

Kopiowanie zasady

Możesz skopiować zasady z jednej grupy administracyjnej do innej.

W celu skopiowania zasady do innej grupy administracyjnej:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.

2. Zaznacz pole obok zasady (lub zasad), którą (które) chcesz skopiować.

3. Kliknij przycisk **Kopiuj**.

   W prawej części okna pojawi się drzewo grup administracyjnych.

4. Z drzewa wybierz grupę docelową, czyli grupę, do której chcesz skopiować zasadę (zasady).

5. W dolnej części okna kliknij przycisk **Kopiuj**.

6. Kliknij **OK**, aby potwierdzić działanie.

Zasada (zasady) zostanie skopiowana do grupy docelowej ze wszystkimi swoimi profilami. Stan każdej skopiowanej zasady w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

Jeżeli zasada z nazwą podobną do nazwy nowo przeniesionej zasady znajduje się już w grupie docelowej, do nazwy nowo przeniesionej zasady zostanie dodany przyrostek (<kolejny numer>), na przykład: (1).

Przenoszenie zasady

Możesz przenieść zasady z jednej grupy administracyjnej do innej. Na przykład, chcesz usunąć grupę, ale chcesz używać jej zasad dla innej grupy. W tym przypadku można przenieść zasadę ze starszej grupy do nowej zanim usuniesz starszą grupę.

Podczas przenoszenia zasady do innej grupy administracyjnej historia rewizji zasady jest usuwana. Karta **Historia rewizji** wyświetla informacje tylko o ostatniej zmianie.

W celu przeniesienia zasady do innej grupy administracyjnej:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Zaznacz pole obok zasady (lub zasad), którą (które) chcesz przenieść.
3. Kliknij przycisk **Przenieś**.

   W prawej części okna pojawi się drzewo grup administracyjnych.
4. Z drzewa wybierz grupę docelową, czyli grupę, do której chcesz przenieść zasadę (lub zasady).
5. W dolnej części okna kliknij przycisk **Przenieś**.
6. Kliknij **OK**, aby potwierdzić działanie.

   Jeśli zasada nie jest dziedziczona z grupy źródłowej, zostaje przeniesiona do grupy docelowej ze wszystkimi swoimi profilami. Stan zasady w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

   Jeśli zasada jest dziedziczona z grupy źródłowej, pozostanie w grupie źródłowej. Zostanie skopiowana do grupy docelowej ze wszystkimi swoimi profilami. Stan zasady w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

Jeżeli zasada z nazwą podobną do nazwy nowo przeniesionej zasady znajduje się już w grupie docelowej, do nazwy nowo przeniesionej zasady zostanie dodany przyrostek (<kolejny numer>), na przykład: (1).

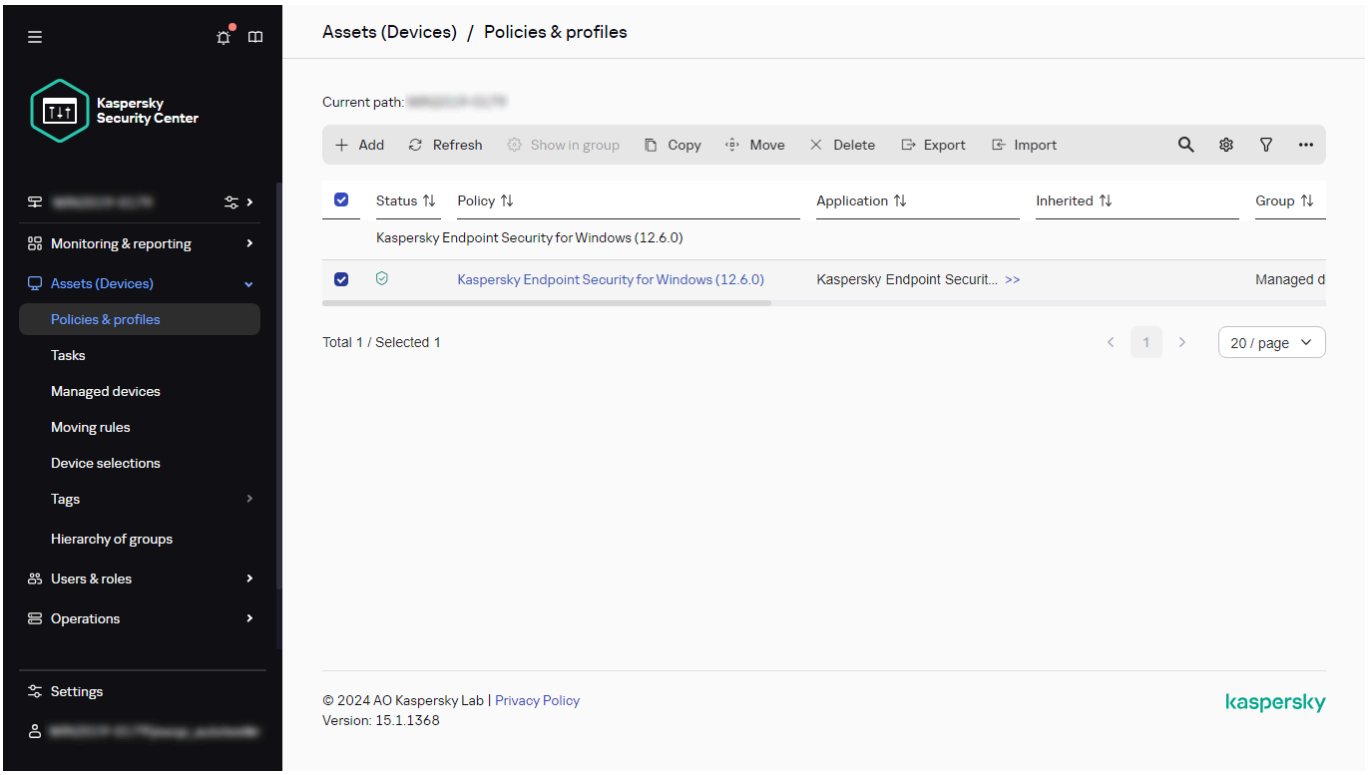
Eksportowanie zasady

Kaspersky Security Center umożliwia zapisanie profilu, jego ustawień i profili zasad w pliku KLP. Możesz użyć tego pliku KLP do zaimportowania zapisanej zasady zarówno do Kaspersky Security Center Windows, jak i Kaspersky Security Center Linux.

W celu wyeksportowania zasady:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Zaznacz pole obok zasady, którą chcesz wyeliminować.

   Nie można jednocześnie eksportować wielu zasad. Jeśli wybierzesz więcej niż jedną zasadę, przycisk **Eksportuj** będzie nieaktywny.



3. Kliknij przycisk **Eksportuj**.

4. W otwartym oknie **Zapisz jako** określ nazwę i ścieżkę dostępu pliku zasady. Kliknij przycisk **Zapisz**.

   Okno **Zapisz jako** jest wyświetlane tylko wtedy, gdy korzystasz z przeglądarki Google Chrome, Microsoft Edge lub Opera. Jeśli używasz innej przeglądarki, plik zasady jest automatycznie zapisywany w folderze **Pobrane**.

Importowanie zasady

Kaspersky Security Center umożliwia importowanie zasady z pliku KLP. Plik KLP zawiera wyeksportowaną zasadę, jej ustawienia oraz profile zasad.

W celu zaimportowania zasady:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.

2. Kliknij przycisk **Importuj**.

3. Kliknij przycisk **Przeglądaj**, aby wybrać plik zasad, który chcesz zaimportować.

4. W otwartym oknie określ ścieżkę do pliku zasady KLP, a następnie kliknij przycisk **Otwórz**. Pamiętaj, że możesz wybrać tylko jeden plik zasady.

   Rozpoczyna się przetwarzanie zasady.

5. Po pomyślnym przetworzeniu zasady wybierz Grupa administracyjna, do których chcesz przypisać zasadę.

6. Kliknij przycisk **Zakończone**, aby zakończyć import zasad.

Pojawi się powiadomienie z wynikami importu. Jeśli zasada została pomyślnie zaimportowana, możesz kliknąć łącze **Szczegóły**, aby wyświetlić właściwości zasady.

Po pomyślnym imporcie zasada zostanie wyświetlona na liście zasad. Importowane są również ustawienia i profile zasad. Niezależnie od statusu zasady, który został wybrany podczas eksportu, importowana zasada jest nieaktywna. Możesz zmienić stan zasady we właściwościach zasady.

Jeżeli nowo importowana zasada ma nazwę identyczną z nazwą istniejącej zasady, nazwa importowanej zasady jest rozszerzana o indeks **(<następny numer kolejny>)**, na przykład: **(1)**, **(2)**.

Przeglądanie wykresu stanu dystrybucji zasad

W Kaspersky Security Center możesz przejrzeć stan zastosowania zasady na każdym urządzeniu w wykresie stanu dystrybucji zasady.

W celu wyświetlenia stanu dystrybucji zasady na każdym urządzeniu:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Zaznacz pole obok nazwy zasady, dla której chcesz przejrzeć stan dystrybucji na urządzeniach.
3. W wyświetlonym menu wybierz odnośnik **Dystrybucja**.

   Zostanie otwarte okno **Wyniki dystrybucji <nazwa zasady>**.
4. W otwartym oknie **Wyniki dystrybucji <nazwa zasady>** zostanie wyświetlony **Opis stanu** zasady.

Możesz zmienić liczbę wyników wyświetlanych na liście z dystrybucją zasady. Maksymalna liczba urządzeń to 100 000.

W celu zmiany liczby urządzeń wyświetlanych na liście z wynikami dystrybucji zasady:

1. W menu głównym przejdź do ustawień konta i wybierz **Opcje interfejsu**.
2. W sekcji **Ogranicz urządzenia wyświetlane w wynikach dystrybucji zasady** wprowadź liczbę urządzeń (do 100 000).

   Domyślnie ustawiona jest liczba 5000.
3. Kliknij **Zapisz**.

   Ustawienia zostaną zapisane i zastosowane.

Usuwanie zasady

Możesz usunąć zasadę, jeśli już jej nie potrzebujesz. Możesz usunąć tylko tą zasadę, która nie jest dziedziczona w określonej grupie administracyjnej. Jeśli zasada została odziedziczona, możesz ją usunąć tylko w grupie wyższego poziomu, dla której została utworzona.

W celu usunięcia zasady:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Zaznacz pole obok zasady, który chcesz usunąć, a następnie kliknij **Usuń**.

   Przycisk **Usuń** stanie się niedostępny (przyciemniony), jeśli wybierzesz zasadę dziedziczoną.
3. Kliknij **OK**, aby potwierdzić działanie.

Zasada jest usuwana ze wszystkimi swoimi profilami.

Zarządzanie profilami zasad

Ta sekcja opisuje zarządzanie profilami zasad i zawiera informacje o wyświetlaniu profili zasad, zmienianiu priorytetu profili zasad, tworzeniu profili zasad, modyfikowaniu profili zasad, kopiowaniu profili zasad, tworzeniu reguł aktywacji profili zasad i usuwaniu profili zasad.

Przeglądanie profili zasad

W celu przejrzenia profili zasad:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Kliknij nazwę zasady, której profile chcesz przejrzeć.

   Okno właściwości zasady zostanie otwarte na wybranej zakładce **Ogólne**.
3. Otwórz zakładke **Profile zasad**.

Lista profili zasad zostanie wyświetlona w postaci tabeli. Jeśli zasada nie zawiera profili, pojawi się pusta tabela.

Zmiana priorytetu profilu zasad

W celu zmiany priorytetu profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.
2. Na zakładce **Profile zasad** zaznacz pole obok profilu zasad, dla którego chcesz zmienić priorytet.
3. Ustaw nową pozycję profilu zasad na liście, klikając **Nadaj priorytet** lub **Usuń priorytet**.

   Im wyżej profil zasad znajduje się na liście, tym wyższy jego priorytet.
4. Kliknij przycisk **Zapisz**.

Priorytet wybranego profilu zasad zostanie zmieniony i zastosowany.

Tworzenie profilu zasad

W celu utworzenia profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad. Jeśli zasada nie zawiera profili, pojawi się pusta tabela.

2. Kliknij **Dodaj**.

3. Jeśli chcesz, zmień domyślną nazwę oraz domyślne ustawienia dziedziczenia profilu.

4. Wybierz zakładkę **Ustawienia aplikacji**.

   Lub kliknij **Zapisz** i zakończ działanie. Utworzony profil pojawia się na liście profili zasad i będzie można w późniejszym czasie zmienić ustawienia.

5. Na zakładce **Ustawienia aplikacji**, w lewej części okna wybierz żądaną kategorię, a w prawej części okna zmień ustawienia profilu. Możesz zmienić ustawienia profilu zasad w każdej kategorii (sekcja).

   Podczas edytowania ustawień możesz kliknąć **Anuluj**, aby anulować ostatnie działanie.

6. Kliknij **Zapisz**, aby zapisać profil.

Profil pojawi się na liście profili zasad.

Modyfikowanie profilu zasad

Możliwość modyfikowania profilu zasad jest dostępna tylko dla profili Kaspersky Endpoint Security for Windows.

W celu zmodyfikowania profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.

2. Na zakładce **Profile zasad** kliknij profil zasady, który chcesz zmodyfikować.

   Zostanie otwarte okno właściwości profilu zasad.

3. Skonfiguruj profil w oknie właściwości:

   - Jeśli to konieczne, na zakładce **Ogólne** zmień nazwę profilu i włącz lub wyłącz profil.
   - Edytuj reguły aktywacji profilu.
   - Edytuj ustawienia aplikacji.

   Szczegółowe informacje dotyczące ustawień aplikacji zabezpieczających można znaleźć w dokumentacji dla odpowiedniej aplikacji.

4. Kliknij **Zapisz**.

Zmodyfikowane ustawienia zostaną zastosowane po zsynchronizowaniu urządzenia z Serwerem administracyjnym (jeśli profil zasad jest aktywny) lub po wyzwoleniu reguły aktywacji (jeśli profil zasad jest nieaktywny).

Kopiowanie profilu zasad

Możesz skopiować profil zasad do bieżącego profilu lub do innego profilu, na przykład, jeśli chcesz mieć identyczne profile dla różnych zasad. Kopiowania możesz użyć także, jeśli chcesz mieć dwa lub więcej profili, które różnią się tylko małą liczbą ustawień.

W celu skopiowania profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad. Jeśli zasada nie zawiera profili, pojawi się pusta tabela.

2. Na zakładce **Profile zasad** wybierz profil zasady, który chcesz skopiować.

3. Kliknij **Kopiuj**.

4. W otwartym oknie wybierz zasadę, do której chcesz skopiować profil.

   Profil zasady możesz skopiować do tej samej zasady lub do zasady, którą określiłeś.

5. Kliknij **Kopiuj**.

   Profil zasad został skopiowany do wybranej zasady. Nowo skopiowany profil uzyskuje najniższy priorytet. Jeśli skopiujesz profil do tej samej zasady, nazwa nowo skopiowanego profilu zostanie poszerzona o indeks (), na przykład: (1), (2).

Później będziesz mógł zmienić ustawienia profilu, w tym jego nazwę i priorytet; w tym przypadku oryginalny profil zasady nie zostanie zmieniony.

Tworzenie reguły aktywacji profilu zasad

W celu utworzenia reguły aktywacji profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.

2. Na zakładce **Profile zasad** kliknij profil zasad, dla którego chcesz utworzyć regułę aktywacji.

   Jeśli lista profili zasad jest pusta, możesz utworzyć profil zasad.

3. Na zakładce **Reguły aktywacji** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno z regułami aktywacji profilu zasad.

4. Określ nazwę reguły.

5. Zaznacz pola obok warunków, które mają wpływać na aktywację tworzonego profilu zasad:

- **Główne reguły dotyczące aktywacji profilu zasad**

  Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od stanu trybu offline urządzenia, regułę połączenia z Serwerem administracyjnym, a także znaczniki przypisywane do urządzenia.

  Dla tej opcji, w następnym kroku określ:

  - **Stan urządzenia**

    Określ warunek obecności urządzenia w sieci:

    - **Online**— Urządzenie jest w sieci, więc Serwer administracyjny jest dostępny.
    - **Offline**— Urządzenie jest w sieci zewnętrznej, co oznacza, że Serwer administracyjny nie jest dostępny.
    - **N/D**—Kryterium nie będzie stosowane.

  - **Reguła dla połączenia Serwera administracyjnego jest aktywna na tym urządzeniu**

    Wybierz warunek aktywacji profilu zasad (czy reguła jest wykonywana) i wybierz nazwę reguły.

    Reguła definiuje lokalizację sieciową urządzenia dla połączenia z Serwerem administracyjnym, którego warunki muszą być spełnione (lub nie muszą być spełnione) dla aktywacji profilu zasad.

    Opis lokalizacji sieciowej urządzeń dla połączenia z Serwerem administracyjnym może zostać utworzony lub skonfigurowany w regule przełączania Agenta sieciowego.

- **Reguły dla określonego właściciela urządzenia**

  Dla tej opcji, w następnym kroku określ:

  - **Właściciel urządzenia**

    Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu zgodnie z jego właścicielem. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

    - Urządzenie należy do określonego właściciela (znak „=").
    - Urządzenie nie należy do określonego właściciela (znak „#").

      Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić właściciela urządzenia, gdy opcja jest włączona. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

  - **Właściciel urządzenia należy do wewnętrznej grupy bezpieczeństwa**

    Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu według przynależności właściciela do wewnętrznej grupy zabezpieczeń Kaspersky Security Center. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

    - Właściciel urządzenia jest członkiem określonej grupy bezpieczeństwa (znak „=").
    - Właściciel urządzenia nie jest członkiem określonej grupy bezpieczeństwa (znak „#").

      Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić grupę zabezpieczeń Kaspersky Security Center. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- **Reguły dla specyfikacji sprzętowej**

  Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od ilości pamięci oraz liczby procesów logicznych.

  Dla tej opcji, w następnym kroku określ:

  - **Rozmiar pamięci RAM, w MB**

    Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu według ilości pamięci RAM dostępnej na tym urządzeniu. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

    - Rozmiar pamięci RAM jest mniejszy niż określona wartość (znak „<").
    - Rozmiar pamięci RAM jest większy niż określona wartość (znak „>").

    Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić ilość pamięci RAM na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

  - **Liczba procesorów logicznych**

    Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu według liczby procesorów logicznych na tym urządzeniu. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

    - Liczba procesorów logicznych na urządzeniu jest mniejsza niż lub równa określonej wartości (znak „<").
    - Liczba procesorów logicznych na urządzeniu jest większa niż lub równa określonej wartości (znak „>").

    Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić liczbę procesorów logicznych na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- **Reguły dla przypisywania roli**

  Dla tej opcji, w następnym kroku określ:

  Aktywuj profil zasad określoną rolą właściciela urządzenia

  Wybierz te opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu w zależności od roli właściciela. Dodaj rolę ręcznie z listy istniejących ról.

  Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium.

- **Reguły dla użycia znaczników**

  Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od znaczników przypisanych do urządzenia. Możesz aktywować profil zasad dla urządzeń, które posiadają znaczniki lub które ich nie posiadają.

  Dla tej opcji, w następnym kroku określ:

  - **Znacznik**

    Na liście znaczników możesz określić regułę uwzględniania urządzenia w profilu zasad, zaznaczając pola obok odpowiednich znaczników.

    Możesz dodać nowe znaczniki do listy, wprowadzając je w polu nad listą i klikając przycisk **Dodaj**.

Profil zasad obejmuje urządzenia z opisami zawierającymi wszystkie zaznaczone tagi. Jeśli pola nie są zaznaczone, kryterium nie jest stosowane. Domyślnie pola te nie są zaznaczone.

- **Zastosuj do urządzeń bez określonych znaczników**

  Włącz tę opcje, jeśli musisz odwrócić wybór znaczników.

  Jeśli ta opcja jest włączona, profil zasad obejmuje urządzenia z opisami, które nie zawierają żadnego z wybranych znaczników. Jeśli ta opcja jest wyłączona, kryterium nie zostanie zastosowane.

  Domyślnie opcja ta jest wyłączona.

- **Reguły dotyczące używania Active Directory**

  Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od obecności urządzenia w jednostce organizacyjnej Active Directory (OU) lub członkostwa urządzenia (lub jego właściciela) w grupie zabezpieczeń Active Directory.

  Dla tej opcji, w następnym kroku określ:

  - **Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory**

    Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu, którego właściciel jest członkiem określonej grupy zabezpieczeń. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

  - **Członkostwo urządzenia w grupie zabezpieczeń Active Directory**

    Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

  - **Alokacja urządzenia w jednostce organizacyjnej Active Directory**

    Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu, które jest uwzględnione w określonej jednostce organizacyjnej Active Directory. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane.

    Domyślnie opcja ta jest wyłączona.

Liczba dodatkowych okien w kreatorze zależy od ustawień wybranych w pierwszym kroku. Reguły aktywacji profili zasad można zmodyfikować w późniejszym czasie.

6. Sprawdź listę skonfigurowanych parametrów. Jeśli lista jest poprawna, kliknij **Utwórz**.

Profil zostanie zapisany. Profil zostanie aktywowany na urządzeniu po wyzwoleniu reguł aktywacji.

Reguły aktywacji profilu zasad utworzone dla profilu będą wyświetlone we właściwościach profilu zasad, na zakładce **Reguły aktywacji**. Możesz zmodyfikować lub usunąć dowolną regułę aktywacji profilu zasad.

Jednocześnie może być wyzwolonych kilka reguł aktywacji.

Usuwanie profilu zasad

W celu usunięcia profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.

2. Na zakładce **Profile zasad** zaznacz pole obok profilu zasady, którą chcesz usunąć, a następnie kliknij **Usuń**.

3. W otwartym oknie ponownie kliknij **Usuń**.

   Profil zasad został usunięty. Jeśli zasada jest dziedziczona przez grupę niskiego poziomu, profil pozostanie w tej grupie, ale stanie się profilem zasady tej grupy. Odbywa się to w celu wyeliminowania znaczących zmian w ustawieniach zarządzanych aplikacji zainstalowanych na urządzeniach grup niskiego poziomu.

Szyfrowanie i ochrona danych

Szyfrowanie danych zmniejsza ryzyko przypadkowego wycieku danych w sytuacji, gdy laptop lub dysk twardy zostanie skradziony lub zgubiony, bądź też, gdy dostęp do danych uzyskują nieautoryzowani użytkownicy lub aplikacje.

Szyfrowanie jest obsługiwane przez następujące aplikacje Kaspersky:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

Za pomocą ustawień interfejsu użytkownika można wyświetlić lub ukryć niektóre elementy interfejsu związane z funkcją zarządzania szyfrowaniem.

Nie zalecamy włączania szyfrowania w VDI.

Szyfrowanie danych w Kaspersky Endpoint Security for Windows

Możesz zarządzać następującymi typami szyfrowania:

- Szyfrowanie dysków funkcją BitLocker na urządzeniach z systemem operacyjnym Windows dla serwerów
- Kaspersky Disk Encryption na urządzeniach z systemem operacyjnym Windows dla stacji roboczej

Korzystając z tych komponentów Kaspersky Endpoint Security for Windows, możesz na przykład włączyć lub wyłączyć szyfrowanie, przeglądać listę zaszyfrowanych dysków lub generować i przeglądać raporty dotyczące szyfrowania.

Szyfrowanie konfiguruje się, definiując zasady Kaspersky Endpoint Security for Windows w Kaspersky Security Center. Kaspersky Endpoint Security for Windows wykonuje szyfrowanie i odszyfrowywanie zgodnie z aktywną zasadą. Szczegółowe instrukcje dotyczące konfigurowania reguł oraz opis funkcji szyfrowania są dostępne w internetowym systemie pomocy dla Kaspersky Endpoint Security for Windows.

Szyfrowanie danych w Kaspersky Endpoint Security for Mac

Możesz użyć szyfrowania FileVault na urządzeniach z systemem macOS. Podczas pracy z Kaspersky Endpoint Security for Mac możesz włączyć lub wyłączyć to szyfrowanie.

Szyfrowanie konfiguruje się, definiując zasady Kaspersky Endpoint Security for Mac w Kaspersky Security Center. Kaspersky Endpoint Security for Mac wykonuje szyfrowanie i deszyfrowanie zgodnie z aktywną zasadą. Szczegółowy opis funkcji szyfrowania znajduje się w Pomocy Kaspersky Endpoint Security for Mac.

Przeglądanie listy zaszyfrowanych dysków

W Kaspersky Security Center możesz przeglądać szczegółowe informacje o zaszyfrowanych dyskach i urządzeniach zaszyfrowanych na poziomie dysku. Po odszyfrowaniu informacji na dysku, dysk jest automatycznie usuwane z listy.

W celu przejrzenia listy zaszyfrowanych dysków:

W menu głównym przejdź do **Operacje** → **Szyfrowanie i ochrona danych** → **Zaszyfrowane dyski**.

Jeśli sekcji nie ma w menu, oznacza to, że jest ukryta. W ustawieniach interfejsu użytkownika włącz opcję **Pokaż szyfrowanie i ochronę danych**, aby wyświetlić sekcję.

Możesz wyeksportować listę zaszyfrowanych dysków do pliku CSV lub pliku TXT. W tym celu kliknij przycisk **Eksportuj do pliku CSV** lub **Eksportuj do pliku TXT**.

Wyświetlanie listy zdarzeń szyfrowania

Podczas wykonywania zadań szyfrowania lub deszyfrowania danych na urządzeniach, Kaspersky Endpoint Security for Windows wysyła do Kaspersky Security Center informacje o zdarzeniach następujących typów:

- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na brak wolnego miejsca na dysku.
- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na problemy z licencją.
- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na brak praw dostępu.
- Dla aplikacji zablokowano dostęp do zaszyfrowanego pliku.
- Nieznane błędy.

W celu wyświetlenia listy zdarzeń, które wystąpiły w trakcie szyfrowania danych na urządzeniach:

W menu głównym przejdź do **Operacje** → **Szyfrowanie i ochrona danych** → **Zdarzenia szyfrowania**.

Jeśli sekcji nie ma w menu, oznacza to, że jest ukryta. W ustawieniach interfejsu użytkownika włącz opcję **Pokaż szyfrowanie i ochronę danych**, aby wyświetlić sekcję.

Możesz wyeksportować listę zaszyfrowanych dysków do pliku CSV lub pliku TXT. W tym celu kliknij przycisk **Eksportuj do pliku CSV** lub **Eksportuj do pliku TXT**.

Alternatywnie możesz przejrzeć listę zdarzeń szyfrowania dla każdego zarządzanego urządzenia.

Aby wyświetlić zdarzenia szyfrowania dla zarządzanego urządzenia:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
2. Kliknij nazwę zarządzanego urządzenia.
3. Na karcie **Ogólne** przejdź do sekcji **Ochrona**.
4. Kliknij łącze **Wyświetl błędy szyfrowania danych**.

Tworzenie i przeglądanie raportów z szyfrowania

Możesz wygenerować następujące raporty:

- Raport o stanie szyfrowania zarządzanych urządzeń. Ten raport zawiera szczegółowe informacje na temat szyfrowania danych na różnych zarządzanych urządzeniach. Na przykład raport pokazuje liczbę urządzeń, do których ma zastosowanie zasada ze skonfigurowanymi regułami szyfrowania. Możesz także dowiedzieć się, na przykład, ile urządzeń wymaga ponownego uruchomienia. Raport zawiera również informacje o technologii i algorytmie szyfrowania dla każdego urządzenia.
- Raport o stanie szyfrowania urządzeń pamięci masowej. Ten raport zawiera podobne informacje jak raport o stanie szyfrowania zarządzanych urządzeń, ale zawiera dane tylko dla urządzeń pamięci masowej i dysków wymiennych.
- Raport o prawach dostępu do zaszyfrowanych dysków. Ten raport pokazuje, które konta użytkowników mają dostęp do zaszyfrowanych dysków.
- Raport o błędach podczas szyfrowania plików. Ten raport zawiera informacje o błędach, które wystąpiły podczas uruchamiania zadań szyfrowania lub odszyfrowywania danych na urządzeniach.
- Raport o zablokowanym dostępie do zaszyfrowanych plików. Ten raport zawiera informacje o blokowaniu dostępu aplikacji do zaszyfrowanych plików. Ten raport jest pomocny, jeśli nieautoryzowany użytkownik lub aplikacja próbuje uzyskać dostęp do zaszyfrowanych plików lub dysków.

Możesz wygenerować dowolny raport w sekcji **Monitorowanie i raportowanie** → **Raporty**. Alternatywnie w sekcji **Operacje** → **Szyfrowanie i ochrona danych** możesz wygenerować następujące raporty dotyczące szyfrowania:

- Raport o stanie szyfrowania urządzeń pamięci masowej
- Raport o prawach dostępu do zaszyfrowanych dysków
- Raport o błędach podczas szyfrowania plików

*Aby wygenerować raport szyfrowania w sekcji **Szyfrowanie i ochrona danych**:*

1. Upewnij się, że włączyłeś opcję **Pokaż szyfrowanie i ochronę danych** w opcjach interfejsu.
2. We właściwościach zasady otwórz zakładkę **Konfiguracja zdarzenia**.
3. W sekcji **Krytyczny** kliknij **Dodaj zdarzenie** i zaznacz pole wyboru obok zdarzenia *Błąd podczas stosowania reguł szyfrowania/odszyfrowywania pliku*.
4. Kliknij **OK**.

5. W menu głównym przejdź do **Operacje** → **Szyfrowanie i ochrona danych**.
6. Wybierz jedną z następujących sekcji:
   - **Zaszyfrowane dyski** generuje raport o stanie szyfrowania urządzeń pamięci masowej lub raport o prawach dostępu do zaszyfrowanych dysków.
   - **Zdarzenia szyfrowania** generuje raport o błędach szyfrowania plików.
7. Kliknij nazwę raportu, który chcesz wygenerować.

Zostanie rozpoczęte tworzenie raportu.

Udzielanie dostępu do zaszyfrowanego dysku w trybie offline

Użytkownik może poprosić o dostęp do zaszyfrowanego urządzenia, na przykład, gdy Kaspersky Endpoint Security for Windows nie jest zainstalowany na zarządzanym urządzeniu. Po otrzymaniu żądania możesz utworzyć plik klucza dostępu i wysłać go do użytkownika. Wszystkie przypadki użycia i szczegółowe instrukcje znajdują się w Pomocy Kaspersky Endpoint Security for Windows.

W celu udzielenia dostępu do zaszyfrowanego dysku w trybie offline:

1. Uzyskaj plik żądania dostępu od użytkownika (plik z rozszerzeniem FDERTC). Postępuj zgodnie z instrukcjami zawartymi w Pomocy Kaspersky Endpoint Security for Windows aby wygenerować plik w Kaspersky Endpoint Security for Windows.
2. W menu głównym przejdź do **Operacje** → **Szyfrowanie i ochrona danych** → **Zaszyfrowane dyski**.

   Zostanie wyświetlona lista zaszyfrowanych dysków.
3. Wybierz dysk, do którego użytkownik zażądał dostępu.
4. Kliknij przycisk **Udziel dostępu do urządzenia w trybie offline**.
5. W oknie, które zostanie otwarte, wybierz wtyczkę odpowiadającą aplikacji Kaspersky, która została użyta do zaszyfrowania wybranego dysku.

   > Jeśli dysk jest zaszyfrowany przy pomocy aplikacji Kaspersky, która nie jest obsługiwana przez konsolę Kaspersky Security Center Web Console, użyj Konsoli administracyjnej opartej na Microsoft Management Console, aby udzielić dostępu offline.
6. Postępuj zgodnie z instrukcjami podanymi w Pomocy Kaspersky Endpoint Security for Windows (patrz rozwijające się bloki na końcu sekcji).

Następnie użytkownik stosuje otrzymany plik, aby uzyskać dostęp do zaszyfrowanego dysku i odczytać dane zapisane na dysku.

Użytkownicy i role użytkownika

Ta sekcja opisuje użytkowników i role użytkownika, a także zawiera instrukcje ich tworzenia i modyfikowania, przydzielania ról i grup do użytkowników, a także kojarzenia profili zasad z rolami.

Informacje o rolach użytkowników

Rola użytkownika (zwana dalej *rolą*) to obiekt zawierający zestaw praw i uprawnień. Rola może zostać skojarzona z ustawieniami aplikacji Kaspersky zainstalowanych na urządzeniu użytkownika. Możesz przypisać rolę do zestawu użytkowników lub do zestawu grup bezpieczeństwa na dowolnym poziomie w hierarchii grup administracyjnych, Serwerów administracyjnych lub na poziomie określonych obiektów.

Jeśli zarządzasz urządzeniami poprzez hierarchię Serwerów administracyjnych, która obejmuje wirtualne Serwery administracyjne, pamiętaj, że możesz tworzyć, modyfikować lub usuwać role użytkowników tylko z fizycznego Serwera administracyjnego. Następnie możesz propagować role użytkowników na drugorzędne Serwery administracyjne, w tym wirtualne.

Możesz skojarzyć role użytkownika z profilami zasad. Jeśli użytkownikowi przydzielono rolę, ten użytkownik uzyska ustawienia zabezpieczeń niezbędne do pełnienia funkcji związanych z jego stanowiskiem pracy.

Rola użytkownika może zostać skojarzona z użytkownikami urządzeń w określonej grupie administracyjnej.

Obszar roli użytkownika

Obszar roli użytkownika to połączenie użytkowników i grup administracyjnych. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup podrzędnych.

Korzyści korzystania z ról

Korzyścią korzystania z ról jest brak konieczności określenia ustawień zabezpieczeń dla każdego z zarządzanych urządzeń lub dla każdego z użytkowników oddzielnie. Liczba użytkowników i urządzeń w firmie może być całkiem duża, ale liczba różnych stanowisk pracy, które wymagają różnych ustawień zabezpieczeń jest znacząco mała.

Różnice wynikające z używania profili zasad

Profile zasad to właściwości zasady tworzone dla każdej aplikacji Kaspersky oddzielnie. Rola jest skojarzona z wieloma profilami zasad utworzonymi dla różnych aplikacji. Dlatego też rola jest metodą zebrania ustawień dla określonego typu użytkownika w jednym miejscu.

Przeglądanie kont użytkowników i sesji

Kaspersky Security Center umożliwia zarządzanie kontami użytkowników i grupami kont. Aplikacja obsługuje dwa typy kont:

- Konta pracowników firmy. Serwer administracyjny pobiera dane kont tych użytkowników podczas przeszukiwania sieci firmowej.
- Konta wewnętrznych użytkowników. Te konta są stosowane, gdy używane są wirtualne Serwery administracyjne. Konta użytkowników wewnętrznych są tworzone i używane tylko w obrębie Kaspersky Security Center.

Listę kont użytkowników można wyświetlić na jeden z następujących sposobów:

- W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy i grupy**.
- W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia** → link <nazwa urządzenia> → karta **Ogólne** → sekcja **Ogólne** → blok **Sesje**.

  Sekcja **Sesje** powinna wyświetlać konta użytkowników z aktywnymi sesjami na urządzeniach z systemem Windows.

Lista kont użytkowników wyświetla się prawidłowo, jeżeli spełnione są następujące wymagania:

- Użyj Agenta sieciowego w tej samej wersji, co Serwer administracyjny lub nowszej.
- Przeszukiwanie usługi Active Directory jest włączone w celu wyświetlania kont użytkowników domeny.
- Na zarządzanych urządzeniach z systemem Windows uruchomiona jest usługa **Serwer** (**LanmanServer**).

Konfigurowanie praw dostępu do funkcji aplikacji. Kontrola dostępu oparta o rolę

Kaspersky Security Center oferuje możliwości dla dostępu opartego na roli do funkcji Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky.

Możesz skonfigurować uprawnienia dostępu do funkcji aplikacji dla użytkowników Kaspersky Security Center w jeden z następujących sposobów:

- Konfigurując uprawnienia dla każdego użytkownika lub grupy użytkowników indywidualnie.
- Tworząc standardowe role użytkownika z predefiniowanym zestawem uprawnień i przypisując te role do użytkowników w zależności od ich zakresu obowiązków.

Stosowanie ról użytkownika jest przeznaczone do uproszczenia i skrócenia rutynowych procedur konfigurowania uprawnień dostępu użytkowników do funkcji aplikacji. Uprawnienia dostępu w obrębie roli są konfigurowane zgodnie ze 'standardowymi' zadaniami i zakresem obowiązków użytkowników.

Rolom użytkownika można przypisać nazwy, które odpowiadają ich przeznaczeniu. Możesz utworzyć nieograniczoną liczbę ról w aplikacji.

Możesz użyć predefiniowanych ról użytkownika z już skonfigurowanym zestawem uprawnień lub utworzyć nowe role i samodzielnie skonfigurować wymagane uprawnienia.

Prawa dostępu do funkcji aplikacji

Poniższa tabela przedstawia funkcje Kaspersky Security Center wraz z prawami dostępu do zarządzania powiązanymi zadaniami, raportami, ustawieniami i wykonywania powiązanych działań użytkownika.

Aby wykonać czynności użytkownika wymienione w tabeli, użytkownik musi mieć określone uprawnienia obok akcji.

Prawa do **odczytu**, **Zapis** i **Wykonywanie** mają zastosowanie do każdego zadania, raportu lub ustawienia. Oprócz tych praw użytkownik musi mieć uprawnienie **Wykonywanie działań dla wyborów urządzeń**, aby zarządzać zadaniami, raportami lub ustawieniami wyborów urządzeń.

Wszystkie zadania, raporty, ustawienia i pakiety instalacyjne, których brakuje w tabeli, należą do obszaru funkcjonalnego **Funkcje ogólne: Podstawowa funkcjonalność**.

Prawa dostępu do funkcji aplikacji

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
Funkcje ogólne: **Zarządzanie grupami administracyjnymi**	**Zapis**	• Dodaj urządzenie do grupy administracyjnej: **Zapis** • Usuń urządzenie z grupy administracyjnej: **Zapis** • Dodaj grupę administracyjną do innej grupy administracyjnej: **Zapis** • Usuń grupę administracyjną z innej grupy administracyjnej: **Zapis**	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
Funkcje ogólne: **Uzyskuj dostęp do obiektów bez względu na ich listy ACL**	**Odczyt**	Uzyskaj dostęp do Odczyt do wszystkich obiektów: **Odczyt**	Brak	Brak	**Funkcje ogólne: Uzyskuj dostęp do obiektów bez względu na ich listy ACL** są przeznaczon do celów audytu. Gd użytkownikom zostar przyznane prawa **Odczyt** w tym obszarze funkcjonalnym, uzyskają pełny dostę do **Odczyt** do wszystkich obiektów będą mogli wykonywać dowolne utworzone zadania na wybranych urządzeniach podłączonych do Serwera administracyjnego poprzez Agenta sieciowego z uprawnieniami administratora lokalnego (root w przypadku systemu Linux). Zalecamy ostrożne przyznanie tych praw ograniczonej grupie użytkowników, którzy potrzebują ich do wykonywania swoich obowiązków służbowych. Dostęp jest przyznawany niezależnie od innych praw, nawet jeśli zabraniają one dostępu do Odczyt określonych obiektów
Funkcje ogólne: **Podstawowa funkcjonalność**	• **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Reguły przenoszenia urządzeń (tworzenie, modyfikowanie lub usuwanie) dla Serwera wirtualnego: **Zapis**, **Wykonywanie działań dla wyborów urządzeń** • Uzyskaj niestandardowy certyfikat protokołu Mobile (LWNGT): **Odczyt** • Ustaw certyfikat niestandardowy protokołu Mobile (LWNGT): **Zapis** • Uzyskaj listę sieci zdefiniowaną przez NLA: **Odczyt** • Dodaj, zmodyfikuj lub usuń listę sieci zdefiniowaną przez NLA: **Zapis**	• „Pobierz aktualizacje do repozytorium serwera administracyjnego” • „Dostarczaj raporty” • „Roześlij pakiet instalacyjny” • „Zdalnie zainstaluj aplikację na podrzędnych Serwerach administracyjnych”	• „Raport o stanie ochrony” • „Raport o zagrożeniach” • „Raport o najbardziej zainfekowanych urządzeniach” • „Raport o stanie antywirusowych baz danych” • „Raport o błędach” • „Raport o atakach sieciowych” • „Raport podsumowujący o zainstalowanych aplikacjach zabezpieczających systemy pocztowe” • „Raport podsumowujący o aplikacjach zabezpieczających styk sieci z internetem”	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		• Wyświetl listę kontroli dostępu grup: **Odczyt** • Wyświetl dziennik zdarzeń aplikacji Kaspersky: **Odczyt** • Wyświetl klucz odzyskiwania, aby przywrócić dostęp do dysku twardego zaszyfrowanego za pomocą Szyfrowania dysków funkcją BitLocker: **Wykonywanie**		• „Raport podsumowujący o typach zainstalowanych aplikacji" • „Raport o użytkownikach zainfekowanych urządzeń" • „Raport incydentów" • „Raport o zdarzeniach" • „Raport aktywności punktów dystrybucji" • „Raport o podrzędnych Serwerach administracyjnych" • „Raport zdarzeń Kontroli urządzeń" • „Raport o lukach" • „Raport o zabronionych aplikacjach" • „Raport Kontroli sieci" • „Raport o stanie szyfrowania zarządzanych urządzeń" • „Raport o stanie szyfrowania urządzeń pamięci masowej" • „Raport o błędach podczas szyfrowania plików" • „Raport o zablokowanym dostępie do zaszyfrowanych plików" • „Raport o uprawnieniach dostępu do zaszyfrowanych urządzeń" • „Raport o obowiązujących uprawnieniach użytkowników" • „Raport na temat praw"	
Funkcje ogólne: **Usunięte obiekty**	• **Odczyt** • **Zapis**	• Wyświetl usunięte obiekty w Koszu: **Odczyt** • Usuń obiekty z Kosza: **Zapis**	Brak	Brak	Brak
Funkcje ogólne: **Przetwarzanie zdarzeń**	• **Usuń zdarzenia** • **Edycja ustawień powiadamiania o zdarzeniach** • **Edycja ustawień rejestrowania zdarzeń** • **Zapis**	• Zmień ustawienia rejestracji zdarzeń: **Edycja ustawień rejestrowania zdarzeń** • Zmień ustawienia powiadomień o zdarzeniach: **Edycja ustawień powiadamiania o zdarzeniach**	Brak	Brak	Ustawienia: • Ustawienia epidemii wirusa: liczba wykryć wirusów wymagana do utworzenia zdarzenia epiden wirusa • Ustawienia

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		• Usuń zdarzenia: **Usuń zdarzenia**			epidemii wirusa: czas na ocenę wykrycia wirusów • Maksymalna liczb zdarzeń przechowywanyc w bazie danych • Okres przechowywania zdarzeń z usuniętych urządzeń
Funkcje ogólne: **Operacje na Serwerze administracyjnym**	• **Odczyt** • **Zapis** • **Wykonywanie** • **Modyfikacja list ACL obiektu** • **Wykonywanie działań dla wyborów urządzeń**	• Określ porty Serwera administracyjnego dla połączenia agenta sieciowego: **Zapis** • Określ porty Serwera proxy aktywacji uruchomionego na serwerze administracyjnym Serwer administracyjny: **Zapis** • Określ porty serwera proxy aktywacji dla urządzeń przenośnych uruchomionych na Serwerze administracyjnym: **Zapis** • Określ porty serwera sieciowego do dystrybucji samodzielnych pakietów: **Zapis** • Określ porty serwera sieciowego do dystrybucji profili MDM: **Zapis** • Określ porty SSL Serwera administracyjnego do połączenia przez Kaspersky Security Center Web Console: **Zapis** • Określ porty serwera administracyjnego Serwer administracyjny dla połączenia mobilnego: **Zapis** • Zmienianie maksymalnej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego: **Zapis**	• „Tworzenie kopii zapasowych danych Serwera administracyjnego" • „Konserwacja baz danych"	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		• Określ maksymalną liczbę zdarzeń, które mogą być wysłane przez Serwer administracyjny: **Zapis** • Określ przedział czasu, w którym zdarzenia mogą być wysyłane przez Serwer administracyjny: **Zapis**			
Funkcje ogólne: **Wdrażanie aplikacji Kaspersky**	• **Zarządzanie poprawkami Kaspersky** • **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	Zaakceptuj lub odrzuć instalację poprawki: **Zarządzanie poprawkami Kaspersky**	Brak	• „Raport użycia klucza licencyjnego przez wirtualny Serwer administracyjny” • „Raport o wersjach oprogramowania Kaspersky” • „Raport o niekompatybilnych aplikacjach” • „Raport o wersjach aktualizacji modułu oprogramowania Kaspersky” • „Raport wdrażania ochrony”	Pakiet instalacyjny: „Kaspersky”
Funkcje ogólne: **Zarządzanie kluczami licencyjnymi**	• **Eksportuj plik klucza** • **Zapis**	• Eksportuj plik klucza: **Eksportuj plik klucza** • Zmodyfikuj ustawienia klucza licencyjnego Serwera administracyjnego: **Zapis**	Brak	Brak	Brak
Funkcje ogólne: **Wymuszone zarządzanie raportami**	• **Odczyt** • **Zapis**	• Twórz raporty niezależnie od ich list ACL: **Zapis** • Wykonywanie raportów niezależnie od ich list ACL: **Odczyt**	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
Funkcje ogólne: **Hierarchia Serwerów administracyjnych**	**Skonfiguruj hierarchię Serwerów administracyjnych**	Zarejestruj, zaktualizuj lub usuń podrzędne Serwery administracyjne: **Skonfiguruj hierarchię Serwerów administracyjnych**	Brak	Brak	Brak
Funkcje ogólne: **Uprawnienia użytkownika**	**Modyfikacja list ACL obiektu**	• Zmień właściwości Zabezpieczenia dowolnego obiektu: **Modyfikacja list ACL obiektu** • Zarządzaj rolami użytkowników: **Modyfikacja list ACL obiektu** • Zarządzaj użytkownikami wewnętrznymi: **Modyfikacja list ACL obiektu** • Zarządzaj grupami zabezpieczeń: **Modyfikacja list ACL obiektu** • Zarządzaj aliasami: **Modyfikacja list ACL obiektu**	Brak	Brak	Brak
Funkcje ogólne: **Wirtualne Serwery administracyjne**	• **Zarządzaj wirtualnymi Serwerami administracyjnymi** • **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Pobierz listę wirtualnych serwerów administracyjnych Serwery administracyjne: **Odczyt** • Uzyskaj informacje na temat wirtualnego Serwera administracyjnego: **Odczyt** • Utwórz, zaktualizuj lub usuń wirtualny Serwer administracyjny: **Zarządzaj wirtualnymi Serwerami administracyjnymi** • Przenieś wirtualny Serwer administracyjny do innej grupy: **Zarządzaj wirtualnymi Serwerami administracyjnymi** • Ustaw uprawnienia do administracyjnego Serwera wirtualnego: **Zarządzaj wirtualnymi Serwerami administracyjnymi**	Brak	„Raport o wynikach instalacji aktualizacji oprogramowania firm trzecich”	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
Funkcje ogólne: **Zarządzanie kluczem szyfrowania**	**Zapis**	Zaimportuj klucze szyfrowania: **Zapis**	Brak	Brak	Brak
Zarządzanie urządzeniami mobilnymi: Ogólny	• **Podłącz nowe urządzenia** • **Przesyłanie do urządzeń mobilnych jedynie informacji o poleceniach** • **Przesyłanie poleceń do urządzeń mobilnych** • **Zarządzanie certyfikatami** • **Odczyt** • **Zapis**	• Uzyskaj dane przywracania Usługi zarządzania kluczami: **Odczyt** • Usuń certyfikaty użytkownika: **Zarządzanie certyfikatami** • Uzyskaj część publiczną certyfikatu użytkownika: **Odczyt** • Sprawdź, czy infrastruktura klucza publicznego jest włączona: **Odczyt** • Sprawdź konto infrastruktury klucza publicznego: **Odczyt** • Uzyskaj szablony infrastruktury klucza publicznego: **Odczyt** • Uzyskaj szablony infrastruktury klucza publicznego za pomocą certyfikatu rozszerzonego użycia klucza: **Odczyt** • Sprawdź, czy certyfikat infrastruktury klucza publicznego został odwołany: **Odczyt** • Zaktualizuj ustawienia wydawania certyfikatów użytkownika: **Zarządzanie certyfikatami** • Uzyskaj ustawienia wydawania certyfikatu użytkownika: **Odczyt** • Pobierz pakiety według nazwy i wersji aplikacji: **Odczyt** • Ustaw lub anuluj certyfikat użytkownika: **Zarządzanie certyfikatami** • Odnów certyfikat użytkownika: **Zarządzanie certyfikatami**	Brak	Brak	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
		• Ustaw tag certyfikatu użytkownika: **Zarządzanie certyfikatami** • Uruchom generację pakietu instalacyjnego MDM; anuluj generowanie pakietu instalacyjnego MDM: **Podłącz nowe urządzenia**			
Zarządzanie systemami: Łączność	• **Uruchom sesje Pulpitu zdalnego** • **Połączenie z istniejącymi sesjami Pulpitu zdalnego** • **Rozpocznij tunelowanie** • **Zapisz pliki z urządzeń na stacji roboczej administratora** • **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Utwórz sesję udostępniania pulpitu: **Uruchom sesje Pulpitu zdalnego** • Utwórz sesję RDP: **Połączenie z istniejącymi sesjami Pulpitu zdalnego** • Utwórz tunel: **Rozpocznij tunelowanie** • Zapisz listę sieci partnerskiej: **Zapisz pliki z urządzeń na stacji roboczej administratora**	Brak	„Raport o użytkownikach urządzenia”	Brak
Zarządzanie systemami: Inwentarz sprzętu	• **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Pobierz lub wyeksportuj obiekt spisu sprzętu: **Odczyt** • Dodaj, ustaw lub usuń obiekt spisu sprzętu: **Zapis**	Brak	• „Raport rejestru sprzętu” • „Raport o zmianach konfiguracji” • „Raport o sprzęcie”	Brak
Zarządzanie systemami: Network Access Control	• **Odczyt** • **Zapis**	• Wyświetl ustawienia CISCO: **Odczyt** • Zmień ustawienia CISCO: **Zapis**	Brak	Brak	Brak
Zarządzanie systemami: Wdrażanie systemu operacyjnego	• **Instalacja serwerów PXE** • **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Zainstaluj serwer PXE: **Instalacja serwerów PXE** • Wyświetl listę serwerów PXE: **Odczyt** • Rozpocznij lub zatrzymaj proces instalacji na klientach PXE: **Wykonywanie** • Zarządzaj sterownikami dla WinPE i obrazów systemu operacyjnego: **Zapis**	„Utwórz pakiet instalacyjny na podstawie obrazu systemu operacyjnego urządzenia odniesienia”	Brak	Pakiet instalacyjny: „Obraz systemu operacyjnego”
Zarządzanie systemami: Zarządzanie lukami i poprawkami	• **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Wyświetl właściwości poprawki trzeciej firmy: **Odczyt** • Zmień właściwości poprawki trzeciej firmy: **Zapis**	• „Wykonać synchronizację Windows Update” • „Instalacja aktualizacji Windows Update”	„Raport o aktualizacjach oprogramowania”	Brak

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport	Inne
			• „Napraw luki" • „Zainstaluj wymagane aktualizacje i napraw luki"		
Zarządzanie systemami: Zdalna instalacja	• **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	• Przejrzyj właściwości pakietu instalacyjnego Zarządzanie lukami i poprawkami innych firm: **Odczyt** • Zmień właściwości pakietu instalacyjnego Zarządzanie lukami i poprawkami innych firm: **Zapis**	Brak	Brak	Pakiety instalacyjne: • „Aplikacja niestandardowa" • „Pakiet VAPM"
Zarządzanie systemami: Inwentaryzacja oprogramowania	• **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	Brak	Brak	• „Raport o zainstalowanych aplikacjach" • „Raport o rejestrze aplikacji" • „Raport o stanie grup licencjonowanych aplikacji" • „Raport dotyczący kluczy licencyjnych oprogramowania innych firm"	Brak
Zarządzanie systemami: Zdalne wykonywanie skryptów	• **Odczyt** • **Zapis** • **Wykonywanie** • **Wykonywanie działań dla wyborów urządzeń**	Użytkownik może przeglądać właściwości zadania: **Odczyt** Użytkownik może utworzyć, usunąć lub zmodyfikować pakiet instalacyjny: **Zapis** Użytkownik może uruchomić zadanie: **Zapis**. Na urządzeniach klienckich z systemem Linux skrypty są wykonywane z uprawnieniami roota. Użytkownik może uruchomić zadanie lub zaplanować jego uruchomienie: **Wykonywanie** Użytkownik może uruchomić zadanie na wybranych urządzeniach: **Wykonywanie działań dla wyborów urządzeń**	„Zdalne wykonywanie skryptów"	Brak	Brak

Informacje o rolach użytkowników

Role użytkowników przypisane do użytkowników Kaspersky Security Center zapewniają im zestawy praw dostępu do funkcji aplikacji.

> Użytkownikom utworzonym na Serwerze wirtualnym nie można przypisać roli na Serwerze administracyjnym.

Możesz użyć predefiniowanych ról użytkownika z już skonfigurowanym zestawem uprawnień lub utworzyć nowe role. W takim przypadku należy samodzielnie ustawić zakres roli i przypisać uprawnienia dostępu do funkcji Kaspersky Security Center. Niektóre z predefiniowanych ról użytkowników dostępnych w Kaspersky Security Center mogą być powiązane z określonymi stanowiskami pracy, na przykład **Audytor**, **Specjalista ds. zabezpieczeń**, **Opiekun** (te role są obecne w Kaspersky Security Center od wersji 11). Prawa dostępu do tych ról są wstępnie skonfigurowane zgodnie ze standardowymi zadaniami i zakresem obowiązków powiązanych stanowisk. Poniższa tabela pokazuje jak role mogą zostać powiązane z określonymi stanowiskami pracy:

Przykłady ról dla określonych stanowisk pracy

Rola	Komentarz
Audytor	Zezwala na wszystkie operacje przeglądania i wykonywania wszelkich utworzonych zadań na wybranych urządzeniach podłączonych do Serwera administracyjnego za pośrednictwem Agenta sieciowego z uprawnieniami administratora lokalnego (root w przypadku Linux). > Zalecamy ostrożne przyznawanie tych praw ograniczonej grupie użytkowników, którzy potrzebują ich do wykonywania swoich obowiązków służbowych.
Opiekun	Zezwala na wszystkie działania przeglądania, ale nie zezwala na pozostałe działania. Możesz przypisać tę rolę do specjalisty ds. zabezpieczeń i innych menadżerów zarządzających bezpieczeństwem IT w Twojej firmie.
Specjalista ds. zabezpieczeń	Zezwala na wszystkie działania przeglądania, zezwala na zarządzanie raportami; przydziela ograniczone uprawnienia w obszarze **Zarządzanie systemami**: **Łączność**. Możesz przypisać tę rolę do specjalisty zarządzającego bezpieczeństwem IT w Twojej firmie.

Poniższa tabela przedstawia prawa dostępu przypisane do każdej predefiniowanej roli użytkownika.

Prawa dostępu do predefiniowanych ról użytkowników

Rola	Opis
Administrator serwera administracyjnego	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Funkcje ogólne**: • **Podstawowa funkcjonalność** • **Przetwarzanie zdarzeń** • **Hierarchia Serwerów administracyjnych** • **Wirtualne Serwery administracyjne** • **Zarządzanie poprawkami i lukami**: • **Łączność** • **Inwentaryzacja sprzętu** • **Inwentaryzacja oprogramowania** Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.

Rola	Opis
Operator serwera administracyjnego	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych: • **Funkcje ogólne**: • **Podstawowa funkcjonalność** • **Wirtualne Serwery administracyjne** • **Zarządzanie poprawkami i lukami**: • **Łączność** • **Inwentaryzacja sprzętu** • **Inwentaryzacja oprogramowania**
Audytor	Zezwala na wszystkie operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Usunięte obiekty** • **Wymuszone zarządzanie raportami** Tę rolę można przypisać do osoby, która przeprowadza audyt w Twojej organizacji.
Administrator instalacji	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Funkcje ogólne**: • **Podstawowa funkcjonalność** • **Wdrażanie oprogramowania Kaspersky** • **Zarządzanie kluczami licencyjnymi** • **Zarządzanie poprawkami i lukami**: • **Wdrażanie systemu operacyjnego** • **Zarządzanie lukami i poprawkami** • **Instalacja zdalna** • **Inwentaryzacja oprogramowania** Przyznaje uprawnienia do **odczytu** i **wykonywania** w obszarze funkcjonalnym **Funkcje ogólne: Wirtualne serwery administracyjne**.
Operator instalacji	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych: • **Funkcje ogólne**: • **Podstawowa funkcjonalność** • **Zdalna instalacja oprogramowania Kaspersky** (zapewnia również **Zarządzanie poprawkami Kaspersky** bezpośrednio w tym obszarze) • **Wirtualne Serwery administracyjne** • **Zarządzanie poprawkami i lukami**: • **Wdrażanie systemu operacyjnego** • **Zarządzanie lukami i poprawkami** • **Instalacja zdalna** • **Inwentaryzacja oprogramowania**
Administrator Kaspersky Endpoint Security	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.

Rola	Opis
Operator Kaspersky Endpoint Security	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje
Główny administrator	Zezwala na wszystkie operacje w obszarach funkcjonalnych, z *wyjątkiem* następujących obszarów w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Wymuszone zarządzanie raportami** Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.
Główny operator	Przyznaje prawa **odczytu** i **wykonywania** (w stosownych przypadkach) we wszystkich następujących obszarach funkcjonalnych: • **Funkcje ogólne**: • **Podstawowa funkcjonalność** • **Usunięte obiekty** • **Operacje na Serwerze administracyjnym** • **Wdrażanie aplikacji Kaspersky** • **Wirtualne Serwery administracyjne** • **Zarządzanie urządzeniami mobilnymi: ogólne** • **Zarządzanie systemem**, w tym wszystkie funkcje • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje
Administrator zarządzania urządzeniami mobilnymi	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • **Zarządzanie urządzeniami mobilnymi: ogólne**
Operator zarządzania urządzeniami mobilnymi	Przyznaje uprawnienia **Odczyt** i **Wykonywanie** w obszarze funkcjonalnym **Funkcje ogólne**: **Podstawowa funkcjonalność**. Przyznaje uprawnienia **odczytu** i **wysyłania** informacji poleceń na urządzenia mobilne w obszarach funkcjonalnych **Zarządzania urządzeniami mobilnymi**: **Ogólne**.
Specjalista ds. zabezpieczeń	Zezwala na następujące operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Wymuszone zarządzanie raportami** Przyznaje uprawnienia **Odczytu**, **Wpisania**, **Wykonywania**, **Zapisywania** plików z urządzeń na stacji roboczej administratora i **wykonywania działań dla wyborów urządzeń w obszarze funkcjonalnym Zarządzanie systemami: Łączność**. Możesz przypisać tę rolę do specjalisty zarządzającego bezpieczeństwem IT w Twojej firmie.
Użytkownik portalu Self Service Portal	Zezwala na wszystkie operacje w obszarze funkcjonalnym **Zarządzanie urządzeniami mobilnymi: Self Service Portal**. Ta funkcja nie jest obsługiwana w Kaspersky Security Center 11 i nowszej wersji.
Opiekun	Przyznaje prawo do **Odczytu** w obszarach funkcjonalnych **Funkcje ogólne**: **Dostęp do obiektów, niezależnie od ich list ACL** i **Funkcje ogólne**: **Wymuszone zarządzanie raportami**. Możesz przypisać tę rolę do specjalisty ds. zabezpieczeń i innych menadżerów zarządzających bezpieczeństwem IT w Twojej firmie.
Administrator zarządzania lukami i poprawkami	Zezwala na wszystkie operacje w obszarach funkcjonalnych **Funkcje ogólne**: **Podstawowa funkcjonalność** i **Zarządzanie systemem** (w tym wszystkie funkcje).
Operator zarządzania lukami i poprawkami	Przyznaje uprawnienia **Odczyt** i **Wykonywanie** (w stosownych przypadkach) w obszarach funkcjonalnych **Funkcje ogólne**: **Podstawowa funkcjonalność** i **Zarządzanie systemem** (w tym wszystkie funkcje).

Nadawanie praw dostępu do określonych obiektów

Oprócz nadawania praw dostępu na poziomie serwera, możesz skonfigurować dostęp do konkretnych obiektów, np. do konkretnego zadania. Aplikacja umożliwia określenie praw dostępu do następujących typów obiektów:

- Grupy administracyjne
- Zadania
- Raporty
- Wybory urządzeń
- Wybory zdarzeń

Aby przypisać prawa dostępu do określonego obiektu:

1. W zależności od typu obiektu, w menu głównym przejdź do odpowiedniej sekcji:
   - **Zasoby (urządzenia)** → **Hierarchia grup**
   - **Zasoby (urządzenia)** → **Zadania**
   - **Monitorowanie i raportowanie** → **Raporty**
   - **Zasoby (urządzenia)** → **Wybory urządzeń**
   - **Monitorowanie i raportowanie** → **Wybory zdarzeń**
2. Otwórz właściwości obiektu, do którego chcesz skonfigurować prawa dostępu.

   Aby otworzyć okno właściwości grupy administracyjnej lub zadania, kliknij nazwę obiektu. Właściwości innych obiektów można otworzyć za pomocą przycisku na pasku narzędzi.
3. W oknie właściwości otwórz sekcję **Prawa dostępu**.

   Zostanie otwarta lista użytkowników. Wymienieni użytkownicy i podane grupy zabezpieczeń mają prawa dostępu do obiektu. Domyślnie, jeśli używasz hierarchii grup administracyjnych lub Serwerów, lista i prawa dostępu są dziedziczone z nadrzędnej grupy administracyjnej lub Serwera podstawowego.
4. Aby móc modyfikować listę, włącz opcję **Użyj uprawnień niestandardowych**.

5. Skonfiguruj prawa dostępu:

   - Użyj przycisków **Dodaj** i **Usuń**, aby zmodyfikować listę.
   - Określ prawa dostępu dla użytkownika lub grupy zabezpieczeń. Wykonaj jedną z poniższych czynności:
     - Jeśli chcesz ręcznie określić prawa dostępu, wybierz użytkownika lub grupę zabezpieczeń, kliknij przycisk **Prawa dostępu**, a następnie określ prawa dostępu.
     - Jeśli chcesz przypisać rolę użytkownika do użytkownika lub grupy zabezpieczeń, wybierz użytkownika lub grupę zabezpieczeń, kliknij przycisk **Role**, a następnie wybierz rolę do przypisania.

6. Kliknij przycisk **Zapisz**.

Prawa dostępu do obiektu zostały skonfigurowane.

Przydzielanie praw dostępu użytkownikom i grupom bezpieczeństwa

Użytkownikom i grupom bezpieczeństwa można przyznać prawa dostępu do różnych funkcji Serwera administracyjnego, na przykład Kaspersky Endpoint Security for Linux.

Aby przypisać prawa dostępu do użytkownika lub grupy bezpieczeństwa:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Prawa dostępu** zaznacz pole wyboru obok nazwy użytkownika lub grupy bezpieczeństwa, której chcesz przypisać prawa, a następnie kliknij przycisk **Prawa dostępu**.

   Nie można jednocześnie wybrać wielu użytkowników lub grup bezpieczeństwa. Jeśli wybierzesz więcej niż jeden element, przycisk **Prawa dostępu** będzie nieaktywny.

3. Skonfiguruj zestaw uprawnień dla użytkownika lub grupy:

   a. Rozwiń węzeł o funkcje Serwera administracyjnego lub innej aplikacji Kaspersky.

   b. Zaznacz pole wyboru **Zezwól** lub **Odmów** obok żądanej funkcji lub uprawnienia dostępu.

      Przykład 1: Zaznacz pole wyboru **Zezwól** obok węzła **Integracja aplikacji**, aby przyznać użytkownikowi lub grupie wszystkie dostępne uprawnienia dostępu do funkcji Integracja aplikacji (**Odczyt**, **Zapis** i **Wykonanie**).

      Przykład 2: Rozwiń węzeł **Zarządzanie kluczami szyfrowania**, a następnie zaznacz pole wyboru **Zezwalaj** obok uprawnienia **Zapis**, aby przyznać użytkownikowi lub grupie uprawnienia dostępu **Zapis** do funkcji zarządzania kluczami szyfrowania.

4. Po skonfigurowaniu zestawu uprawnień dostępu kliknij przycisk **OK**.

Zestaw uprawnień dla użytkownika lub grupy użytkowników zostanie skonfigurowany.

Uprawnienia Serwera administracyjnego (lub grupy administracyjnej) są podzielone na następujące obszary:

- Funkcje ogólne:
  - Zarządzanie grupami administracyjnymi
  - Uzyskuj dostęp do obiektów bez względu na ich listy ACL

- Podstawowa funkcjonalność
- Usunięte obiekty
- Zarządzanie kluczem szyfrowania
- Przetwarzanie zdarzeń
- Operacje na Serwerze administracyjnym (tylko w oknie właściwości Serwera administracyjnego)
- Znaczniki urządzenia
- Wdrażanie aplikacji Kaspersky
- Zarządzanie kluczami licencyjnymi
- Integracja aplikacji
- Wymuszone zarządzanie raportami
- Hierarchia Serwerów administracyjnych
- Uprawnienia użytkownika
- Wirtualne Serwery administracyjne

- Zarządzanie urządzeniami mobilnymi:
  - Ogólne
  - Self Service Portal
- Zarządzanie systemami:
  - Łączność
  - Zdalne wykonywanie skryptów
  - Inwentarz sprzętu
  - Network Access Control
  - Wdrażanie systemu operacyjnego
  - Zarządzanie lukami i poprawkami
  - Zdalna instalacja
  - Inwentaryzacja oprogramowania

Jeśli dla uprawnienia dostępu nie wybrano opcji **Zezwól** ani **Odmów**, wówczas uprawnienie dostępu jest uznawane za *niezdefiniowane*: zostaje odrzucone, dopóki wyraźnie nie zostanie dozwolone lub odrzucone dla użytkownika.

Uprawnienia użytkownika są sumą:

- Własnych uprawnień użytkownika
- Uprawnień wszystkich ról przypisanych do tego użytkownika
- Uprawnień wszystkich grup bezpieczeństwa, do których należy użytkownik
- Uprawnień wszystkich ról przypisanych do grupy bezpieczeństwa, do których należy użytkownik

Jeśli przynajmniej jeden z tych zestawów uprawnień posiada opcję **Odmów** dla uprawnienia, wówczas dla użytkownika zostaje zabronione to uprawnienie nawet wtedy, gdy inne zestawy zezwalają na nie lub pozostawiają je niezdefiniowane.

Można również dodać użytkowników i grupy zabezpieczeń do obszaru roli użytkownika, aby korzystać z różnych funkcji Serwera administracyjnego. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup podrzędnych.

Dodawanie konta użytkownika wewnętrznego

Jeśli chcesz dodać konto użytkownika, upewnij się, że Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym Funkcje ogólne: Uprawnienia użytkownika.

W celu dodania nowego konta użytkownika wewnętrznego do Kaspersky Security Center:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.
2. Kliknij **Dodaj**.
3. W otwartym oknie **Dodaj użytkownika** określ ustawienia nowego konta użytkownika:
   - **Nazwa**
   - **Hasło**
     Hasło musi być zgodne z następującymi regułami:
     - Hasło musi zawierać od 8 do 256 znaków.
     - Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
       - Wielkie litery (A-Z)
       - Małe litery (a-z)
       - Cyfry (0-9)
       - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków "." i "@", gdy "." jest umieszczane przed "@".

Aby zobaczyć wprowadzone hasło kliknij .

Możesz włączyć opcję **Użytkownik musi zmienić hasło przy pierwszym logowaniu** aby wymusić zmianę hasła przy pierwszym uwierzytelnieniu użytkownika.

4. Zapisz zmiany, aby dokończyć tworzenie nowego konta użytkownika.

Nowe konto użytkownika zostanie dodane do listy użytkowników.

Aby zalogować się przy użyciu utworzonego wewnętrznego konta użytkownika w Kaspersky Security Center Web Console, należy przypisać rolę do konta. Przed zalogowaniem upewnij się, że domena lub konto użytkownika wewnętrznego mają przypisaną rolę. W przeciwnym razie wystąpi błąd logowania.

Tworzenie grupy bezpieczeństwa

W celu utworzenia grupy bezpieczeństwa:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz kartę **Grupy**.
2. Kliknij **Dodaj**.
3. W otwartym oknie **Utwórz grupę bezpieczeństwa** określ następujące ustawienia dla nowej grupy bezpieczeństwa:
   - **Nazwa grupy**
   - **Opis**
4. Kliknij **Zapisz**, aby zachować zmiany.

Nowa grupa bezpieczeństwa zostanie dodana do listy grup.

Edytowanie konta użytkownika wewnętrznego

Jeśli chcesz edytować konto użytkownika, upewnij się, że Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym Funkcje ogólne: Uprawnienia użytkownika.

W celu edytowania konta użytkownika wewnętrznego w Kaspersky Security Center:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.
2. Kliknij nazwę konta użytkowników, które chcesz edytować.

3. W otwartym oknie ustawień użytkownika, na zakładce **Ogólne** zmień ustawienia konta użytkownika:

- **Status użytkownika**

  Jeśli to konieczne, przesuń przełącznik na **Wyłączone**, aby zabronić użytkownikowi możliwość łączenia z aplikacją. Możesz wyłączyć konto, na przykład, gdy pracownik opuści teren firmy.

- **Nazwa**

- **Pełna nazwa**

- **Opis**

- **Adres e-mail**

- **Główny numer telefonu**

- **Hasło**

  W razie potrzeby możesz ustawić nowe hasło dla połączenia użytkownika z Kaspersky Security Center w następujący sposób:

  a. Kliknij przycisk **Zmień hasło**, a następnie ustaw nowe hasło dla konta użytkownika.

  Hasło musi być zgodne z następującymi regułami:

  - Hasło musi zawierać od 8 do 256 znaków.
  - Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
    - Wielkie litery (A-Z)
    - Małe litery (a-z)
    - Cyfry (0-9)
    - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków "." i "@", gdy "." jest umieszczane przed "@".

  Aby zobaczyć wprowadzone hasło kliknij .

  b. W razie potrzeby włącz opcję **Użytkownik musi zmienić hasło przy pierwszym logowaniu** aby wymusić zmianę hasła przy kolejnym uwierzytelnieniu użytkownika.

  c. Jeśli konto użytkownika jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** określ dane uwierzytelniające konta, które ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym Funkcje ogólne: Uprawnienia użytkownika.

4. Na zakładce **Bezpieczeństwo uwierzytelniania** możesz określić ustawienia zabezpieczeń dla tego konta.

5. Na zakładce **Grupy** możesz dodać użytkownika do grup zabezpieczeń.

6. Na zakładce **Urządzenia** możesz przypisać urządzenia do użytkownika.

7. Na zakładce **Role** możesz przypisać role do użytkownika.

8. Zapisz zmiany, aby zakończyć edycję konta użytkownika.

Zaktualizowane konto użytkownika pojawi się na liście użytkowników.

Edytowanie grupy bezpieczeństwa

W celu edytowania grupy bezpieczeństwa:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz kartę **Grupy**.

2. Kliknij nazwę grupy bezpieczeństwa, którą chcesz edytować.

3. W otwartym oknie ustawień grupy zmień ustawienia grupy bezpieczeństwa:

   - Na zakładce **Ogólne** możesz zmienić ustawienia **Nazwa** i **Opis**. Te ustawienia są dostępne tylko dla wewnętrznych grup bezpieczeństwa.

   - Na zakładce **Użytkownicy** możesz dodać użytkownika do grup zabezpieczeń. To ustawienie jest dostępne tylko dla użytkowników wewnętrznych i wewnętrznych grup bezpieczeństwa.

   - Na zakładce **Role** możesz przypisać rolę do grupy bezpieczeństwa.

4. Kliknij **Zapisz**, aby zachować zmiany.

Zmiany zostaną zastosowane do grupy bezpieczeństwa.

Przypisywanie roli do użytkownika lub grupy bezpieczeństwa

Aby przypisać rolę do użytkownika lub grupy bezpieczeństwa:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz kartę **Użytkownicy** lub **Grupy**.

2. Wybierz nazwę użytkownika lub grupy bezpieczeństwa, do których chcesz przypisać rolę.

   Można wybrać kilka nazw.

3. W wierszu menu kliknij przycisk **Przypisz rolę**.

   Zostanie uruchomiony Kreator przypisywania roli.

4. Postępuj zgodnie z instrukcjami kreatora: wybierz rolę, którą chcesz przypisać wybranym użytkownikom lub grupom bezpieczeństwa, a następnie wybierz zakres roli.

   Obszar roli użytkownika to połączenie użytkowników i grup administracyjnych. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup podrzędnych.

Rola z zestawem uprawnień do pracy z Serwerem administracyjnym zostanie przypisana do użytkownika (lub użytkowników lub grupy bezpieczeństwa). Na liście użytkowników lub grup bezpieczeństwa w kolumnie **Ma przypisane role** pojawia się pole wyboru.

Użytkownikom utworzonym na Serwerze wirtualnym nie można przypisać roli na Serwerze administracyjnym.

Dodawanie kont użytkowników do wewnętrznej grupy bezpieczeństwa

Do wewnętrznej grupy bezpieczeństwa możesz dodać tylko konta użytkowników wewnętrznych.

W celu dodania kont użytkowników do wewnętrznej grupy bezpieczeństwa:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.
2. Zaznacz pola obok kont użytkowników, które chcesz dodać do grupy bezpieczeństwa.
3. Kliknij przycisk **Przypisz grupę**.
4. W oknie **Przypisz grupę**, które zostanie otwarte, wybierz grupę, do której chcesz dodać konta użytkowników.
5. Kliknij przycisk **Zapisz**.

Konta użytkowników zostaną dodane do grupy bezpieczeństwa. Możesz także dodać użytkowników wewnętrznych do grupy bezpieczeństwa, korzystając z ustawień grupy.

Wskazywanie użytkownika jako właściciela urządzenia

Aby uzyskać informacje na temat przypisywania użytkownika jako właściciela urządzenia mobilnego, zobacz pomoc dla Kaspersky Secure Mobility Management.

W celu wskazania użytkownika jako właściciela urządzenia:

1. Jeżeli chcesz przypisać właściciela urządzenia podłączonego do wirtualnego Serwera administracyjnego, najpierw przełącz się na wirtualny Serwer administracyjny:
   a. W menu głównym kliknij ikonę jodełki (▪) po prawej stronie bieżącej nazwy Serwera administracyjnego.
   b. Wybierz wymagany Serwer administracyjny.
2. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.
   Zostanie otwarta lista użytkowników. Jeśli jesteś aktualnie połączony z wirtualnym Serwerem administracyjnym, lista zawiera użytkowników z bieżącego wirtualnego Serwera administracyjnego oraz głównego Serwera administracyjnego.
3. Kliknij nazwę konta użytkownika, które chcesz przypisać jako właściciel urządzenia.

4. W otwartym oknie ustawień użytkownika kliknij zakładkę **Urządzenia**.
5. Kliknij **Dodaj**.
6. Z listy urządzeń wybierz urządzenie, które chcesz przypisać do użytkownika.
7. Kliknij **OK**.

Wybrane urządzenie zostanie dodane do listy urządzeń przypisanych do użytkownika.

To samo działanie możesz wykonać w **Zasoby (urządzenia)** → **Zarządzane urządzenia**, klikając nazwę urządzenia, które chcesz przypisać, a następnie klikając odnośnik **Zarządzaj właścicielem urządzenia**.

Konfigurowanie weryfikacji dwuetapowej dla wszystkich użytkowników

W tym scenariuszu opisano sposób włączenia weryfikacji dwuetapowej dla wszystkich użytkowników oraz sposób wykluczenia konta użytkowników z weryfikacji dwuetapowej. Jeśli nie włączyłeś weryfikacji dwuetapowej dla swojego konta przed włączeniem go dla innych użytkowników, aplikacja najpierw otworzy okno umożliwiające włączenie weryfikacji dwuetapowej dla Twojego konta. W tym scenariuszu opisano również sposób włączenia weryfikacji dwuetapowej na swoim koncie.

> Jeśli włączyłeś weryfikację dwuetapową na swoim koncie, możesz przejść do etapu włączenia weryfikacji dwuetapowej dla wszystkich użytkowników.

Wymagania wstępne

Zanim zaczniesz:

- Upewnij się, że Twoje konto użytkownika ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** służącym do modyfikacji ustawień zabezpieczeń dla kont innych użytkowników.
- Upewnij się, że inni użytkownicy Serwera administracyjnego zainstalowali aplikację uwierzytelniającą na swoich urządzeniach.

Etapy

Włączenie weryfikacji dwuetapowej dla wszystkich użytkowników przebiega etapami:

1. **Instalacja aplikacji uwierzytelniającej na urządzeniu**

   Można zainstalować dowolną aplikację obsługującą algorytm czasowego hasła jednorazowego (TOTP), np:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP

- Yandex ID
- Avanpost Authenticator
- Aladdin 2FA

Aby sprawdzić, czy Kaspersky Security Center obsługuje aplikację uwierzytelniającą, której chcesz użyć, włącz weryfikację dwuetapową dla wszystkich użytkowników lub dla określonego użytkownika.

Jeden z kroków sugeruje podanie kodu zabezpieczającego wygenerowanego przez aplikację uwierzytelniającą. Jeśli się powiedzie, Kaspersky Security Center obsługuje wybrany token uwierzytelniający.

> Zdecydowanie nie zalecamy instalowania aplikacji uwierzytelniającej na tym samym urządzeniu, z którego nawiązywane jest połączenie z Serwerem administracyjnym.

2. **Synchronizowanie czasu aplikacji uwierzytelniającej z czasem urządzenia, na którym zainstalowany jest Serwer administracyjny**

   Upewnij się, że czas na urządzeniu z aplikacją uwierzytelniającą i czas na urządzeniu z Serwerem administracyjnym są zsynchronizowane z czasem UTC, z użyciem zewnętrznych źródeł czasu. W przeciwnym razie mogą wystąpić awarie podczas uwierzytelniania i aktywacji weryfikacji dwuetapowej.

3. **Włączenie weryfikacji dwuetapowej dla Twojego konta i otrzymanie tajnego klucza do Twojego konta**

   Dostępne instrukcje:

   - Konsola administracyjna oparta na MMC: Włączanie weryfikacji dwuetapowej na własnym koncie
   - Dla Kaspersky Security Center Web Console: Włączanie weryfikacji dwuetapowej dla własnego konta

   Po włączeniu weryfikacji dwuetapowej na koncie możesz włączyć weryfikację dwuetapową dla wszystkich użytkowników.

4. **Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników**

   Użytkownicy z włączoną weryfikacją dwuetapową muszą jej używać do logowania się do Serwera administracyjnego.

   Dostępne instrukcje:

   - Konsola administracyjna oparta na MMC: Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników
   - Dla Kaspersky Security Center Web Console: Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników

5. **Edytowanie nazwy wystawcy kodu zabezpieczającego**

   Jeśli masz kilka Serwerów administracyjnych o podobnych nazwach, konieczna może być zmiana nazw wystawców kodów zabezpieczających w celu lepszego rozpoznawania różnych Serwerów administracyjnych.

   Dostępne instrukcje:

   - Konsola administracyjna oparta na MMC: Edytowanie nazwy wystawcy kodu zabezpieczającego
   - Dla Kaspersky Security Center Web Console: Edytowanie nazwy wystawcy kodu zabezpieczającego

6. **Z wyłączeniem kont użytkowników, dla których nie musisz włączać weryfikacji dwuetapowej**

   W razie potrzeby możesz wykluczyć użytkowników z weryfikacji dwuetapowej. Użytkownicy z wykluczonymi kontami nie muszą używać weryfikacji dwuetapowej, aby zalogować się do Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna oparta na MMC: Wykluczanie kont z weryfikacji dwuetapowej
- Dla Kaspersky Security Center Web Console: Wykluczanie kont z weryfikacji dwuetapowej

7. **Konfigurowanie weryfikacji dwuetapowej dla własnego konta**

   Jeśli użytkownicy nie są wykluczeni z weryfikacji dwuetapowej, a weryfikacja dwuetapowa nie została jeszcze skonfigurowana dla posiadanych przez nich kont, należy ją skonfigurować w oknie otwieranym po zalogowaniu się do Kaspersky Security Center. W przeciwnym razie nie będą mogli uzyskać dostępu do Serwera administracyjnego zgodnie ze swoimi uprawnieniami.

   Dostępne instrukcje:

   - Konsola administracyjna oparta na MMC: Konfigurowanie weryfikacji dwuetapowej na własnym koncie
   - Dla Kaspersky Security Center Web Console: Konfigurowanie weryfikacji dwuetapowej dla własnego konta

Wyniki

Po zakończeniu tego scenariusza:

- Weryfikacja dwuetapowa jest włączona na Twoim koncie.
- Weryfikacja dwuetapowa jest włączona dla wszystkich kont użytkowników Serwera administracyjnego, z wyjątkiem kont użytkowników, które zostały wykluczone.

Informacje o weryfikacji dwuetapowej

Gdy dla danego konta włączona jest weryfikacja dwuetapowa, do zalogowania się do Konsoli administracyjnej lub Kaspersky Security Center Web Console oprócz nazwy użytkownika i hasła wymagany jest również jednorazowy kod zabezpieczający. Po aktywowaniu uwierzytelniania domeny, użytkownik musi jedynie wprowadzić jednorazowy kod zabezpieczający.

Aby korzystać z weryfikacji dwuetapowej, zainstaluj aplikację uwierzytelniającą generującą jednorazowe kody zabezpieczające na urządzeniu mobilnym lub komputerze. Można użyć dowolnej aplikacji obsługującej algorytm czasowego hasła jednorazowego (TOTP), jak np.:

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- Yandex ID
- Avanpost Authenticator
- Aladdin 2FA

Aby sprawdzić, czy Kaspersky Security Center obsługuje aplikację uwierzytelniającą, której chcesz użyć, włącz weryfikację dwuetapową dla wszystkich użytkowników lub dla określonego użytkownika.

Jeden z kroków sugeruje podanie kodu zabezpieczającego wygenerowanego przez aplikację uwierzytelniającą. Jeśli się powiedzie, Kaspersky Security Center obsługuje wybrany token uwierzytelniający.

Zdecydowanie zalecamy, aby zapisać klucz tajny lub kod QR i przechowywać go w bezpiecznym miejscu. Pomoże to w przywróceniu dostępu do Kaspersky Security Center Web Console w przypadku utraty dostępu do urządzenia mobilnego.

Aby zabezpieczyć korzystanie z Kaspersky Security Center, możesz włączyć weryfikację dwuetapową dla swojego konta i włączyć weryfikację dwuetapową dla wszystkich użytkowników.

Możesz wykluczyć konta z weryfikacji dwuetapowej. Może to być konieczne w przypadku kont usług, które nie mogą otrzymać kodu zabezpieczającego dla uwierzytelnienia.

Zasady i ograniczenia

Aby móc aktywować weryfikację dwuetapową dla wszystkich użytkowników i dezaktywować weryfikację dwuetapową dla poszczególnych użytkowników:

- Upewnij się, że Twoje konto ma uprawnienia do modyfikacji obiektów ACL w obszarze funkcjonalnym **Funkcje ogólne: Uprawnienia użytkownika**.
- Włącz weryfikację dwuetapową dla swojego konta.

Aby móc dezaktywować weryfikację dwuetapową dla wszystkich użytkowników:

- Upewnij się, że Twoje konto ma uprawnienia do modyfikacji obiektów ACL w obszarze funkcjonalnym **Funkcje ogólne: Uprawnienia użytkownika**.
- Zaloguj się do Kaspersky Security Center Web Console przy użyciu weryfikacji dwuetapowej.

Jeśli weryfikacja dwuetapowa jest włączona dla konta użytkownika na Serwerze administracyjnym Kaspersky Security Center w wersji 13 lub nowszej, użytkownik nie będzie mógł zalogować się do Kaspersky Security Center Web Console w wersji 12, 12.1 lub 12.2.

Ponowne wydanie tajnego klucza

Każdy użytkownik może ponownie wydać tajny klucz używany do weryfikacji dwuetapowej. Gdy użytkownik loguje się do Serwera administracyjnego przy użyciu ponownie wydanego klucza, taki nowy tajny klucz jest zapisywany dla danego konta użytkownika. Jeśli użytkownik wprowadzi nowy tajny klucz niepoprawnie, taki nowy tajny klucz nie zostanie zapisany, a ważny pozostanie bieżący tajny klucz.

Kod zabezpieczający posiada identyfikator, o którym mowa w *nazwie wystawcy*. Nazwa wystawcy kodu zabezpieczającego jest używana jako identyfikator Serwera administracyjnego w aplikacji uwierzytelniającej. Nazwa wystawcy kodu zabezpieczającego ma domyślną wartość, która jest taka sama, jak nazwa Serwera administracyjnego. Możesz zmienić nazwę wystawcy kodu zabezpieczającego. Jeśli zmienisz nazwę wystawcy kodu zabezpieczającego, musisz wydać nowy klucz tajny i przekazać go do aplikacji uwierzytelniającej.

Włączanie weryfikacji dwuetapowej dla własnego konta (Web Console)

Użytkownik może włączyć weryfikację dwuetapową tylko dla swojego konta.

Zanim włączysz weryfikację dwuetapową dla swojego konta, upewnij się, że aplikacja uwierzytelniająca jest zainstalowana na urządzeniu mobilnym. Upewnij się, że czas ustawiony w aplikacji uwierzytelniającej jest zsynchronizowany z czasem ustawionym na urządzeniu, na którym zainstalowany jest Serwer administracyjny.

W celu włączenia weryfikacji dwuetapowej na koncie użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Kliknij nazwę swojego konta.
3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Bezpieczeństwo uwierzytelniania**.
4. W zakładce **Bezpieczeństwo uwierzytelniania**:
   a. Wybierz opcję **Zażądaj nazwę użytkownika, hasło i kod zabezpieczający (weryfikacja dwuetapowa)**. Kliknij przycisk **Zapisz**.
   b. W otwartym oknie weryfikacji dwuetapowej kliknij **Zobacz, jak skonfigurować weryfikację dwuetapową**.
      Wprowadź klucz tajny w aplikacji uwierzytelniającej lub też kliknij opcję **Wyświetl kod QR** i zeskanuj kod QR za pomocą aplikacji uwierzytelniającej na urządzeniu mobilnym, aby uzyskać jednorazowy kod zabezpieczający.
   c. W oknie weryfikacji dwuetapowej określ kod zabezpieczający, wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **Sprawdź i zastosuj**.
5. Kliknij przycisk **Zapisz**.

Weryfikacja dwuetapowa jest włączona na Twoim koncie.

Włączanie weryfikacji dwuetapowej dla własnego konta (opartej na MMC)

Zanim włączysz weryfikację dwuetapową dla swojego konta, upewnij się, że aplikacja uwierzytelniająca jest zainstalowana na urządzeniu mobilnym. Upewnij się, że czas ustawiony w aplikacji uwierzytelniającej jest zsynchronizowany z czasem Serwera administracyjnego.

W celu włączenia weryfikacji dwuetapowej na swoim koncie:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego przejdź do panelu **Sekcje** i wybierz **Zaawansowane**, a następnie **Weryfikacja dwuetapowa**.
3. W sekcji **Weryfikacja dwuetapowa** kliknij przycisk **Konfiguruj**.

> Jeśli weryfikacja dwuetapowa jest już włączona na Twoim koncie, kliknięcie przycisku **Konfiguruj** spowoduje zresetowanie klucza tajnego, dzięki czemu będziesz mógł ponownie skonfigurować weryfikację dwuetapową.

W otwartym oknie właściwości weryfikacji dwuetapowej wyświetlany jest tajny klucz.

4. Wprowadź tajny klucz w aplikacji uwierzytelniającej, aby uzyskać jednorazowy kod zabezpieczający. Możesz wprowadzić tajny klucz w aplikacji uwierzytelniającej ręcznie lub zeskanować kod QR za pomocą aplikacji uwierzytelniającej w urządzeniu mobilnym.

5. Określ kod zabezpieczający wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **OK**, aby zamknąć okno właściwości weryfikacji dwuetapowej.

6. Kliknij przycisk **Zastosuj**.

7. Kliknij przycisk **OK**.

Weryfikacja dwuetapowa jest włączona na Twoim koncie.

Włączanie wymaganej weryfikacji dwuetapowej dla wszystkich użytkowników (Web Console)

Możesz włączyć weryfikację dwuetapową dla wszystkich użytkowników Serwera administracyjnego, jeśli Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** i jeśli jesteś uwierzytelniony za pomocą weryfikacji dwuetapowej.

W celu włączenia weryfikacji dwuetapowej dla wszystkich użytkowników:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Bezpieczeństwo uwierzytelniania** w oknie właściwości ustaw przycisk przełącznika opcji **weryfikacja dwuetapowa dla wszystkich użytkowników** w pozycji włączenia.

3. Jeśli nie włączyłeś weryfikacji dwuetapowej na swoim koncie, aplikacja otworzy okno dla włączenia weryfikacji dwuetapowej dla Twojego konta.

   a. W oknie weryfikacji dwuetapowej kliknij **Zobacz, jak skonfigurować weryfikację dwuetapową**.

   b. Wprowadź ręcznie klucz tajny w aplikacji uwierzytelniającej lub kliknij opcję **Wyświetl kod QR** i zeskanuj kod QR za pomocą aplikacji uwierzytelniającej na urządzeniu mobilnym, aby uzyskać jednorazowy kod zabezpieczający.

   c. W oknie weryfikacji dwuetapowej określ kod zabezpieczający, wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **Sprawdź i zastosuj**.

Weryfikacja dwuetapowa jest włączona dla wszystkich użytkowników. Od teraz wszyscy użytkownicy Serwera administracyjnego, w tym użytkownicy dodani po włączeniu weryfikacji dwuetapowej dla wszystkich użytkowników, muszą konfigurować weryfikację dwuetapową dla swoich kont, z wyjątkiem użytkowników, których konta są wykluczone z weryfikacji dwuetapowej.

Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników (opartej na MMC)

Możesz włączyć weryfikację dwuetapową dla wszystkich użytkowników Serwera administracyjnego, jeśli Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** i jeśli jesteś uwierzytelniony za pomocą weryfikacji dwuetapowej.

W celu włączenia weryfikacji dwuetapowej dla wszystkich użytkowników:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Zaawansowane**, a następnie **Weryfikacja dwuetapowa**.
3. Kliknij przycisk **Skonfiguruj wymagane**, aby włączyć weryfikację dwuetapową dla wszystkich użytkowników.
4. Jeśli nie włączyłeś weryfikacji dwuetapowej na swoim koncie, aplikacja otworzy okno dla włączenia weryfikacji dwuetapowej dla Twojego konta.
   a. Wprowadź tajny klucz w aplikacji uwierzytelniającej, aby uzyskać jednorazowy kod zabezpieczający. Tajny klucz można wprowadzić do aplikacji uwierzytelniającej ręcznie lub zeskanować kod QR za pomocą aplikacji uwierzytelniającej na urządzeniu mobilnym, aby uzyskać jednorazowy kod zabezpieczający.
   b. Określ kod zabezpieczający wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **OK**, aby zamknąć okno właściwości weryfikacji dwuetapowej.
5. W sekcji **Weryfikacja dwuetapowa** kliknij przycisk **Zastosuj**, a następnie kliknij przycisk **OK**.

Weryfikacja dwuetapowa jest włączona dla wszystkich użytkowników. Od teraz wszyscy użytkownicy Serwera administracyjnego, w tym użytkownicy dodani po włączeniu tej opcji, muszą konfigurować weryfikację dwuetapową dla swoich kont, z wyjątkiem użytkowników, których konta są wykluczone z weryfikacji dwuetapowej.

Wyłączanie weryfikacji dwuetapowej dla konta użytkownika (Web Console)

Możesz wyłączyć weryfikację dwuetapową na swoim koncie, a także na koncie dowolnego innego użytkownika.

Możesz wyłączyć weryfikację dwuetapową dla konta kolejnego użytkownika, jeśli Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** i pod warunkiem uwierzytelnienia za pomocą weryfikacji dwuetapowej.

W celu wyłączenia weryfikacji dwuetapowej dla konta użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Kliknij nazwę wewnętrznego konta użytkownika, dla którego chcesz wyłączyć weryfikację dwuetapową. Może to być Twoje własne konto lub konto innego użytkownika.
3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Ochrona konta**.

4. Na zakładce **Ochrona konta** wybierz opcję **Zażądaj tylko nazwę użytkownika i hasło**, jeśli chcesz wyłączyć weryfikację dwuetapową dla konta użytkownika.

5. Kliknij przycisk **Zapisz**.

Weryfikacja dwuetapowa jest wyłączona dla konta użytkownika.

Jeśli chcesz przywrócić dostęp użytkownikowi, który nie może zalogować się do Kaspersky Security Center Web Console przy użyciu weryfikacji dwuetapowej, wyłącz weryfikację dwuetapową dla tego konta użytkownika, a następnie wybierz opcję **Zażądaj tylko nazwę użytkownika i hasło** zgodnie z powyższym opisem. Po wykonaniu tej czynności zaloguj się do Kaspersky Security Center Web Console na koncie użytkownika, dla którego wyłączyłeś weryfikację dwuetapową, a następnie włącz weryfikację ponownie.

Wyłączanie weryfikacji dwuetapowej dla konta użytkownika (opartej na MMC)

W celu wyłączenia weryfikacji dwuetapowej na swoim koncie:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.

2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Zaawansowane**, a następnie **Weryfikacja dwuetapowa**.

3. W sekcji **Weryfikacja dwuetapowa** kliknij przycisk **Wyłącz**.

4. Kliknij przycisk **Zastosuj**.

5. Kliknij przycisk **OK**.

Weryfikacja dwuetapowa jest wyłączona na Twoim koncie.

Możesz wyłączyć weryfikację dwuetapową kont innych użytkowników. Zapewnia to ochronę w przypadku, gdy, na przykład, użytkownik zgubi lub zepsuje urządzenie mobilne.

Możesz wyłączyć weryfikację dwuetapową dla konta kolejnego użytkownika, jeśli masz uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** i pod warunkiem uwierzytelnienia za pomocą weryfikacji dwuetapowej. Wykonując poniższe czynności, możesz również wyłączyć weryfikację dwuetapową na swoim koncie.

W celu wyłączenia weryfikacji dwuetapowej dla dowolnego konta użytkownika:

1. W drzewie konsoli otwórz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. W obszarze roboczym kliknij dwukrotnie konto użytkownika, dla którego chcesz wyłączyć weryfikację dwuetapową.

   Dla wszystkich kont użytkowników, dla których włączona jest weryfikacja dwuetapowa, kolumna **Wymagana weryfikacja dwuetapowa** ma wartość **Tak**.

3. W oknie **Właściwości:<nazwa użytkownika>**, które zostanie otwarte, wybierz sekcję **Weryfikacja dwuetapowa**.

4. W sekcji **Weryfikacja dwuetapowa** wybierz następujące opcje:

   - Jeśli chcesz wyłączyć weryfikację dwuetapową dla konta użytkownika, kliknij przycisk **Wyłącz**.
   - Jeśli chcesz wykluczyć to konto użytkownika z weryfikacji dwuetapowej, wybierz opcję **Użytkownik może przejść uwierzytelnianie tylko przy użyciu nazwy użytkownika i hasła**.

5. Kliknij przycisk **Zastosuj**.

6. Kliknij przycisk **OK**.

Weryfikacja dwuetapowa dla konta użytkownika jest wyłączona.

Jeśli chcesz przywrócić dostęp użytkownikowi, który nie może zalogować się do Konsoli administracyjnej przy użyciu weryfikacji dwuetapowej, wyłącz weryfikację dwuetapową dla tego konta użytkownika i zaznacz opcję **Użytkownik może przejść uwierzytelnianie tylko przy użyciu nazwy użytkownika i hasła** w obszarze **Weryfikacja dwuetapowa** zgodnie z powyższym opisem. Po wykonaniu tej czynności zaloguj się do Konsoli administracyjnej na koncie użytkownika, dla którego wyłączono weryfikację dwuetapową, a następnie włącz weryfikację ponownie.

Wyłączanie wymaganej weryfikacji dwuetapowej dla wszystkich użytkowników (Web Console)

Możesz wyłączyć wymaganą weryfikację dwuetapową dla wszystkich użytkowników, jeśli weryfikacja dwuetapowa jest włączona dla Twojego konta, a Twoje konto posiada uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika**. Jeśli weryfikacja dwuetapowa nie jest włączona na Twoim koncie, musisz włączyć weryfikację dwuetapową dla swojego konta przed wyłączeniem jej dla wszystkich użytkowników.

W celu wyłączenia weryfikacji dwuetapowej dla wszystkich użytkowników:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Bezpieczeństwo uwierzytelniania** w oknie właściwości ustaw przycisk przełącznika opcji **weryfikacja dwuetapowa dla wszystkich użytkowników** w pozycji wyłączenia.

Weryfikacja dwuetapowa jest wyłączona dla wszystkich użytkowników. Wyłączenie weryfikacji dwuetapowej dla wszystkich użytkowników nie dotyczy określonych kont, w przypadku których wcześniej weryfikacja dwuetapowa była włączona osobno.

Wyłączanie wymaganej weryfikacji dwuetapowej dla wszystkich użytkowników (opartej na MMC)

Możesz wyłączyć wymaganą weryfikację dwuetapową dla wszystkich użytkowników Serwera administracyjnego, jeśli masz uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** i jeśli jesteś uwierzytelniony za pomocą weryfikacji dwuetapowej.

W celu wyłączenia weryfikacji dwuetapowej dla wszystkich użytkowników:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Zaawansowane**, a następnie **Weryfikacja dwuetapowa**.
3. Kliknij przycisk **Skonfiguruj opcjonalne**, aby wyłączyć weryfikację dwuetapową dla wszystkich użytkowników.
4. Kliknij przycisk **Zastosuj** w sekcji **Weryfikacja dwuetapowa**.
5. Kliknij przycisk **OK** w sekcji **Weryfikacja dwuetapowa**.

Weryfikacja dwuetapowa jest wyłączona dla wszystkich użytkowników. Wyłączenie weryfikacji dwuetapowej dla wszystkich użytkowników nie dotyczy określonych kont, w przypadku których wcześniej weryfikacja dwuetapowa była włączona osobno.

Wykluczanie kont z weryfikacji dwuetapowej (Web Console)

Możesz wykluczyć konta użytkowników z weryfikacji dwuetapowej, jeśli masz uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika**.

Jeśli konto użytkownika jest wykluczone z listy weryfikacji dwuetapowej dla wszystkich użytkowników, ten użytkownik nie musi korzystać z weryfikacji dwuetapowej.

> Wykluczenie kont z weryfikacji dwuetapowej może być konieczne w przypadku kont usług, które nie mogą przekazać kodu zabezpieczającego podczas uwierzytelniania.

Jeśli chcesz wykluczyć niektóre konta użytkowników z weryfikacji dwuetapowej:

1. W pierwszej kolejności musisz przeprowadzić Przeszukiwanie kontrolera domeny Active Directory, aby odświeżyć listę użytkowników Serwera administracyjnego, jeśli chcesz wykluczyć konta Active Directory.
2. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.
3. Na zakładce **Bezpieczeństwo uwierzytelniania** w oknie właściwości, w tabeli wykluczeń weryfikacji dwuetapowej kliknij przycisk **Dodaj**.
4. W oknie, które zostanie otwarte:
   a. Wybierz konta użytkowników, które chcesz wykluczyć.
   b. Kliknij przycisk **OK**.

Wybrane konta użytkowników są wykluczone z weryfikacji dwuetapowej.

Wykluczanie kont z weryfikacji dwuetapowej (opartej na MMC)

Możesz wykluczyć konto z weryfikacji dwuetapowej, jeśli Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika**.

Jeśli konto użytkownika zostało wykluczone z weryfikacji dwuetapowej, użytkownik ten może zalogować się do Konsoli administracyjnej lub Kaspersky Security Center Web Console bez korzystania z weryfikacji dwuetapowej.

Wykluczenie kont z weryfikacji dwuetapowej może być konieczne w przypadku kont usług, które nie mogą przekazać kodu zabezpieczającego podczas uwierzytelniania.

W celu wykluczenia konta użytkownika z weryfikacji dwuetapowej:

1. Jeśli chcesz wykluczyć konto Active Directory, wykonaj Przeszukiwanie Active Directory, aby odświeżyć listę użytkowników Serwera administracyjnego.
2. W drzewie konsoli otwórz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.
3. W obszarze roboczym kliknij dwukrotnie konto użytkownika, które chcesz wykluczyć z weryfikacji dwuetapowej
4. W oknie **Właściwości:<nazwa użytkownika>**, które zostanie otwarte, wybierz sekcję **Weryfikacja dwuetapowa**.
5. W otwartej sekcji wybierz opcję **Użytkownik może przejść uwierzytelnianie tylko przy użyciu nazwy użytkownika i hasła**.
6. W sekcji **Weryfikacja dwuetapowa** kliknij przycisk **Zastosuj**, a następnie kliknij przycisk **OK**.

To konto użytkownika jest wykluczone z weryfikacji dwuetapowej. Wykluczone konta możesz sprawdzić na liście kont użytkowników.

Edytowanie nazwy wystawcy kodu zabezpieczającego (Web Console)

Możesz mieć kilka identyfikatorów (nazywanych wystawcami) dla różnych Serwerów administracyjnych. Możesz zmienić nazwę wystawcy kodu zabezpieczającego w przypadku, gdy, na przykład, jeśli Serwer administracyjny już używa podobnej nazwy wystawcy kodu zabezpieczającego dla innego Serwera administracyjnego. Domyślnie, nazwa wystawcy kodu zabezpieczającego jest taka sama, jak nazwa Serwera administracyjnego.

Po zmianie nazwy wystawcy kodu zabezpieczającego należy ponownie wystawić nowy klucz tajny i przekazać go do aplikacji uwierzytelniającej.

W celu określenia nowej nazwy wystawcy kodu zabezpieczającego:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.
2. W otwartym oknie ustawień użytkownika wybierz zakładkę **Ochrona konta**.

3. Na zakładce **Ochrona konta** kliknij odnośnik **Edytuj**.

   Zostanie otwarta sekcja **Edytuj wydawcę kodu zabezpieczającego**.

4. Określ nową nazwę wydawcy kodu zabezpieczającego.

5. Kliknij przycisk **OK**.

Nowa nazwa wystawcy kodu zabezpieczającego została określona dla Serwera administracyjnego.

Edytowanie nazwy wystawcy kodu zabezpieczającego (opartej na MMC)

Możesz mieć kilka identyfikatorów (nazywanych wystawcami) dla różnych Serwerów administracyjnych. Możesz zmienić nazwę wystawcy kodu zabezpieczającego w przypadku, gdy, na przykład, Serwer administracyjny już używa podobnej nazwy wystawcy kodu zabezpieczającego dla innego Serwera administracyjnego. Domyślnie, nazwa wystawcy kodu zabezpieczającego jest taka sama, jak nazwa Serwera administracyjnego.

Po zmianie nazwy wystawcy kodu zabezpieczającego należy ponownie wystawić nowy klucz tajny i przekazać go do aplikacji uwierzytelniającej.

W celu określenia nowej nazwy wystawcy kodu zabezpieczającego:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.

2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Zaawansowane**, a następnie **Weryfikacja dwuetapowa**.

3. Podaj nową nazwę wystawcy kodu zabezpieczającego w polu **Wystawca kodu zabezpieczającego**.

4. Kliknij przycisk **Zastosuj** w sekcji **Weryfikacja dwuetapowa**.

5. Kliknij przycisk **OK** w sekcji **Weryfikacja dwuetapowa**.

Nowa nazwa wystawcy kodu zabezpieczającego została określona dla Serwera administracyjnego.

Konfigurowanie weryfikacji dwuetapowej dla własnego konta (Web Console)

Gdy po raz pierwszy zalogujesz się do Kaspersky Security Center po włączeniu weryfikacji dwuetapowej, otworzy się okno umożliwiające skonfigurowanie weryfikacji dwuetapowej konta.

Zanim skonfigurujesz weryfikację dwuetapową dla swojego konta, upewnij się, że aplikacja uwierzytelniająca jest zainstalowana na urządzeniu mobilnym.

Upewnij się, że czas na urządzeniu z aplikacją uwierzytelniającą i czas na urządzeniu z Serwerem administracyjnym są zsynchronizowane z czasem UTC, z użyciem zewnętrznych źródeł czasu.

W celu skonfigurować weryfikacji dwuetapowej na swoim koncie:

1. Wygeneruj jednorazowy kod bezpieczeństwa z użyciem aplikacji uwierzytelniającej na urządzeniu mobilnym. W tym celu wykonaj jedną z następujących czynności:

   - Wprowadź ręcznie klucz tajny w aplikacji uwierzytelniającej.
   - Kliknij opcję **Wyświetl kod QR** i zeskanuj kod QR za pomocą aplikacji uwierzytelniającej.

   Na urządzeniu mobilnym wyświetli się kod bezpieczeństwa.

2. W oknie konfiguracji weryfikacji dwuetapowej określ kod zabezpieczający, wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **Sprawdź i zastosuj**.

Weryfikacja dwuetapowa jest skonfigurowany na Twoim koncie. Możesz uzyskać dostęp do Serwera administracyjnego zgodnie ze swoimi uprawnieniami.

Konfigurowanie weryfikacji dwuetapowej dla własnego konta (opartej na MMC)

Gdy po raz pierwszy zalogujesz się do Kaspersky Security Center po włączeniu weryfikacji dwuetapowej, otworzy się okno umożliwiające skonfigurowanie weryfikacji dwuetapowej konta.

Zanim skonfigurujesz weryfikację dwuetapową dla swojego konta, upewnij się, że aplikacja uwierzytelniająca jest zainstalowana na urządzeniu mobilnym. Upewnij się, że czas na urządzeniu z aplikacją uwierzytelniającą i czas na urządzeniu z Serwerem administracyjnym są zsynchronizowane z czasem UTC, z użyciem zewnętrznych źródeł czasu.

W celu skonfigurować weryfikacji dwuetapowej na swoim koncie:

1. Wygeneruj jednorazowy kod bezpieczeństwa z użyciem aplikacji uwierzytelniającej na urządzeniu mobilnym. W tym celu wykonaj jedną z następujących czynności:

   - Wprowadź ręcznie klucz tajny w aplikacji uwierzytelniającej.
   - Zeskanuj kod QR za pomocą aplikacji uwierzytelniającej.

   Na urządzeniu mobilnym wyświetli się kod zabezpieczający.

2. W oknie **Ustaw weryfikację dwuetapową** określ kod zabezpieczający, wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **OK**.

Weryfikacja dwuetapowa jest skonfigurowany na Twoim koncie. Możesz uzyskać dostęp do Serwera administracyjnego zgodnie ze swoimi uprawnieniami.

Generowanie nowego tajnego klucza

Możesz wygenerować nowy tajny klucz do weryfikacji dwuetapowej dla swojego konta tylko wtedy, gdy jesteś autoryzowany za pomocą weryfikacji dwuetapowej.

W celu wygenerowania nowego tajnego klucza dla konta użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Kliknij nazwę konta użytkownika, dla którego chcesz wygenerować nowy tajny klucz dla weryfikacji dwuetapowej.
3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Ochrona konta**.
4. Na zakładce **Ochrona konta** kliknij odnośnik **Wygeneruj nowy tajny klucz**.
5. W oknie weryfikacji dwuetapowej, które zostanie otwarte, określ nowy klucz zabezpieczeń wygenerowany przez aplikację uwierzytelniającą.
6. Kliknij przycisk **Sprawdź i zastosuj**.

Dla użytkownika jest generowany nowy tajny klucz.

Jeśli zgubisz urządzenie mobilne, możesz zainstalować aplikację uwierzytelniającą na innym urządzeniu mobilnym i wygenerować nowy klucz tajny, aby przywrócić dostęp do Kaspersky Security Center Web Console.

Uniemożliwienie nowym użytkownikom konfigurowania dla siebie weryfikacji dwuetapowej

Aby jeszcze bardziej poprawić bezpieczeństwo dostępu do Kaspersky Security Center Web Console, możesz zabronić nowym użytkownikom konfigurowania dla siebie weryfikacji dwuetapowej.

Jeśli ta opcja jest włączona, użytkownik z wyłączoną weryfikacją dwuetapową, na przykład nowy administrator domeny, nie może skonfigurować dla siebie weryfikacji dwuetapowej. W związku z tym takiego użytkownika nie można uwierzytelnić na Serwerze administracyjnym ani zalogować się do Kaspersky Security Center Web Console bez zgody innego administratora Kaspersky Security Center, który ma już włączoną weryfikację dwuetapową.

Ta opcja jest dostępna, jeśli dla wszystkich użytkowników włączona jest weryfikacja dwuetapowa.

Aby zabronić nowym użytkownikom konfigurowania dla siebie weryfikacji dwuetapowej:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.
2. Na karcie **Bezpieczeństwo uwierzytelniania** okna właściwości przełącz przycisk przełączania **Zabroń nowym użytkownikom konfigurowania weryfikacji dwuetapowej dla siebie** w pozycję włączenia.

Ta opcja nie ma wpływu na konta użytkowników dodane do wykluczeń weryfikacji dwuetapowej.

Aby przyznać użytkownikowi z włączoną weryfikacją dwuetapową dostęp do Kaspersky Security Center Web Console, wyłącz tymczasowo opcję **Zabroń nowym użytkownikom konfigurowania weryfikacji dwuetapowej dla siebie**, poproś użytkownika o włączenie weryfikacji dwuetapowej, a następnie włącz tę opcję z powrotem.

Przypisywanie użytkownika jako właściciela urządzenia z systemem Linux po instalacji Agenta sieciowego

Aby umożliwić użytkownikowi zarejestrowanie się jako właściciel urządzenia z systemem Linux:

1. W Kaspersky Security Center Web Console przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**.

   Otworzy się lista pakietów instalacyjnych.

2. Kliknij pakiet instalacyjny Agenta sieciowego.

   Zostanie otwarte okno właściwości pakietu instalacyjnego.

3. W oknie właściwości pakietu instalacyjnego kliknij **Ustawienia** → **Zaawansowane**.

4. W sekcji **Rejestracja użytkownika jako właściciela urządzenia (tylko Linux)** włącz opcję **Zezwól na uruchomienie narzędzia rejestracji użytkownika po instalacji Agenta sieciowego** i kliknij **Zapisz**.

Narzędzie do rejestracji użytkownika jako właściciela urządzenia można uruchomić z wiersza poleceń na urządzeniu klienckim.

Aby zarejestrować użytkownika jako właściciela urządzenia z systemem Linux na urządzeniu klienckim:

1. Wykonaj następujące polecenie w wierszu poleceń na urządzeniu klienckim:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Wprowadź login i hasło, jeśli zostanie wyświetlony taki monit.

   Jeśli login i hasło znajdują się w pliku odpowiedzi lub pakiecie instalacyjnym Agenta sieciowego, wykonaj następujące polecenie w wierszu poleceń na urządzeniu klienckim:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

Jeśli użytkownik należy do wewnętrznej grupy zabezpieczeń, login musi zawierać nazwę użytkownika.

Jeżeli użytkownik należy do grupy zabezpieczeń Active Directory, login musi zawierać nazwę użytkownika i nazwę domeny.

Jeśli dla użytkownika włączona jest weryfikacja dwuetapowa, należy wprowadzić z aplikacji jednorazowe hasło czasowe (TOTP).

Użytkownik zostanie zarejestrowany jako właściciel urządzenia.

Usuwanie użytkownika lub grupy bezpieczeństwa

Możesz usunąć tylko użytkowników wewnętrznych lub wewnętrzne grupy bezpieczeństwa.

W celu usunięcia użytkownika lub grupy bezpieczeństwa:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz kartę **Użytkownicy** lub **Grupy**.
2. Zaznacz pole obok użytkownika lub grupy bezpieczeństwa, którą chcesz usunąć.
3. Kliknij **Usuń**.
4. W otwartym oknie potwierdzenia kliknij **OK**.

Użytkownik lub grupa bezpieczeństwa zostanie usunięta.

Zmiana hasła do konta użytkownika

Zmiana hasła do własnego konta lub konta innego użytkownika może być konieczna, jeśli obecne hasło wkrótce wygaśnie lub chcesz je zmienić na bezpieczniejsze.

Hasło musi być zgodne z następującymi regułami:

- Hasło musi zawierać od 8 do 256 znaków.
- Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
  - Wielkie litery (A-Z)
  - Małe litery (a-z)
  - Cyfry (0-9)
  - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków "." i "@", gdy "." jest umieszczane przed "@".

Zmiana hasła do własnego konta

Aby edytować hasło do swojego konta:

1. W menu głównym przejdź do ustawień konta i wybierz **Zmień hasło**.
2. Wprowadź aktualne hasło, a następnie określ nowe hasło do połączenia z Kaspersky Security Center.

   Aby zobaczyć wprowadzone hasło kliknij .
3. Jeśli Twoje konto jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** podaj dane uwierzytelniające własnego konta lub konta, które ma uprawnienie Modyfikowanie list ACL obiektów w obszarze funkcjonalnym Funkcje ogólne: Uprawnienia użytkownika.
4. Jeśli dla konta użytego w poprzednim kroku włączona jest weryfikacja dwuetapowa, wprowadź kod bezpieczeństwa wygenerowany przez aplikację uwierzytelniającą na urządzeniu mobilnym.

Zmiana hasła do konta użytkownika wewnętrznego

Aby edytować hasło dla konta użytkownika wewnętrznego:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.

2. Kliknij nazwę konta użytkowników, które chcesz edytować.

3. W otwartym oknie ustawień użytkownika, na karcie **Ogólne** kliknij przycisk **Zmień hasło**.

4. Ustaw nowe hasło dla połączenia użytkownika z Kaspersky Security Center.

   Aby zobaczyć wprowadzone hasło kliknij .

5. W razie potrzeby włącz opcję **Użytkownik musi zmienić hasło przy pierwszym logowaniu**, aby wymusić zmianę hasła przy kolejnym uwierzytelnieniu użytkownika.

6. Jeśli konto użytkownika jest chronione przed nieautoryzowaną modyfikacją, musisz potwierdzić, że masz uprawnienia do wprowadzania zmian na tym koncie. W oknie **Ochrona konta** określ dane uwierzytelniające konta, które ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym Funkcje ogólne: Uprawnienia użytkownika.

7. Jeśli dla konta użytego w poprzednim kroku włączona jest weryfikacja dwuetapowa, wprowadź kod bezpieczeństwa wygenerowany przez aplikację uwierzytelniającą na urządzeniu mobilnym.

Konfigurowanie opcji zmiany hasła za pomocą flag serwera

Aby skonfigurować zmianę hasła, możesz użyć narzędzia klscflag, używając następujących poleceń:

- Konfigurowanie okresu rotacji hasła (flaga `LP_SplPwdChangePeriodDays`)

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <okres rotacji>
  ```

  Gdzie `<okres_rotacji>` to okres czasu w dniach, po którym hasło użytkownika wygasa. Możliwe wartości: 0–730. Jeżeli wartość parametru wynosi 0, rotacja haseł jest wyłączona.

- Konfigurowanie czasu wstępnego ostrzeżenia o konieczności zmiany hasła (flaga `LP_SplPwdChangeNotificationHours`)

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <czas_ostrzeżenia>
  ```

  Gdzie `<czas_ostrzeżenia>` to okres czasu w godzinach, po którym hasło użytkownika wygasa. W tym czasie wyświetla się powiadomienie o konieczności zmiany hasła. Możliwe wartości: 0–17520. Jeżeli wartość parametru wynosi 0, czas ostrzeżenia wynosi 25 procent okresu rotacji hasła.

- Określenie wartości domyślnej opcji **Użytkownik musi zmienić hasło przy pierwszym logowaniu** (flaga `LP_SplPwdForceChange`)

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <wartość>
  ```

  Gdzie możliwe wartości flagi `<wartość>` to:

`1`—Opcja **Użytkownik musi zmienić hasło przy pierwszym logowaniu** jest włączona.

`0`—Opcja **Użytkownik musi zmienić hasło przy pierwszym logowaniu** jest wyłączona.

Aby wyświetlić bieżącą wartość flagi, uruchom następujące polecenie:

```
klscflag.exe -fget -pv .core/.independent -s KLLIM -n <flaga> -t d
```

Gdzie `<flaga>` jest flagą `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` lub `LP_SplPwdForceChange`.

Tworzenie roli użytkownika

W celu utworzenia roli użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Kliknij **Dodaj**.
3. W oknie **Nazwa nowej roli**, które zostanie otwarte, wprowadź nazwę nowej roli.
4. Kliknij **OK**, aby zastosować zmiany.
5. W oknie właściwości roli, które zostanie otwarte, zmień ustawienia roli:
   - Na zakładce **Ogólne** edytuj nazwę roli.
     Nie możesz edytować nazwy predefiniowanej roli.
   - Na zakładce **Ustawienia** edytuj zakres roli oraz zasady i profile skojarzone z rolą.
   - Na zakładce **Prawa dostępu** edytuj uprawnienia dostępu do aplikacji firmy Kaspersky.
6. Kliknij **Zapisz**, aby zachować zmiany.

Nowa rola pojawi się na liście ról użytkownika.

Edytowanie roli użytkownika

W celu edytowania roli użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Kliknij nazwę roli, którą chcesz edytować.
3. W oknie właściwości roli, które zostanie otwarte, zmień ustawienia roli:
   - Na zakładce **Ogólne** edytuj nazwę roli.
     Nie możesz edytować nazwy predefiniowanej roli.

- Na zakładce **Ustawienia** edytuj zakres roli oraz zasady i profile skojarzone z rolą.
- Na zakładce **Prawa dostępu** edytuj uprawnienia dostępu do aplikacji firmy Kaspersky.

4. Kliknij **Zapisz**, aby zachować zmiany.

Zaktualizowana rola pojawi się na liście ról użytkownika.

Edytowanie obszaru roli użytkownika

Obszar roli użytkownika to połączenie użytkowników i grup administracyjnych. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup podrzędnych.

W celu dodania użytkowników, grup bezpieczeństwa i grup administracyjnych do obszaru roli użytkownika, możesz użyć jednej z następujących metod:

Metoda 1:

1. W menu głównym przejdź do opcji **Użytkownicy i role** → **Użytkownicy i grupy**, a następnie wybierz kartę **Użytkownicy** lub **Grupy**.
2. Zaznacz pola obok użytkowników lub grup bezpieczeństwa, które chcesz dodać do obszaru roli użytkownika.
3. Kliknij przycisk **Przypisz rolę**.

   Zostanie uruchomiony Kreator przypisywania roli. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
4. W kroku **Wybierz rolę** wybierz rolę użytkownika, którą chcesz przypisać.
5. W kroku **Zdefiniuj zakres** wybierz grupę administracyjną, którą chcesz dodać do obszaru roli użytkownika.
6. W celu zakończenia działania Kreatora kliknij przycisk **Przypisz rolę**.

Wybrani użytkownicy lub grupy bezpieczeństwa i wybrana grupa administracyjna zostaną dodane do obszaru roli użytkownika.

Metoda 2:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Kliknij nazwę roli, dla której chcesz określić obszar.
3. W otwartym oknie właściwości roli wybierz zakładkę **Ustawienia**.
4. W sekcji **Zakres roli** kliknij **Dodaj**.

   Zostanie uruchomiony Kreator przypisywania roli. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
5. W kroku **Zdefiniuj zakres** wybierz grupę administracyjną, którą chcesz dodać do obszaru roli użytkownika.
6. W kroku **Wybierz użytkowników** wybierz użytkowników i grupy zabezpieczeń, które chcesz dodać do obszaru roli użytkownika.

7. W celu zakończenia działania Kreatora kliknij przycisk **Przypisz rolę**.

8. Kliknij przycisk **Zamknij** (✕), aby zamknąć okno właściwości roli.

Wybrani użytkownicy lub grupy bezpieczeństwa i wybrana grupa administracyjna zostaną dodane do obszaru roli użytkownika.

Metoda 3:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Prawa dostępu** zaznacz pole wyboru obok nazwy użytkownika lub grupy bezpieczeństwa, którą chcesz dodać do obszaru roli użytkownika, a następnie kliknij przycisk **Role**.

   Nie można jednocześnie wybrać wielu użytkowników lub grup bezpieczeństwa. Jeśli wybierzesz więcej niż jeden element, przycisk **Role** będzie nieaktywny.

3. W oknie **Role** wybierz rolę użytkownika, którą chcesz przypisać, a następnie zastosuj i zapisz zmiany.

   Wybrani użytkownicy lub grupy bezpieczeństwa zostaną dodani do obszaru roli użytkownika.

Usuwanie roli użytkownika

W celu usunięcia roli użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.

2. Zaznacz pole obok nazwy roli, którą chcesz usunąć.

3. Kliknij **Usuń**.

4. W otwartym oknie potwierdzenia kliknij **OK**.

Rola użytkownika zostanie usunięta.

Kojarzenie profili zasad z rolami

Możesz skojarzyć role użytkownika z profilami zasad. W tym przypadku reguła aktywacji dla tego profilu zasad jest oparta na roli: profil zasad staje się aktywny dla użytkownika, który posiada określoną rolę.

Na przykład, zasada zabrania wszelkich programów do nawigacji GPS na wszystkich urządzeniach w grupie administracyjnej. Program do nawigacji GPS jest wymagany tylko na jednym urządzeniu w grupie administracyjnej Użytkownicy—na urządzeniu, które należy do użytkownika zatrudnionego w charakterze kuriera. W tym przypadku możesz przypisać rolę „Kurier" do jego właściciela, a następnie utworzyć profil zasad zezwalający na uruchamianie programu do nawigacji GPS tylko na urządzeniach, których właściciele posiadają rolę „Kurier". Wszystkie pozostałe ustawienia zasady zostają zachowane. Tylko użytkownik z rolą „Kurier" będzie mógł uruchamiać program do nawigacji GPS. Później, jeśli innemu pracownikowi przypisano rolę „Kurier", nowy pracownik także może uruchomić program do nawigacji na urządzeniu należącym do organizacji. Uruchamianie programu do nawigacji GPS wciąż będzie zabronione na innych urządzeniach w tej samej grupie administracyjnej.

W celu skojarzenia roli z profilem zasad:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Kliknij nazwę roli, którą chcesz skojarzyć z profilem zasad.

   Okno właściwości roli zostanie otwarte na wybranej zakładce **Ogólne**.
3. Wybierz zakładkę **Ustawienia** i przewiń w dół do sekcji **Profile zasad**.
4. Kliknij **Edytuj**.
5. W celu skojarzenia roli z:

   - **Istniejącym profilem zasad**—kliknij ikonę strzałki (>) obok nazwy żądanej zasady, a następnie zaznacz pole obok profilu, z którym chcesz skojarzyć rolę.
   - **Nowy profil zasad**:

     a. Zaznacz pole obok zasady, dla której chcesz utworzyć profil.

     b. Kliknij **Nowy profil zasad**.

     c. Określ nazwę dla nowego profilu i skonfiguruj ustawienia profilu.

     d. Kliknij przycisk **Zapisz**.

     e. Zaznacz pole obok nowego profilu.
6. Kliknij **Przypisz do roli**.

Profil zostanie skojarzony z rolą i pojawi się we właściwościach roli. Profil jest stosowany automatycznie do dowolnego urządzenia, którego właścicielowi przypisano rolę.

Przydzielanie ról użytkownika do podrzędnych Serwerów administracyjnych

Domyślnie, listy ról użytkownika głównego i podrzędnego Serwera administracyjnego są niezależne. Możesz skonfigurować aplikację w taki sposób, aby automatycznie rozsyłała role użytkownika utworzone na głównym Serwerze administracyjnym do wszystkich podrzędnych Serwerów administracyjnych. Role użytkownika mogą także zostać rozesłane z podrzędnego Serwera administracyjnego na swoje własne podrzędne Serwery administracyjne.

W celu przesłania ról użytkownika z głównego Serwera administracyjnego na podrzędne Serwery administracyjne:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.
2. Przejdź do sekcji **Hierarchia Serwerów administracyjnych**.
3. Włącz opcję **Przekaż listę reguł do podrzędnych Serwerów administracyjnych**, a następnie kliknij przycisk **Zapisz**.

Aplikacja kopiuje role użytkownika głównego Serwera administracyjnego na podrzędne Serwery administracyjne.

Jeśli opcja **Przekaż listę reguł do podrzędnych Serwerów administracyjnych** jest włączona, a role użytkownika są przesyłane, nie mogą być edytowane ani usuwane na podrzędnych Serwerach administracyjnych. Jeśli tworzysz nową rolę lub edytujesz już tę istniejącą na głównym Serwerze administracyjnym, zmiany są automatycznie kopiowane do podrzędnych Serwerów administracyjnych. Jeśli usuwasz rolę użytkownika na głównym Serwerze administracyjnym, ta rola pozostanie na podrzędnych Serwerach administracyjnych, ale może być edytowana lub zostać usunięta.

Role, które są przesyłane na podrzędny Serwer administracyjny z Serwera głównego, są wyświetlane z zielonymi znacznikami wyboru (✓). Nie możesz edytować tych ról na podrzędnym Serwerze administracyjnym.

Jeśli tworzysz rolę na głównym Serwerze administracyjnym i istnieje rola z tą samą nazwą na swoim podrzędnym Serwerze administracyjnym, nowa rola zostaje skopiowana do podrzędnego Serwera administracyjnego z indeksem dodanym do jego nazwy, na przykład: ~~1, ~~2 (indeks może być losowy).

Jeśli wyłączysz opcję **Przekaż listę reguł do podrzędnych Serwerów administracyjnych**, wszystkie role użytkownika pozostaną na podrzędnych Serwerach administracyjnych, ale staną się niezależne od tych na głównym Serwerze administracyjnym. Po tym, jak role użytkownika staną się niezależne, role użytkownika na podrzędnych Serwerach administracyjnych mogą być edytowane lub usuwane.

Zmiana hasła do konta

Hasło do konta lokalnego możesz zmienić na przykład wtedy, gdy użytkownik zapomni hasła do konta lokalnego lub w celu zaplanowanej zmiany hasła.

Zmiana hasła będzie obowiązywać nawet jeśli użytkownik nie zalogował się do konta. Możesz także zmienić hasło do lokalnego konta root.

To zadanie można wykonać tylko na urządzeniach z systemem Linux.

Aby zmienić hasło do konta lokalnego na określonych urządzeniach:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W polu **Typ zadania** wybierz opcję **Zmień hasło do konta (tylko Linux)**.
4. Wybierz jedną z następujących opcji:

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

     Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

  Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

  Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

- **Przypisz zadanie do wyboru urządzeń**

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

Dla określonych urządzeń tworzone jest zadanie *Zmień hasło do konta (tylko w przypadku systemu Linux)*. Jeśli wybrano opcję **Przypisz zadanie do grupy administracyjnej**, zadanie jest zadaniem grupowym.

5. W kroku **Zakres zadania** określ grupę administracyjną, urządzenia o określonych adresach lub wybór urządzeń.

   Dostępne ustawienia zależą od opcji wybranej w poprzednim kroku.

6. W kroku **Wprowadź nazwę użytkownika i nowe hasło** określ następujące ustawienia:

   - W polu **Nazwa konta** podaj nazwę konta, dla którego chcesz zmienić hasło.
   - W polu **Nowe hasło** podaj hasło, które zostanie ustawione dla konta podanego w poprzednim polu.

     Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.
   - W razie potrzeby zaznacz pole wyboru **Ustaw jako hasło jednorazowe (użytkownik musi zmienić hasło po pierwszym zalogowaniu)**.

     - **Ustaw jako hasło jednorazowe (użytkownik musi zmienić hasło po pierwszym zalogowaniu)**

       Jeżeli to pole wyboru jest zaznaczone, użytkownik zostanie poproszony o ustawienie nowego hasła po pierwszym logowaniu.

       Jeśli to pole wyboru nie jest zaznaczone, użytkownik nie będzie proszony o ustawienie nowego hasła po pierwszym logowaniu.

       Domyślnie pole to nie jest zaznaczone.

7. Na etapie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby utworzyć zadanie i zamknąć kreatora.

   Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, zostanie otwarte okno ustawień zadania. W tym oknie możesz sprawdzić parametry zadania, zmodyfikować je lub skonfigurować harmonogram uruchamiania zadania, jeśli to konieczne.

8. Na liście zadań wybierz utworzone zadanie, a następnie kliknij przycisk **Start**.

   Ewentualnie poczekaj na uruchomienie zadania zgodnie z harmonogramem określonym w ustawieniach zadania.

Po zakończeniu zadania zmiany hasła do konta hasło dla określonego konta lokalnego na określonych urządzeniach zostanie zmienione.

Aby zapewnić poprawne działanie zadań zmiany hasła do konta, opcja SELinux musi być wyłączona na urządzeniu użytkownika.

Wycofanie uprawnień lokalnego administratora

Możesz wycofać uprawnienia administratora lokalnego z kont. Zapewnia to dodatkową warstwę kontroli nad kontami użytkowników. Można na przykład wycofać uprawnienia administratora lokalnego po zakończeniu jednorazowego przypisania.

Po uruchomieniu tego zadania sprawdzane jest określone konto lokalne, czy należy do lokalnych grup administratorów. Grupy te są zdefiniowane w ustawieniach zasad Agenta sieciowego. Możesz dostosować listę lokalnych grup administratorów w ustawieniach zasad Agenta sieciowego. Możesz także sprawdzić listę kont użytkowników uprzywilejowanych, korzystając z **Raport o uprzywilejowanych użytkownikach urządzenia (tylko Linux)**.

To zadanie można wykonać tylko na urządzeniach z systemem Linux.

Aby wycofać uprawnienia administratora lokalnego z określonych urządzeń:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W polu **Typ zadania** wybierz opcję **Odbierz uprawnienia administratora lokalnego (tylko Linux)**.
4. Wybierz jedną z następujących opcji:

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

     Jeśli zadanie jest przypisane do grupy administracyjnej, zakładka **Zabezpieczenia** nie jest wyświetlana w oknie właściwości zadania, ponieważ zadania grupowe podlegają ustawieniom zabezpieczeń grup, do których się odnoszą.

   - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

     Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

     Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

   - **Przypisz zadanie do wyboru urządzeń**

     Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

Dla określonych urządzeń tworzone jest zadanie *Odbierz uprawnienia administratora lokalnego (tylko w przypadku systemu Linux)*. Jeśli wybrano opcję **Przypisz zadanie do grupy administracyjnej**, zadanie jest zadaniem grupowym.

5. W kroku **Zakres zadania** określ grupę administracyjną, urządzenia o określonych adresach lub wybór urządzeń.

   Dostępne ustawienia zależą od opcji wybranej w poprzednim kroku.

6. W tym kroku kreatora należy ustawić następujące ustawienia:

   - W grupie ustawień **Tryb pracy** wybierz tryb pracy:

     - **Cofnij uprawnienia administratora lokalnego wymienionym kontom**

       Jeśli ta opcja zostanie wybrana, uprawnienia administratora lokalnego zostaną wycofane z określonych kont lokalnych.

       Domyślnie opcja ta jest zaznaczona.

     - **Wyklucz wymienione konta z możliwości cofnięcia uprawnień administratora lokalnego**

       Jeśli ta opcja zostanie wybrana, uprawnienia administratora lokalnego zostaną odebrane wszystkim kontom lokalnym, z wyjątkiem określonych.

       Domyślnie ta opcja nie jest zaznaczona.

   - Określ konta lokalne:

     - Kliknij **Dodaj**.

     - W otwartym oknie wykonaj następujące czynności:

       - W polu **Nazwa konta** podaj nazwę nowego zadania.

       - Wybierz działanie w grupie ustawień **Działanie na koncie** (dostępnej tylko w przypadku zaznaczenia opcji **Cofnij uprawnienia administratora lokalnego wymienionym kontom**).

       - **Zachowaj konto**

         Jeżeli ta opcja jest zaznaczona, konto lokalne nie zostanie usunięte po odebraniu uprawnień administratora lokalnego.

         Domyślnie opcja ta jest zaznaczona.

       - **Usuń konto**

         W przypadku wybrania tej opcji konto lokalne zostanie usunięte niezależnie od tego, czy posiada uprawnienia administratora lokalnego.

         Domyślnie ta opcja nie jest zaznaczona.

7. Na etapie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby utworzyć zadanie i zamknąć kreatora.

   Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, zostanie otwarte okno ustawień zadania. W tym oknie możesz sprawdzić parametry zadania, zmodyfikować je lub skonfigurować harmonogram uruchamiania zadania, jeśli to konieczne.

8. Na liście zadań wybierz utworzone zadanie, a następnie kliknij przycisk **Start**.

   Ewentualnie poczekaj na uruchomienie zadania zgodnie z harmonogramem określonym w ustawieniach zadania.

Po zakończeniu zadania wycofania uprawnień administratora lokalnego uprawnienia administratora lokalnego zostaną wycofane z określonych kont lokalnych na określonych urządzeniach.

Zarządzanie rewizjami obiektów

Ta sekcja zawiera informacje dotyczące zarządzania rewizjami obiektów. Kaspersky Security Center umożliwia śledzenie modyfikacji obiektów. Za każdym razem, gdy zapisujesz zmiany wprowadzone w obiekcie, tworzona jest *rewizja*. Każda rewizja posiada numer.

Obiekty aplikacji, które obsługują zarządzanie rewizjami, obejmują:

- Właściwości Serwera administracyjnego
- Zasady
- Zadania
- Grupy administracyjne
- Konta użytkowników
- Pakiety instalacyjne

Na rewizjach obiektów możesz wykonać następujące działania:

- Wyświetlić wybraną rewizję (opcja dostępna tylko w przypadku zasad)
- Wycofać zmiany wprowadzone w obiekcie dla wybranej rewizji
- Zapisać wersje jako plik JSON (opcja dostępna tylko w przypadku zasad)

W oknie właściwości dowolnego obiektu obsługującego zarządzanie rewizjami sekcja **Historia rewizji** wyświetla listę rewizji obiektów z następującymi szczegółami:

- **Zmiana** — Numer rewizji obiektu.
- **Czas** — Data i godzina modyfikacji obiektu.
- **Użytkownik** — Nazwa użytkownika, który zmodyfikował obiekt.
- **Adres IP urządzenia użytkownika** — Adres IP urządzenia, z którego obiekt został zmodyfikowany.
- **Adres IP Web Console** — Adres IP Kaspersky Security Center Web Console, za pomocą którego obiekt został zmodyfikowany.
- **Akcja** — Działanie wykonane na obiekcie.
- **Opis** — Opis rewizji związanej ze zmianą wprowadzoną w ustawieniach obiektu.

  Domyślnie, pole opisu rewizji obiektu jest puste. Aby dodać opis do rewizji, wybierz żądaną rewizję i kliknij przycisk **Edytuj opis**. W otwartym oknie wprowadź tekst opisu rewizji.

Przywracanie poprzedniej wersji obiektu

Jeśli to konieczne, możesz wycofać zmiany wprowadzone w obiekcie. Na przykład, konieczne może być przywrócenie ustawień zasady z określonego dnia.

W celu wycofania zmian wprowadzonych w obiekcie:

1. W oknie właściwości obiektu otwórz zakładkę **Historia rewizji**.
2. Na liście rewizji obiektu wybierz rewizję, do której chcesz wycofać zmiany.
3. Kliknij przycisk **Wycofaj**.
4. Kliknij **OK**, aby potwierdzić działanie.

Obiekt zostanie wycofany do wybranej rewizji. Lista rewizji obiektu wyświetla wpis dotyczący podjętego działania. Opis rewizji wyświetla informacje o numerze rewizji, do której wycofałeś obiekt.

Operacja wycofywania jest dostępna tylko w przypadku obiektów zasad i zadań.

Dodawanie opisu rewizji

Kaspersky Security Center umożliwia śledzenie modyfikacji obiektów. Za każdym razem, gdy zapisujesz zmiany wprowadzone w obiekcie, tworzona jest rewizja. Każda rewizja posiada numer.

Możesz dodać opis dla rewizji, aby uprościć wyszukiwanie rewizji na liście.

W celu dodania opisu rewizji:

1. W oknie właściwości obiektu otwórz zakładkę **Historia rewizji**.
2. Na liście rewizji obiektu wybierz rewizję, dla której chcesz dodać opis.
3. Kliknij przycisk **Edytuj opis**.
   Zostanie otwarte okno **Opis**.
4. W oknie **Opis** wprowadź opis rewizji.
   Domyślnie, pole opisu rewizji obiektu jest puste.
5. Zapisz opis rewizji.

Opis jest dodawany do wersji obiektu.

Wyświetlanie i zapisywanie rewizji zasady

Kaspersky Security Center umożliwia sprawdzenie, jakie modyfikacje zostały wprowadzone w zasadzie w określonym przedziale czasu, a także zapisanie informacji o tych modyfikacjach w pliku.

Przeglądanie i zapisywanie rewizji zasad jest możliwe, jeśli odpowiednia wtyczka webowa do zarządzania obsługuje tę funkcję.

Aby wyświetlić rewizję zasad:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Kliknij zasadę dotyczącą wersji, którą chcesz wyświetlić, a następnie przejdź do sekcji **Historia rewizji**.
3. Na liście rewizji zasad kliknij numer rewizji, którą chcesz wyświetlić.

   Jeśli rozmiar rewizji jest większy niż 10 MB, nie będzie można jej wyświetlić przy użyciu Kaspersky Security Center Web Console. Wyświetlony zostanie monit o zapisanie wybranej wersji w pliku JSON.

   Jeżeli rozmiar rewizji nie przekracza 10 MB, wyświetlony zostanie raport w formacie HTML z ustawieniami wybranej rewizji zasady. Ponieważ raport jest wyświetlany w wyskakującym oknie, upewnij się, że w Twojej przeglądarce dozwolone są wyskakujące okienka.

Aby zapisać rewizję zasady w pliku JSON,

Na liście rewizji zasad wybierz rewizję, którą chcesz zapisać, a następnie kliknij **Zapisz do pliku**.

Rewizja zostanie zapisana w pliku JSON.

Usuwanie obiektów

W tej sekcji znajdują się informacje dotyczące usuwania obiektów.

Możesz usuwać obiekty, w tym:

- Zasady
- Zadania
- Pakiety instalacyjne
- Wirtualne Serwery administracyjne
- Użytkownicy
- Grupy bezpieczeństwa
- Grupy administracyjne

W celu usunięcia obiektu:

1. Otwórz wymaganą sekcję Kaspersky Security Center Web Console, a następnie wybierz obiekt.
2. Na pasku narzędzi kliknij przycisk **Usuń**.
3. W otwartym oknie kliknij **OK**, aby potwierdzić swój wybór.

   Wybrany obiekt zostanie usunięty.

Jeśli usuniesz obiekt, informacje o nim pozostaną w bazie danych. Okres przechowywania informacji o usuniętych obiektach jest taki sam, jak okres przechowywania rewizji obiektu (zalecany okres wynosi 90 dni). Możesz zmienić okres przechowywania tylko wtedy, gdy posiadasz uprawnienie **Modyfikacja** w obszarze uprawnień **Usunięte obiekty**.

Informacje o usuwaniu urządzeń klienckich

Gdy usuniesz urządzenie zarządzane z grupy administracyjnej, aplikacja przeniesie je do grupy Urządzenia nieprzypisane. Po usunięciu urządzenia zainstalowane aplikacje Kaspersky — Agent sieciowy i dowolna aplikacja zabezpieczająca, na przykład Kaspersky Endpoint Security — pozostają na urządzeniu.

Kaspersky Security Center obsługuje urządzenia w grupie Urządzenia nieprzypisane zgodnie z następującymi zasadami:

- Jeśli skonfigurowałeś reguły przenoszenia urządzeń i urządzenie spełnia kryteria reguły przenoszenia, urządzenie jest automatycznie przenoszone do grupy administracyjnej zgodnie z regułą.
- Urządzenie jest przechowywane w grupie Urządzenia nieprzypisane i automatycznie usuwane z grupy zgodnie z regułami przechowywania urządzeń.

  Reguły przechowywania urządzeń nie mają wpływu na urządzenia, które mają jeden lub więcej napędów zaszyfrowanych za pomocą pełnego szyfrowania dysku. Takie urządzenia nie są usuwane automatycznie — można je usunąć tylko ręcznie. Jeśli chcesz usunąć urządzenie z zaszyfrowanym dyskiem, najpierw odszyfruj dysk, a następnie usuń urządzenie.

  > Przy usuwaniu urządzenia z zaszyfrowanym dyskiem dane wymagane do odszyfrowania dysku są również usuwane. Jeżeli zaznaczysz pole **Rozumiem ryzyko i chcę usunąć wybrane urządzenia** w oknie potwierdzenia otwierającym się po usunięciu takich urządzeń (z grupy **Urządzenia nieprzypisane** lub z grupy **Zarządzane urządzenia**), oznacza to, że masz świadomość związanego z tym usunięcia danych.

  Aby odszyfrować dysk, muszą zostać spełnione następujące warunki:

  - Urządzenie zostaje ponownie podłączone do Serwera administracyjnego w celu przywrócenia danych wymaganych do odszyfrowania dysku.
  - Użytkownik urządzenia zapamięta hasło do odszyfrowania.
  - Aplikacja zabezpieczająca, która została użyta do zaszyfrowania dysku, na przykład Kaspersky Endpoint Security for Windows, jest nadal zainstalowana na urządzeniu.

Jeśli dysk został zaszyfrowany przy użyciu technologii Kaspersky Disk Encryption, możesz również spróbować odzyskiwania danych przy użyciu narzędzia FDERT Restore Utility.

W przypadku VDI, jeśli masz urządzenie z zaszyfrowanymi dyskami, informacje na zaszyfrowanym dysku zostaną usunięte po usunięciu urządzenia.

Gdy ręcznie usuniesz urządzenie z grupy Urządzenia nieprzypisane, aplikacja usunie je z listy. Po usunięciu urządzenia zainstalowane aplikacje Kaspersky (jeśli istnieją) pozostają na urządzeniu. Następnie, jeśli urządzenie jest nadal widoczne dla Serwera administracyjnego i przeprowadzona została regularna konfiguracja przeszukiwania sieci Kaspersky Security Center wykrywa urządzenie podczas przeszukiwania sieci i dodaje je z powrotem do grupy Urządzenia nieprzypisane. Dlatego też wskazane jest ręczne usunięcie urządzenia tylko wtedy, gdy jest ono niewidoczne dla Serwera administracyjnego.

Kaspersky Security Network (KSN)

Ta sekcja opisuje sposób korzystania z infrastruktury usług online o nazwie Kaspersky Security Network (KSN). Sekcja zawiera szczegóły dotyczące KSN, a także instrukcje związane z włączaniem KSN, konfiguracją dostępu do KSN oraz wyświetlaniem statystyk korzystania z serwera proxy KSN.

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), przy czym funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Informacje o KSN

Kaspersky Security Network (KSN) jest to usługa sieciowa oferująca dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji Kaspersky po wykryciu zagrożeń, ulepszenie działania niektórych składników ochrony oraz zmniejszenie ryzyka fałszywych alarmów. KSN umożliwia korzystanie z baz danych reputacji firmy Kaspersky, z których pobierane są informacje o aplikacjach zainstalowanych na zarządzanych urządzeniach.

Kaspersky Security Center obsługuje następujące rozwiązania infrastrukturalne:

- *KSN* to rozwiązanie umożliwiające wymianę informacji z Kaspersky Security Network. Uczestnicząc w KSN, wyrażasz zgodę na wysyłanie do Kaspersky w trybie automatycznym informacji dotyczących działania aplikacji firmy Kaspersky, zainstalowanych na urządzeniach klienckich, które są zarządzane przez Kaspersky Security Center. Informacje są wysyłane zgodnie z bieżącymi ustawieniami dostępu KSN. Analitycy firmy Kaspersky dodatkowo analizują otrzymane informacje i umieszczają je w reputacyjnych i statystycznych bazach danych Kaspersky Security Network. Kaspersky Security Center domyślnie korzysta z tego rozwiązania.

- *Kaspersky Private Security Network (KPSN)* to rozwiązanie, które umożliwia użytkownikom urządzeń z zainstalowanymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do Globalnej sieci KSN z ich własnych urządzeń. Sieć KPSN została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z jednego z następujących powodów:

  - Urządzenia użytkowników nie są podłączone do internetu.

  - Przekazywanie jakichkolwiek danych poza granice kraju lub poza korporacyjną sieć LAN jest zabronione przez prawo lub ograniczone przez korporacyjną politykę bezpieczeństwa.

  Możesz skonfigurować ustawienia dostępu do Kaspersky Private Security Network w sekcji **Ustawienia KSN Proxy** w oknie właściwości Serwera administracyjnego.

Aplikacja wyświetla pytanie o przyłączenie się do KSN podczas działania kreatora wstępnej konfiguracji. Można rozpocząć lub zakończyć korzystanie z KSN w dowolnym momencie, podczas korzystania z aplikacji.

Korzystasz z KSN zgodnie z Oświadczeniem KSN, które czytasz i akceptujesz, gdy włączasz KSN. Jeśli Oświadczenie KSN zostanie zaktualizowane, zostanie wyświetlone podczas aktualizacji Serwera administracyjnego. Możesz zaakceptować zaktualizowane Oświadczenie KSN lub odrzucić je. Jeśli odrzucisz Oświadczenie, będziesz nadal korzystać z KSN zgodnie z poprzednią wersją Oświadczenia KSN, które zaakceptowałeś wcześniej.

Gdy KSN jest włączone, Kaspersky Security Center sprawdza, czy serwery KSN są dostępne. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Jest to konieczne, aby zapewnić utrzymanie poziomu bezpieczeństwa zarządzanych urządzeń.

Urządzenia klienckie zarządzane przez Serwer administracyjny wchodzą w interakcję z KSN poprzez serwer KSN proxy. Serwer proxy KSN posiada następujące cechy:

- Urządzenia klienckie mogą wysyłać żądania do KSN, otrzymywać informacje z KSN oraz przesyłać informacje do KSN nawet wtedy, gdy nie mają bezpośredniego dostępu do internetu.

- Serwer KSN proxy buforuje przetwarzane dane, ograniczając obciążenie połączenia wychodzącego i czas oczekiwania na informacje żądane przez urządzenie klienckie.

Serwer KSN Proxy można skonfigurować w sekcji **Ustawienia KSN Proxy** dostępnej w oknie właściwości Serwera administracyjnego.

Konfigurowanie dostępu do KSN

Możesz skonfigurować dostęp do Kaspersky Security Network (KSN) na Serwerze administracyjnym i na punkcie dystrybucji.

W celu skonfigurowania dostępu Serwera administracyjnego do KSN:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.

3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Włączono**.

   Jeśli ta opcja jest włączona, serwer proxy KSN wysyła dane do KSN w celu zwiększenia efektywności działania komponentów Kaspersky Security Center i poprawienia działania aplikacji Kaspersky. Dane są wysyłane z urządzeń klienckich do KSN zgodnie z zasadą Kaspersky Endpoint Security, która jest aktywna na tych urządzeniach klienckich. Jeśli to pole jest odznaczone, żadne dane nie będą wysyłane do KSN z Serwera administracyjnego i urządzeń klienckich poprzez Kaspersky Security Center. Jednakże urządzenia klienckie mogą wysyłać dane bezpośrednio do KSN (z pominięciem Kaspersky Security Center) zgodnie z ich ustawieniami. Zasada Kaspersky Endpoint Security, aktywna na urządzeniach klienckich, określa, które dane będą wysyłane bezpośrednio z tych urządzeń do KSN (z pominięciem Kaspersky Security Center).

4. Przełącz przycisk przełącznika na pozycję **Użyj Kaspersky Security Network Włączono**.

   Jeśli ta opcja jest włączona, urządzenia klienckie będą wysyłać wyniki instalacji łat do Kaspersky. Przed włączeniem tej opcji należy przeczytać i zaakceptować warunki Oświadczenia KSN.

   Jeśli używasz sieci KPSN, ustaw przycisk przełącznika opcji **Oświadczenie Kaspersky Private Security Network Włączone** i kliknij przycisk **Określ plik z ustawieniami KSN**, aby pobrać ustawienia prywatnej sieci KPSN (pliki z rozszerzeniami pkcs7 i pem). Po pobraniu ustawień, interfejs wyświetla kontakty i nazwę dostawcy, a także datę utworzenia pliku z ustawieniami prywatnej sieci KPSN.

   > Jeśli włączysz sieć KPSN, zwróć uwagę na punkty dystrybucji skonfigurowane do wysyłania żądań KSN bezpośrednio do Cloud KSN. Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej) będzie nadal wysyłał żądania KSN do Cloud KSN. Aby ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do sieci KPSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji. Możesz włączyć tę opcję we właściwościach punktu dystrybucji lub w zasadzie Agenta sieciowego.

   Po ustawieniu przycisku przełącznika opcji **Oświadczenie Kaspersky Private Security Network Włączone**, pojawi się komunikat ze szczegółami dotyczącymi sieci KPSN.

   Sieć KPSN jest obsługiwane przez następujące aplikacje Kaspersky:

   - Kaspersky Security Center
   - Kaspersky Endpoint Security for Windows
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
   - Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

   Jeśli włączysz sieć KPSN w Kaspersky Security Center, te aplikacje otrzymają informację o obsłudze KPSN. W oknie ustawień aplikacji, w podsekcji **Kaspersky Security Network** sekcji **Zaawansowana ochrona przed zagrożeniami** wyświetlana jest informacja dotycząca wybranego dostawcy sieci KSN – KSN lub KPSN.

Jeśli podczas działania sieci KPSN korzystasz z wcześniejszej wersji aplikacji Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 lub Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent, zalecamy korzystanie z podrzędnych Serwerów administracyjnych, dla których włączono korzystanie z sieci KPSN.

Kaspersky Security Center nie wysyła żadnych danych statystycznych do Kaspersky Security Network, jeśli sieć KPSN została skonfigurowana w sekcji **Ustawienia KSN Proxy** okna właściwości Serwera administracyjnego.

5. Jeśli skonfigurowałeś ustawienia serwera proxy we właściwościach Serwera administracyjnego, ale Twoja sieć wymaga, abyś korzystał bezpośrednio z prywatnej sieci KSN, włącz opcję **Ignoruj ustawienia serwera proxy w przypadku łączenia z KPSN**. W przeciwnym razie, żądania z zarządzanych aplikacji nie będą mogły dotrzeć do KPSN.

6. Skonfiguruj połączenie Serwera administracyjnego z usługą KSN proxy:

   - W sekcji **Ustawienia połączenia**, w polu **Port TCP** określ numer portu TCP, który będzie używany do nawiązywania połączenia z serwerem proxy KSN. Domyślny port do nawiązywania połączenia z serwerem KSN proxy to 13111.

   - Jeśli chcesz, żeby Serwer administracyjny nawiązywał połączenie z serwerem proxy KSN poprzez port UDP, włącz opcję **Użyj portu UDP** i w polu **Port UDP** określ numer portu. Domyślnie opcja ta jest wyłączona i używany jest port TCP. Jeśli ta opcja jest włączona, domyślny port UDP do nawiązywania połączenia z serwerem KSN proxy to 15111.

   - Jeśli chcesz, żeby Serwer administracyjny nawiązywał połączenie z serwerem proxy KSN poprzez port HTTPS, włącz opcję **Użyj HTTPS** i w polu **HTTPS przez port** określ numer portu. Domyślnie opcja ta jest wyłączona i używany jest port TCP. Jeśli ta opcja jest włączona, domyślny port HTTPS do nawiązywania połączenia z serwerem KSN proxy to 17111.

7. Przełącz przycisk przełącznika na pozycję **Połącz podrzędne Serwery administracyjne z KSN przez główny Serwer administracyjny Włączone**.

   Jeśli ta opcja jest włączona, podrzędne Serwery administracyjne używają głównego Serwera administracyjnego jako serwera KSN proxy. Jeśli ta opcja jest wyłączona, podrzędne Serwery administracyjne same łączą się z KSN. W tym przypadku zarządzane urządzenia używają podrzędnych Serwerów administracyjnych jako serwerów KSN proxy.

   Podrzędne Serwery administracyjne używają głównego Serwera administracyjnego jako serwera proxy, jeśli w prawej części sekcji **Ustawienia KSN Proxy**, dostępnej we właściwościach podrzędnych Serwerów administracyjnych, przycisk przełącznika jest ustawiony w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Włączono**.

8. Kliknij przycisk **Zapisz**.

   Ustawienia dostępu do KSN zostaną zapisane.

Możesz także skonfigurować dostęp punktu dystrybucji do KSN, na przykład, jeśli chcesz zmniejszyć obciążenie na Serwerze administracyjnym. Punkt dystrybucji działający jako serwer KSN proxy wysyła żądania KSN z zarządzanych urządzeń bezpośrednio do Kaspersky, bez używania Serwera administracyjnego.

W celu skonfigurowania dostępu punktu dystrybucji do Kaspersky Security Network (KSN):

1. Upewnij się, że punkt dystrybucji został przypisany ręcznie.
2. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.
3. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.
4. Kliknij nazwę punktu dystrybucji, aby otworzyć okno właściwości.
5. W oknie właściwości punktu dystrybucji, w sekcji **KSN Proxy** włącz opcję **Włącz KSN Proxy po stronie punktu dystrybucji**, a następnie włącz opcję **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**.
6. Kliknij **OK**.

Punkt dystrybucji będzie działał jako serwer KSN proxy.

Włączanie i wyłączanie korzystania z KSN

Aby umożliwić korzystanie z KSN:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.
2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.
3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Włączono**.

Serwer proxy KSN jest włączony i wysyła dane do KSN w celu zwiększenia efektywności działania komponentów Kaspersky Security Center i usprawnienia działania aplikacji Kaspersky.

1. W zależności od używanego rozwiązania infrastruktury KSN włącz odpowiednie przyciski przełączające.

   - Jeśli korzystasz z Globalnej sieci KSN, ustaw przycisk przełącznika w pozycji **Użyj Kaspersky Security Network Włączono**.

     Wysyłanie danych do KSN jest już możliwe. Przed włączeniem tej opcji należy przeczytać i zaakceptować warunki Oświadczenia KSN.

   - Jeśli używasz sieci KPSN, ustaw przycisk przełącznika w pozycji **Oświadczenie Kaspersky Private Security Network Włączone** i kliknij przycisk ustawień **Określ plik z ustawieniami KSN**, aby pobrać ustawienia sieci KPSN (pliki z rozszerzeniami pkcs7 i pem). Po pobraniu ustawień, interfejs wyświetla kontakty i nazwę dostawcy, a także datę utworzenia pliku z ustawieniami prywatnej sieci KPSN.

     Po ustawieniu przycisku przełącznika w pozycji **Oświadczenie Kaspersky Private Security Network Włączone**, pojawi się komunikat ze szczegółami dotyczącymi sieci KPSN.
2. Kliknij przycisk **Zapisz**.

Aby wyłączyć korzystanie z KSN:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.

3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Wyłączono**, aby wyłączyć usługę KSN Proxy.

4. Kliknij przycisk **Zapisz**.

Przeglądanie zaakceptowanego Oświadczenia KSN

Po włączeniu Kaspersky Security Network (KSN) musisz przeczytać i zaakceptować Oświadczenie KSN. W każdej chwili możesz przejrzeć zaakceptowane Oświadczenie KSN.

W celu przejrzenia zaakceptowanego Oświadczenia KSN:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.

3. Kliknij odnośnik **Zobacz Oświadczenie Kaspersky Security Network**.

W otwartym oknie możesz przejrzeć treść zaakceptowanego Oświadczenia KSN.

Akceptowanie zaktualizowanego Oświadczenia KSN

Korzystasz z KSN zgodnie z Oświadczeniem KSN, które czytasz i akceptujesz, gdy włączasz KSN. Jeśli Oświadczenie KSN zostanie zaktualizowane, zostanie wyświetlone podczas aktualizacji Serwera administracyjnego. Możesz zaakceptować zaktualizowane Oświadczenie KSN lub odrzucić je. Jeśli odrzucisz Oświadczenie, będziesz kontynuować korzystanie z KSN zgodnie z wersją Oświadczenia KSN, którą zaakceptowałeś wcześniej.

Po uaktualnieniu wersji Serwera administracyjnego zaktualizowane Oświadczenie KSN zostanie wyświetlona automatycznie. Jeśli odrzucisz zaktualizowane Oświadczenie KSN, nadal możesz je przejrzeć i zaakceptować później.

W celu wyświetlenia, a następnie zaakceptowania lub odrzucenia zaktualizowanego Oświadczenia KSN:

1. Kliknij odnośnik **Wyświetl powiadomienia** znajdujący się w prawym górnym rogu okna głównego aplikacji.

   Zostanie otwarte okno **Powiadomienia**.

2. Kliknij odnośnik **Wyświetl zaktualizowane Oświadczenie KSN**.

   Zostanie otwarte okno **Aktualizacja Oświadczenia Kaspersky Security Network**.

3. Przeczytaj Oświadczenie KSN, a następnie podejmij decyzję, klikając jeden z następujących przycisków:

   - **Akceptuję zaktualizowane Oświadczenie KSN**
   - **Użyj KSN w ramach starego Oświadczenia**

W zależności od Twojego wyboru KSN działa zgodnie z warunkami aktualnego lub zaktualizowanego Oświadczenia KSN. Możesz wyświetlić tekst zaakceptowanego Oświadczenia KSN we właściwościach Serwera administracyjnego w dowolnym momencie.

Sprawdzanie, czy punkt dystrybucji działa jako serwer proxy KSN

Na zarządzanym urządzeniu przypisanym do pracy jako punkt dystrybucji możesz włączyć serwer proxy KSN. Zarządzane urządzenie działa jako serwer proxy KSN, gdy usługa ksnproxy jest uruchomiona na urządzeniu. Możesz lokalnie sprawdzić, włączyć lub wyłączyć tę usługę na urządzeniu.

Jako punkt dystrybucji można przypisać urządzenie z systemem Windows lub Linux. Metoda sprawdzania punktu dystrybucji zależy od systemu operacyjnego tego punktu dystrybucji.

Aby sprawdzić, czy punkt dystrybucji oparty na systemie Windows działa jako serwer proxy KSN:

1. Na urządzeniu punktu dystrybucji, w systemie Windows otwórz **Usługi** (**Wszystkie programy** → **Narzędzia administracyjne** → **Usługi**).

2. Na liście usług sprawdź, czy usługa ksnproxy jest uruchomiona.

   Jeśli usługa ksnproxy jest uruchomiona, Agent sieciowy na urządzeniu uczestniczy w Kaspersky Security Network i działa jako serwer proxy KSN dla zarządzanych urządzeń należących do obszaru punktu dystrybucji.

Jeśli chcesz, możesz wyłączyć usługę ksnproxy. W takim przypadku Agent sieciowy w punkcie dystrybucji przestaje uczestniczyć w Kaspersky Security Network. To działanie wymaga uprawnień administratora lokalnego.

Aby sprawdzić, czy punkt dystrybucji oparty na systemie Linux działa jako serwer proxy KSN:

1. Na urządzeniu punktu dystrybucji wyświetl listę uruchomionych procesów.

2. Na liście uruchomionych procesów sprawdź, czy proces `/opt/kaspersky/ksc64/sbin/ksnproxy` jest uruchomiony.

Jeśli proces `/opt/kaspersky/ksc64/sbin/ksnproxy` jest uruchomiony, Agent sieciowy na urządzeniu uczestniczy w Kaspersky Security Network i działa jako serwer proxy KSN dla zarządzanych urządzeń należących do obszaru punktu dystrybucji.

Scenariusz: Aktualizowanie Kaspersky Security Center i zarządzanych aplikacji zabezpieczających

Ta sekcja opisuje główny krótki scenariusz aktualizacji Kaspersky Security Center i zarządzanych aplikacji zabezpieczających.

Aktualizacja Kaspersky Security Center i zarządzanych aplikacji zabezpieczających odbywa się w etapach:

1. **Sprawdzanie wymagań sprzętowych i programowych**

   Upewnij się, że sprzęt spełnia wymagania i zainstaluj wymagane aktualizacje.

2. **Rozplanowywanie zasobów**

   Oceń, ile miejsca na dysku zajmuje Twoja baza danych. Upewnij się, że posiadasz wystarczającą ilość miejsca na dysku do przechowywania kopii zapasowej ustawień i bazy danych Serwera administracyjnego.

3. **Uzyskiwanie pliku instalatora dla Kaspersky Security Center**

   Uzyskiwanie pliku wykonywalnego dla bieżącej wersji Kaspersky Security Center i zapisywanie go na urządzeniu, które działa jako Serwer administracyjny. Zapoznaj się z Informacjami o kompilacji dla nowej wersji Kaspersky Security Center, której chcesz użyć.

4. **Tworzenie kopii zapasowej poprzedniej wersji**

   Użyj narzędzia do tworzenia kopii zapasowej i odzyskiwania danych, aby utworzyć kopię zapasową danych Serwera administracyjnego. Możesz także utworzyć zadanie tworzenia kopii zapasowej.

   Zaleca się wyeksportowanie listy zainstalowanych wtyczek.

5. **Uruchamianie instalatora**

   Uruchom plik wykonywalny dla najnowszej wersji Kaspersky Security Center. Podczas uruchamiania pliku określ, czy masz kopię zapasową i określ jej lokalizację. Twoje dane zostaną przywrócone z kopii zapasowej.

6. **Aktualizowanie zarządzanych aplikacji**

   Możesz zaktualizować aplikację, jeśli jest dostępna nowsza wersja. Zapoznaj się z listą obsługiwanych aplikacji Kaspersky i upewnij się, że Twoja wersja Kaspersky Security Center jest kompatybilna z tą aplikacją. Następnie przeprowadź aktualizację aplikacji w sposób opisany w jej Informacjach o kompilacji.

Wyniki

Po zakończeniu scenariusza aktualizacji, upewnij się, że nowa wersja Serwera administracyjnego została pomyślnie zainstalowana w konsoli Microsoft Management Console. Kliknij **Pomoc** → **Informacje o Kaspersky Security Center**. Zostanie wyświetlona wersja.

Aby upewnić się, że korzystasz z nowszej wersji Serwera administracyjnego w Kaspersky Security Center Web Console, w górnej części ekranu kliknij ikonę ustawień ( ) obok nazwy Serwera administracyjnego. W otwartym oknie właściwości Serwera administracyjnego, na zakładce **Ogólne** wybierz sekcję **Ogólne**. Zostanie wyświetlona wersja.

Jeśli chcesz odzyskać dane Serwera administracyjnego, wykonaj czynności opisane w następującym temacie: Tworzenie kopii zapasowej i przywracanie danych w trybie interaktywnym.

Jeśli zaktualizowałeś zarządzaną aplikację zabezpieczającą, upewnij się, że jest ona poprawnie zainstalowana na zarządzanym urządzeniu (zarządzanych urządzeniach). Więcej informacji znajdziesz w dokumentacji dla tej aplikacji.

Aktualizowanie baz danych i aplikacji Kaspersky

Ta sekcja opisuje kroki, które musisz podjąć, aby regularnie aktualizować następujące elementy:

- Baz danych i modułów oprogramowania firmy Kaspersky
- Zainstalowane aplikacje firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), przy czym funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Scenariusz: Regularne aktualizowanie baz danych i aplikacji Kaspersky

Ta sekcja oferuje scenariusz regularnego aktualizowania baz danych, modułów i aplikacji firmy Kaspersky. Po zakończeniu Konfigurowania scenariusza ochrony sieci, musisz zachować niezawodność systemu ochrony, aby upewnić się, że Serwery administracyjne i zarządzane urządzenia są chronione przed różnymi zagrożeniami, w tym wirusami, atakami sieciowymi i atakami phishingowymi.

Aktualność ochrony sieci jest zapewniana przez regularne aktualizacje:

- Baz danych i modułów oprogramowania firmy Kaspersky
- Zainstalowane aplikacje firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające

Po zakończeniu tego scenariusza, możesz być pewny, że:

- Twoja sieć jest chroniona przez najaktualniejsze oprogramowanie firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające.
- Antywirusowe bazy danych i inne bazy danych Kaspersky krytyczne dla bezpieczeństwa sieci są zawsze aktualne.

Wymagania wstępne

Zarządzane urządzenia muszą mieć połączenie z Serwerem administracyjnym. Jeśli nie mają połączenia, rozważ ręczne zaktualizowanie baz danych, modułów i aplikacji Kaspersky lub bezpośrednio z serwerów aktualizacji Kaspersky.

Serwer administracyjny musi mieć połączenie z Internetem.

Przed rozpoczęciem upewnij się, że:

1. Wdrożono aplikacje zabezpieczające Kaspersky na zarządzanych urządzeniach zgodnie ze scenariuszem wdrażania aplikacji Kaspersky poprzez Kaspersky Security Center Web Console.
2. Utworzyłeś i skonfigurowałeś wszystkie wymagane zasady, profile zasad i zadania zgodnie ze scenariuszem konfigurowania ochrony sieci.
3. Przydzieliłeś odpowiednią liczbę punktów dystrybucji zgodnie z liczbą zarządzanych urządzeń i topologią sieci.

Aktualizowanie baz danych i aplikacji Kaspersky odbywa się w etapach:

1. **Wybranie schematu aktualizacji**

   Istnieje kilka schematów, których możesz użyć do zainstalowania aktualizacji dla komponentów Kaspersky Security Center i aplikacji zabezpieczających. Wybierz schemat lub kilka schematów, które najlepiej spełniają wymagania Twojej sieci.

2. **Tworzenie zadania pobierania aktualizacji do repozytorium Serwera administracyjnego**

To zadanie jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Jeśli nie uruchamiałeś kreatora, utwórz zadanie teraz.

To zadanie jest wymagane do pobrania uaktualnień z serwerów aktualizacji Kaspersky do repozytorium Serwera administracyjnego, a także do zaktualizowania baz danych i modułów Kaspersky dla aplikacji Kaspersky Security Center. Po pobraniu uaktualnień, mogą one zostać przesłane na zarządzane urządzenia.

Jeśli w Twojej sieci są przypisane punkty dystrybucji, uaktualnienia są automatycznie pobierane z repozytorium Serwera administracyjnego do repozytoriów punktów dystrybucji. W tym przypadku zarządzane urządzenia, znajdujące się w obszarze punktu dystrybucji, pobierają uaktualnienia z repozytorium punktu dystrybucji zamiast repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna: Tworzenie zadania pobierania uaktualnień do repozytorium Serwera administracyjnego
- Kaspersky Security Center Web Console: Tworzenie zadania pobierania uaktualnień do repozytorium Serwera administracyjnego

3. **Tworzenie zadania pobierania aktualizacji do repozytoriów punktów dystrybucji (opcjonalne)**

   Domyślnie, uaktualnienia są pobierane do punktów dystrybucji z Serwera administracyjnego. Możesz skonfigurować Kaspersky Security Center do pobierania uaktualnień do punktów dystrybucji bezpośrednio z serwerów aktualizacji Kaspersky. Pobranie do repozytoriów punktów dystrybucji jest preferowane, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktami dystrybucji jest droższy niż ruch sieciowy pomiędzy punktami dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu.

   Jeśli do Twojej sieci są przypisane punkty dystrybucji i utworzone jest zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, punkty dystrybucji pobiorą uaktualnienia z serwerów aktualizacji Kaspersky, a nie z repozytorium Serwera administracyjnego.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie zadania pobierania uaktualnień do repozytoriów punktów dystrybucji
   - Kaspersky Security Center Web Console: Tworzenie zadania pobierania uaktualnień do repozytoriów punktów dystrybucji

4. **Konfigurowanie punktów dystrybucji**

   Jeśli w Twojej sieci są przypisane punkty dystrybucji, upewnij się, że opcja **Roześlij aktualizacje** jest włączona we właściwościach wszystkich wymaganych punktów dystrybucji. Jeśli ta opcja jest włączona dla punktu dystrybucji, urządzenia znajdujące się w obszarze punktu dystrybucji pobierają uaktualnienia z repozytorium Serwera administracyjnego.

   Jeśli chcesz, żeby zarządzane urządzenia pobierały uaktualnienia tylko z punktów dystrybucji, włącz opcję **Rozsyłaj pliki tylko poprzez punkty dystrybucji** w zasadzie Agenta sieciowego.

5. **Optymalizowanie procesu aktualizacji przy użyciu trybu offline pobierania uaktualnień lub plików diff (opcjonalne)**

   Możesz zoptymalizować proces aktualizacji przy użyciu trybu offline pobierania uaktualnień (włączone domyślnie) lub przy użyciu plików diff. Dla każdego segmentu sieci musisz wybrać, którą z tych dwóch funkcji włączyć, ponieważ nie mogą działać jednocześnie.

   Jeśli tryb offline pobierania uaktualnień jest włączony, Agent sieciowy pobierze wymagane uaktualnienia na zarządzane urządzenie po pobraniu uaktualnień do repozytorium Serwera administracyjnego, zanim aplikacja zabezpieczająca zażąda uaktualnień. Zwiększy to niezawodność procesu aktualizacji. Aby korzystać z tej funkcji, włącz opcję **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)** w zasadzie Agenta sieciowego.

Jeśli nie używasz trybu offline pobierania uaktualnień, możesz zoptymalizować ruch sieciowy między Serwerem administracyjnym a zarządzanymi urządzeniami przy użyciu plików diff. Jeśli ta funkcja jest włączona, Serwer administracyjny lub punkt dystrybucji pobierze pliki diff zamiast całych plików baz danych lub modułów Kaspersky. Plik diff opisuje różnice między dwoma wersjami pliku bazy danych lub modułu programu. Dlatego też plik diff zajmuje mniej miejsca niż cały plik. Spowoduje to zmniejszenie ruchu sieciowego między Serwerem administracyjnym lub punktami dystrybucji a zarządzanymi urządzeniami. Aby użyć tej funkcji, włącz opcję **Pobierz pliki diff** we właściwościach zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* i/lub zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

Dostępne instrukcje:

- Używanie plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky
- Konsola administracyjna: Włączanie i wyłączanie trybu offline pobierania uaktualnień
- Kaspersky Security Center Web Console: Włączanie i wyłączanie trybu offline pobierania uaktualnień

6. **Sprawdzanie pobranych uaktualnień (opcjonalne)**

Przed zainstalowaniem pobranych uaktualnień możesz zweryfikować uaktualnienia poprzez zadanie *Weryfikacja uaktualnień*. To zadanie kolejno uruchamia zadania aktualizacji i zadania skanowania w poszukiwaniu złośliwego oprogramowania urządzeń, skonfigurowane poprzez ustawienia dla określonego zbioru urządzeń testowych. Po uzyskaniu wyników zadania, Serwer administracyjny uruchamia lub blokuje propagację aktualizacji na pozostałe urządzenia.

Zadanie *Weryfikacja uaktualnień* jest wykonywane jako część zadania *Pobierz uaktualnienia do repozytorium serwera administracyjnego*. We właściwościach zadania *Pobierz uaktualnienia do repozytorium serwera administracyjnego* włącz opcję **Zweryfikuj uaktualnienia przed rozesłaniem** przed dystrybucją w konsoli administracyjnej lub opcję **Uruchom weryfikację aktualizacji** w Kaspersky Security Center Web Console.

Dostępne instrukcje:

- Konsola administracyjna: Weryfikowanie pobranych uaktualnień
- Kaspersky Security Center Web Console: Weryfikowanie pobranych uaktualnień

7. **Zatwierdzanie i odrzucanie aktualizacji oprogramowania**

Domyślnie pobrane aktualizacje oprogramowania posiadają stan *Niezdefiniowane*. Możesz zmienić stan na *Zatwierdzone* lub *Odrzucone*. Zatwierdzone aktualizacje są zawsze instalowane. Jeśli aktualizacja wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej użytkownika końcowego, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia. Niezdefiniowane aktualizacje mogą zostać zainstalowane tylko na Agencie sieciowym, a inne komponenty Kaspersky Security Center zgodnie z ustawieniami zasady Agenta sieciowego. Aktualizacje, dla których ustawiłeś stan *Odrzucone*, nie zostaną zainstalowane na urządzeniach. Jeśli odrzucona aktualizacja dla aplikacji zabezpieczającej została wcześniej zainstalowana, Kaspersky Security Center spróbuje odinstalować aktualizację ze wszystkich urządzeń.

Zatwierdzanie i odrzucanie aktualizacji jest dostępne tylko w przypadku Agenta sieciowego i aplikacji zarządzanych Kaspersky zainstalowanych na urządzeniach klienckich z systemem Windows i Linux. Bezproblemowa aktualizacja Serwera administracyjnego, Kaspersky Security Center Web Console i webowych wtyczek administracyjnych nie jest obsługiwana.

Dostępne instrukcje:

- Konsola administracyjna: Zatwierdzanie i odrzucanie aktualizacji oprogramowania
- Kaspersky Security Center Web Console: Zatwierdzanie i odrzucanie aktualizacji oprogramowania

8. **Konfigurowanie automatycznej instalacji uaktualnień i poprawek dla komponentów Kaspersky Security Center**

Pobrane aktualizacje i poprawki dla Agenta sieciowego i innych komponentów Kaspersky Security Center są instalowane automatycznie. Jeśli pozostawiłeś opcję **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany** włączoną we właściwościach Agenta sieciowego, wówczas wszystkie uaktualnienia zostaną zainstalowane automatycznie po ich pobraniu do repozytorium (lub kilku repozytoriów). Jeśli ta opcja jest wyłączona, poprawki Kaspersky, które zostały pobrane i oznaczone jako *Niezdefiniowane*, zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzone*.

Dostępne instrukcje:

- Konsola administracyjna: Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center
- Kaspersky Security Center Web Console: Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center

9. **Instalacja uaktualnień dla Serwera administracyjnego**

   Aktualizacje oprogramowania dla Serwera administracyjnego nie zależą od stanów aktualizacji. Nie są instalowane automatycznie i muszą być wcześniej zatwierdzone przez administratora na zakładce **Monitorowanie** w Konsoli administracyjnej (**Serwer administracyjny** <nazwa serwera> → **Monitorowanie**) lub w sekcji **Powiadomienia** w Kaspersky Security Center Web Console (**Monitorowanie i raportowanie** → **Powiadomienia**). Następnie administrator musi wyraźnie uruchomić instalację uaktualnień.

10. **Konfigurowanie automatycznej instalacji uaktualnień dla aplikacji zabezpieczających**

    Utwórz zadania *Aktualizacji* dla zarządzanych aplikacji, aby zapewnić najnowsze aktualizacje aplikacji, modułów oprogramowania i baz danych Kaspersky, w tym antywirusowych baz danych. Aby zapewnić terminowe aktualizacje, zalecamy wybranie opcji **Po pobraniu nowych aktualizacji do repozytorium** podczas konfigurowania terminarza zadań.

    Jeśli Twoja sieć zawiera urządzenia obsługujące tylko protokół IPv6 i chcesz regularnie aktualizować aplikacje zabezpieczające zainstalowane na tych urządzeniach, upewnij się, że na zarządzanych urządzeniach zainstalowany jest Serwer administracyjny (w wersji nie wcześniejszej niż 13.2) oraz Agent sieciowy (w wersji nie wcześniejszej niż 13.2).

    Domyślnie, uaktualnienia dla Kaspersky Endpoint Security for Windows i Kaspersky Endpoint Security for Linux są instalowane dopiero po zmianie stanu aktualizacji na *Zatwierdzone*. Ustawienia aktualizacji można zmienić w zadaniu *Aktualizacja*.

    Jeśli aktualizacja wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej użytkownika końcowego, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia.

    Dostępne instrukcje:

    - Konsola administracyjna: Automatyczna instalacja uaktualnień dla Kaspersky Endpoint Security na urządzeniach
    - Kaspersky Security Center Web Console: Automatyczna instalacja uaktualnień dla Kaspersky Endpoint Security na urządzeniach

Wyniki

Po zakończeniu scenariusza, Kaspersky Security Center jest konfigurowany do aktualizowania baz danych Kaspersky i zainstalowanych aplikacji Kaspersky po pobraniu uaktualnień do repozytorium Serwera administracyjnego lub do repozytoriów punktów dystrybucji. Możesz przejść do monitorowania stanu sieci.

Informacje o aktualizowaniu baz danych, modułów i aplikacji Kaspersky

W celu upewnienia się, że ochrona Serwerów administracyjnych i zarządzanych urządzeń jest aktualna, w odpowiednim czasie należy dostarczać aktualizacje:

- Baz danych i modułów oprogramowania firmy Kaspersky

  Przed pobraniem baz danych i modułów oprogramowania Kaspersky oprogramowanie Kaspersky Security Center sprawdza, czy serwery Kaspersky są dostępne. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Jest to konieczne, aby zapewnić aktualizację antywirusowych baz danych oraz zachować poziom bezpieczeństwa zarządzanych urządzeń.

- Zainstalowane aplikacje firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające

  Kaspersky Security Center umożliwia automatyczną aktualizację Agenta sieciowego i aplikacji Kaspersky zainstalowanych na urządzeniach klienckich z systemem Windows i Linux. Bezproblemowa aktualizacja Serwera administracyjnego, Kaspersky Security Center Web Console i webowych wtyczek administracyjnych nie jest obsługiwana. Aby zaktualizować aplikacje, pobierz najnowsze wersje aplikacji z witryny internetowej Kaspersky, a następnie zainstaluj je ręcznie.

W zależności od konfiguracji sieci, możesz użyć następujących schematów pobierania i rozsyłania żądanych aktualizacji na zarządzane urządzenia:

- Za pomocą jednego zadania: *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
- Używanie dwóch zadań:
  - Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
  - Zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*
- Ręcznie poprzez folder lokalny, folder współdzielony lub serwer FTP
- Bezpośrednio z serwerów aktualizacji Kaspersky do Kaspersky Endpoint Security na zarządzanych urządzeniach
- Poprzez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

Używanie zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego

W tym schemacie Kaspersky Security Center pobiera aktualizacje za pośrednictwem zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. W małych sieciach, które zawierają mniej niż 300 zarządzanych urządzeń w jednym segmencie sieci lub mniej niż 10 zarządzanych urządzeń w każdym segmencie sieci, aktualizacje są rozsyłane na zarządzane urządzenia bezpośrednio z repozytorium Serwera administracyjnego (patrz rysunek poniżej).

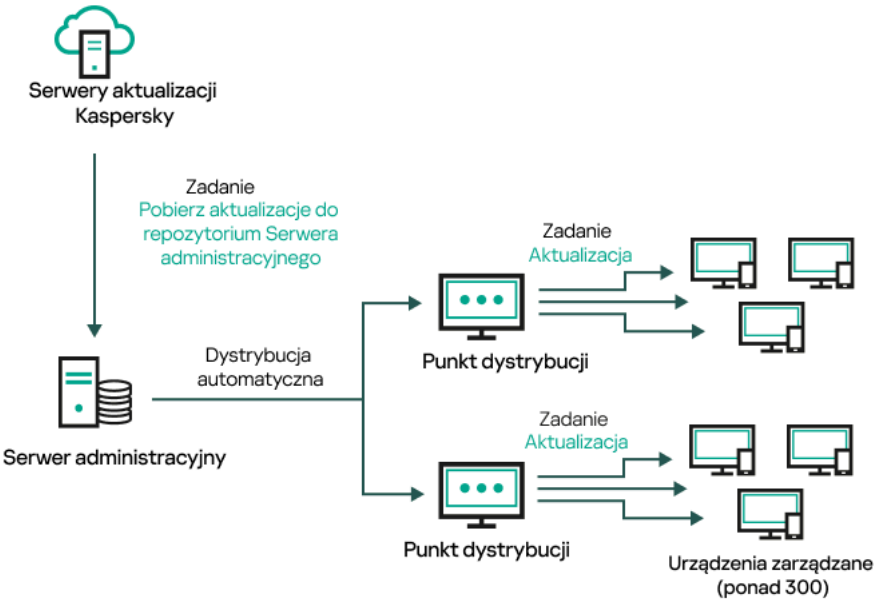


Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego bez punktów dystrybucji

Domyślnie, Serwer administracyjny komunikuje się z serwerami aktualizacji Kaspersky i pobiera uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny, aby używał protokołu HTTP zamiast HTTPS.

Jeśli sieć zawiera ponad 300 zarządzanych urządzeń w jednym segmencie sieci lub jeśli sieć zawiera kilka segmentów sieci z ponad 9 zarządzanymi urządzeniami w każdym segmencie sieci, zalecane jest użycie punktów dystrybucji do przesyłania aktualizacji na zarządzane urządzenia (patrz rysunek poniżej). Punkty dystrybucji zmniejszają obciążenie na Serwerze administracyjnym i optymalizują ruch sieciowy między Serwerem administracyjnym i zarządzanymi urządzeniami. Możesz obliczyć liczbę i konfigurację punktów dystrybucji wymaganych dla Twojej sieci.

W tym schemacie, uaktualnienia są automatycznie pobierane z repozytorium Serwera administracyjnego do repozytoriów punktów dystrybucji. Zarządzane urządzenia, znajdujące się w obszarze punktu dystrybucji, pobierają uaktualnienia z repozytorium punktu dystrybucji zamiast repozytorium Serwera administracyjnego.



Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego z punktami dystrybucji

Jeśli zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* zostało zakończone, z repozytorium Serwera administracyjnego zostają pobrane następujące aktualizacje:

- Bazy danych i moduły Kaspersky dla Kaspersky Security Center

  Te aktualizacje są instalowane automatycznie.

- Bazy danych i moduły Kaspersky dla aplikacji zabezpieczających na zarządzanych urządzeniach

  Te aktualizacje są instalowane poprzez zadanie Aktualizacja dla Kaspersky Endpoint Security for Windows.

- Aktualizacje dla Serwera administracyjnego

  Te aktualizacje nie są instalowane automatycznie. Administrator musi wyraźnie zatwierdzić i uruchomić instalację aktualizacji.

  > Uprawnienia lokalnego administratora są wymagane do zainstalowania łat na Serwerze administracyjnym.

- Aktualizacje dla komponentów Kaspersky Security Center

  Domyślnie, te aktualizacje są instalowane automatycznie. Możesz zmienić ustawienia w zasadzie Agenta sieciowego.

- Aktualizacje dla aplikacji zabezpieczających

  Domyślnie Kaspersky Endpoint Security for Windows zainstaluje tylko te aktualizacje, które zatwierdzisz. (Aktualizacje możesz zatwierdzić za pośrednictwem Konsoli administracyjnej lub za pośrednictwem konsoli Kaspersky Security Center Web Console). Aktualizacje są instalowane poprzez zadanie *Aktualizacja* i mogą zostać skonfigurowane we właściwościach tego zadania.

> Zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego* nie jest dostępne na wirtualnych Serwerach administracyjnych. Repozytorium wirtualnego Serwera administracyjnego wyświetla uaktualnienia pobrane na główny Serwer administracyjny.

Możesz skonfigurować sprawdzanie aktualizacji pod kątem łatwości obsługi i błędów na zestawie urządzeń testowych. Jeśli weryfikacja zostanie zakończona pomyślnie, aktualizacje będą rozsyłane na inne zarządzane urządzenia.

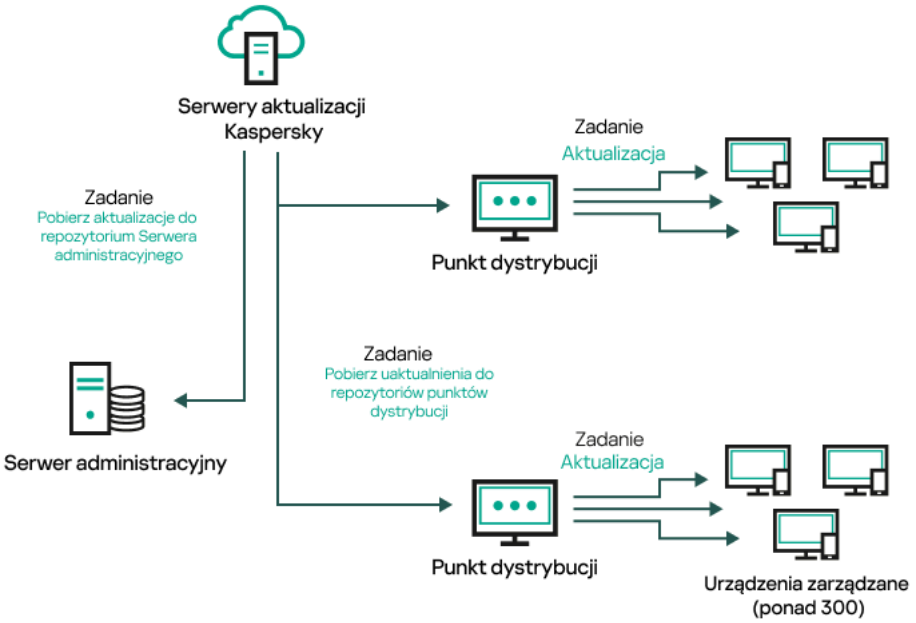
Każda aplikacja Kaspersky żąda wymaganych aktualizacji z Serwera administracyjnego. Serwer administracyjny gromadzi te żądania i pobiera tylko te uaktualnienia, które zostały zażądane przez aplikację. Dzięki temu te same uaktualnienia nie są pobierane kilka razy, a niepotrzebne uaktualnienia nie są pobierane wcale. Podczas wykonywania zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, Serwer administracyjny automatycznie wysyła następujące informacje do serwerów aktualizacji Kaspersky w celu zapewnienia pobrania najnowszych wersji baz danych i modułów aplikacji Kaspersky:

- Identyfikator i wersja aplikacji
- Identyfikator instalacji aplikacji
- Identyfikator aktywnego klucza
- ID uruchamiania zadania *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*

Żadna z przesyłanych informacji nie zawiera danych osobowych ani innych poufnych danych. Firma AO Kaspersky Lab chroni informacje zgodnie z wymogami wynikającymi z przepisów prawa.

Używanie dwóch zadań: zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego oraz zadanie Pobierz aktualizacje do repozytoriów punktów dystrybucji

Możesz pobrać aktualizacje do repozytoriów punktów dystrybucji bezpośrednio z serwerów aktualizacji Kaspersky zamiast repozytorium Serwera administracyjnego, a następnie rozesłać aktualizacje na zarządzane urządzenia (patrz rysunek poniżej). Pobranie do repozytoriów punktów dystrybucji jest preferowane, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktami dystrybucji jest droższy niż ruch sieciowy pomiędzy punktami dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu.



Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego oraz zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji

Domyślnie, Serwer administracyjny i punkty dystrybucji komunikują się z serwerami aktualizacji Kaspersky i pobierają uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny i/lub punkty dystrybucji do używania protokołu HTTP zamiast HTTPS.

Aby zaimplementować ten schemat, utwórz zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji* jako dodatek do zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Po pobraniu przez punkty dystrybucji aktualizacji z serwerów aktualizacji Kaspersky, a nie z repozytorium Serwera administracyjnego.

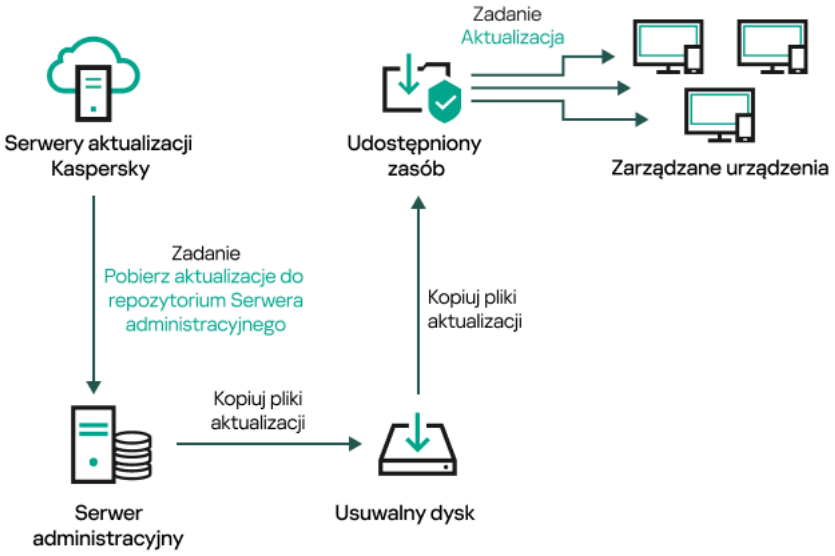
Urządzenia punktów dystrybucji działające pod kontrolą systemu operacyjnego macOS nie mogą pobierać uaktualnień z serwerów aktualizacji Kaspersky.

W przypadku, gdy jedno lub więcej urządzeń działających pod kontrolą systemu operacyjnego macOS znajduje się w obszarze zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, zadanie zostaje zakończone ze stanem *Niepowodzenie* nawet wtedy, gdy zadanie zostaje zakończone pomyślnie na wszystkich urządzeniach z systemem Windows.

Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* jest także wymagane dla tego schematu, ponieważ to zadanie jest używane do pobrania baz danych i modułów Kaspersky dla Kaspersky Security Center.

Ręcznie poprzez folder lokalny, folder współdzielony lub serwer FTP

Jeśli urządzenia klienckie nie mają połączenia z Serwerem administracyjnym, możesz użyć folderu lokalnego lub zasobu współdzielonego jako źródła dla aktualizacji baz danych, modułów i aplikacji Kaspersky. W tym schemacie możesz skopiować wymagane aktualizacje z repozytorium Serwera administracyjnego na dysk wymienny, a następnie skopiować aktualizacje do folderu lokalnego lub zasobu współdzielonego, określonego jako źródło uaktualnień w ustawieniach Kaspersky Endpoint Security (patrz rysunek poniżej).



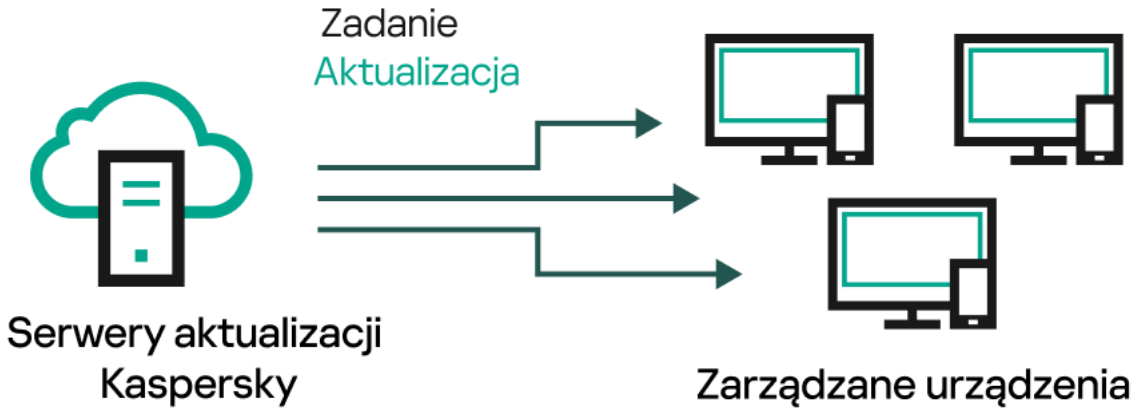
Aktualizowanie poprzez folder lokalny, folder współdzielony lub serwer FTP

Aby uzyskać więcej informacji na temat źródeł aktualizacji w Kaspersky Endpoint Security, zobacz następujące Pomoce:

- Pomoc Kaspersky Endpoint Security for Windows
- Pomoc Kaspersky Endpoint Security for Linux

Bezpośrednio z serwerów aktualizacji Kaspersky do Kaspersky Endpoint Security na zarządzanych urządzeniach

Na zarządzanych urządzeniach możesz skonfigurować Kaspersky Endpoint Security w celu pobierania aktualizacji bezpośrednio z serwerów aktualizacji Kaspersky (patrz rysunek poniżej).



Aktualizowanie aplikacji zabezpieczających bezpośrednio z serwerów aktualizacji Kaspersky

W tym schemacie aplikacja zabezpieczająca nie używa repozytoriów dostarczonych przez Kaspersky Security Center. Aby pobierać uaktualnienia bezpośrednio z serwerów aktualizacji Kaspersky, określ serwery aktualizacji Kaspersky jako źródło uaktualnień w interfejsie aplikacji zabezpieczającej. Aby uzyskać więcej informacji na temat tych ustawień, zobacz następujące Pomoce:

- Pomoc Kaspersky Endpoint Security for Windows
- Pomoc Kaspersky Endpoint Security for Linux

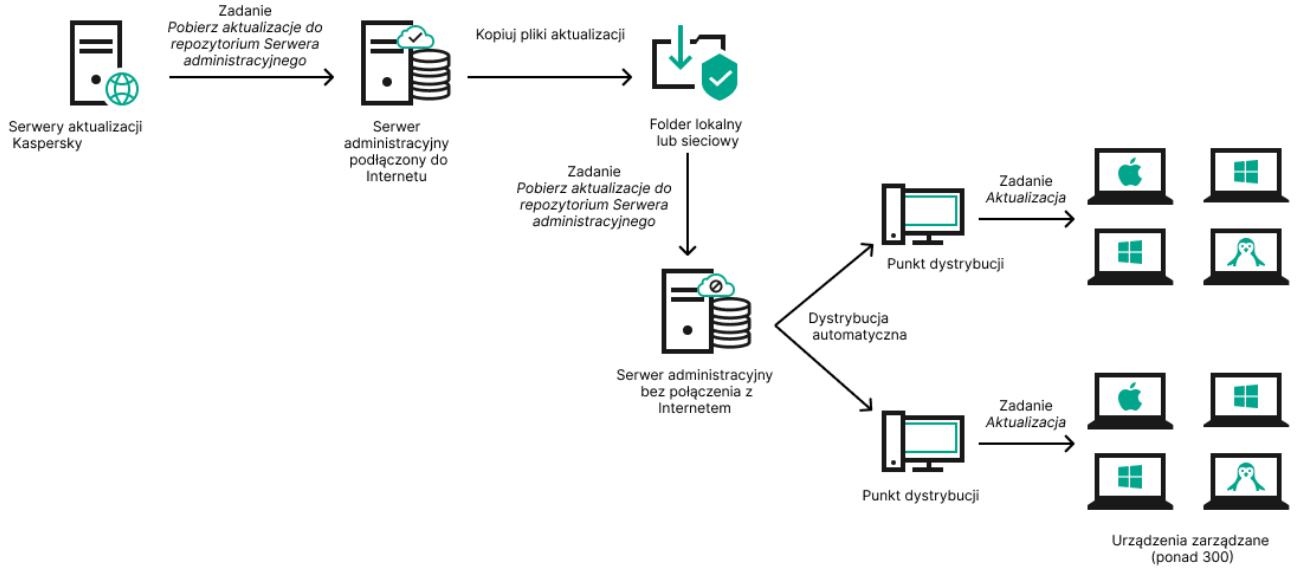
Poprzez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

Jeżeli Serwer administracyjny nie ma połączenia z Internetem, możesz skonfigurować zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, aby pobierać uaktualnienia z folderu lokalnego lub sieciowego. W takim przypadku należy od czasu do czasu kopiować wymagane pliki aktualizacji do określonego folderu. Na przykład możesz skopiować wymagane pliki aktualizacji z jednego z następujących źródeł:

- Serwer administracyjny z połączeniem internetowym (patrz rysunek poniżej)

  Ponieważ serwer administracyjny pobiera tylko aktualizacje wymagane przez aplikacje zabezpieczające, zestawy aplikacji zabezpieczających zarządzanych przez serwery administracyjne — ten, który ma połączenie z Internetem i ten, który go nie ma — muszą być zgodne.

  Jeżeli Serwer administracyjny, którego używasz do pobierania uaktualnień, ma wersję 13.2 lub wcześniejszą, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję **Pobierz aktualizacje za pomocą starego schematu**.



Aktualizacja przez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

- Kaspersky Update Utility

  Ponieważ narzędzie to wykorzystuje stary schemat do pobierania uaktualnień, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję **Pobierz aktualizacje za pomocą starego schematu**.

Tworzenie zadania Pobierz aktualizacje do repozytorium serwera administracyjnego

Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* Serwera administracyjnego jest automatycznie tworzone podczas działania Kreatora wstępnej konfiguracji Kaspersky Security Center. Możesz utworzyć tylko jedno zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Dlatego też zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* możesz utworzyć tylko wtedy, gdy takie zadanie zostało usunięte z listy zadań Serwera administracyjnego.

To zadanie jest wymagane do pobrania uaktualnień z serwera aktualizacji Kaspersky do repozytorium Serwera administracyjnego. Lista aktualizacji obejmuje:

- Aktualizacje baz danych i modułów dla Serwera administracyjnego
- Aktualizacje baz danych i modułów dla aplikacji zabezpieczających Kaspersky
- Aktualizacje komponentów Kaspersky Security Center
- Aktualizacje aplikacji zabezpieczających Kaspersky

Po pobraniu uaktualnień, mogą one zostać przesłane na zarządzane urządzenia.

Przed dystrybucją aktualizacji do urządzeń zarządzanych możesz uruchomić zadanie *Weryfikacja uaktualnień*. Pozwala to upewnić się, że serwer administracyjny prawidłowo zainstaluje pobrane aktualizacje, a poziom bezpieczeństwa nie zmniejszy się z powodu aktualizacji. Aby zweryfikować je przed dystrybucją, skonfiguruj opcję **Uruchom weryfikację aktualizacji** w ustawieniach zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

*W celu utworzenia zadania **Pobierz aktualizacje do repozytorium Serwera administracyjnego**:*

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
6. Kliknij przycisk **Utwórz**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.
7. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

8. W oknie właściwości zadania, na zakładce **Ustawienia aplikacji** określ następujące ustawienia:

- **Źródła aktualizacji**

  Jako źródła uaktualnień dla Serwera administracyjnego można użyć następujących zasobów:

  - Serwery aktualizacji Kaspersky

    Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji. Domyślnie, Serwer administracyjny komunikuje się z serwerami aktualizacji Kaspersky i pobiera uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny, aby używał protokołu HTTP zamiast HTTPS.

    Ta opcja jest wybrana domyślnie.

  - Główny Serwer administracyjny

    Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.

  - Folder lokalny lub sieciowy

    Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

    > Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

  Jeśli folder współdzielony zawierający aktualizacje jest chroniony hasłem, włącz opcję **Określ konto, które posiada dostęp do udostępnionego folderu źródła aktualizacji (jeśli takie jest)** i wprowadź dane konta wymagane do uzyskania dostępu.

- **Folder do przechowywania aktualizacji**

  Ścieżka do określonego folderu na potrzeby przechowywania zapisanych aktualizacji. Możesz skopiować ścieżkę do określonego folderu do schowka. Nie możesz zmienić ścieżki do określonego folderu w przypadku zadania grupowego.

- Inne ustawienia:

  - **Wymuś aktualizację podrzędnych Serwerów administracyjnych**

    Jeżeli ta opcja jest włączona, Serwer administracyjny uruchomi zadania aktualizacji na podrzędnych Serwerach administracyjnych zaraz po pobraniu nowych aktualizacji. Zadania aktualizacji są uruchamiane przy użyciu źródła aktualizacji skonfigurowanego we właściwościach zadania na podrzędnych Serwerach administracyjnych.

    Jeśli ta opcja jest wyłączona, zadania aktualizacji na podrzędnych Serwerach administracyjnych będą uruchamiane zgodnie ze swoimi terminarzami.

    Domyślnie opcja ta jest wyłączona.

  - **Kopiuj pobrane aktualizacje do dodatkowych folderów**

    Po otrzymaniu przez Serwer administracyjny uaktualnień skopiuje on je do określonych folderów. Użyj tej opcji, jeśli chcesz ręcznie zarządzać dystrybucją uaktualnień w sieci.

Na przykład, chcesz użyć tej opcji w następującej sytuacji: sieć Twojej organizacji zawiera kilka niezależnych podsieci, a urządzenia z każdej podsieci nie mają dostępu do innych podsieci. Jednakże urządzenia we wszystkich podsieciach mają dostęp do wspólnego udziału sieciowego. W tym przypadku skonfiguruj Serwer administracyjny w jednej z podsieci tak, aby pobierał uaktualnienia z serwerów aktualizacji Kaspersky, włącz tę opcję, a następnie określ ten udział sieciowy. W zadaniach pobierania uaktualnień do repozytorium dla innych Serwerów administracyjnych określ ten sam udział sieciowy jako źródło uaktualnień.

Jeżeli zdecydujesz się na skopiowanie pobranych aktualizacji do folderu lokalnego, musisz wskazać folder na urządzeniu, na którym jest zainstalowany Serwer administracyjny. Ścieżka do folderu zależy od systemu operacyjnego urządzenia. Ponieważ folder lokalny znajduje się na Serwerze administracyjnym opartym na systemie Linux, należy określić ścieżkę POSIX, na przykład: /path/to/dir.

Wybierając folder sieciowy znajdujący się na Serwerze administracyjnym opartym na systemie Linux, należy wcześniej zapewnić dostęp do folderu sieciowego z urządzenia z zainstalowanym Serwerem administracyjnym, montując folder. Dostęp do folderu odbywa się za pomocą protokołu SMB.

Domyślnie opcja ta jest wyłączona.

- **Nie wymuszaj aktualizacji urządzeń i podrzędnych Serwerów administracyjnych przed zakończeniem kopiowania**

  Zadania pobierania aktualizacji na urządzenia klienckie i podrzędne Serwery administracyjne zostaną uruchomione dopiero po skopiowaniu aktualizacji z głównego folderu aktualizacji do dodatkowych folderów aktualizacji.

  Ta opcja musi być włączona, jeśli urządzenia klienckie i podrzędne Serwery administracyjne pobierają aktualizacje z dodatkowych folderów sieciowych.

  Domyślnie opcja ta jest wyłączona.

- **Zawartość aktualizacji**:

  - **Pobierz pliki diff**

    Ta opcja włącza funkcję pobierania plików diff.

    Domyślnie opcja ta jest wyłączona.

- **Pobierz aktualizacje za pomocą starego schematu**

  Począwszy od wersji 14, Kaspersky Security Center pobiera aktualizacje baz danych i modułów oprogramowania przy użyciu nowego schematu. Aby aplikacja pobierała aktualizacje przy użyciu nowego schematu, źródło aktualizacji musi zawierać pliki aktualizacji z metadanymi zgodnymi z nowym schematem. Jeśli źródło aktualizacji zawiera pliki aktualizacji z metadanymi zgodnymi tylko ze starym schematem, włącz opcję **Pobierz aktualizacje za pomocą starego schematu**. W przeciwnym razie zadanie pobierania aktualizacji zakończy się niepowodzeniem.

  Na przykład musisz włączyć tę opcję, gdy folder lokalny lub sieciowy jest określony jako źródło aktualizacji, a pliki aktualizacji w tym folderze zostały pobrane przez jedną z następujących aplikacji:

  - Kaspersky Update Utility

    To narzędzie pobiera aktualizacje przy użyciu starego schematu.

  - Kaspersky Security Center 13.2 lub wcześniejsza wersja

    Na przykład Twój serwer administracyjny 1 nie ma połączenia z Internetem. W takim przypadku możesz pobrać aktualizacje za pomocą serwera administracyjnego 2, który ma połączenie z Internetem, a następnie umieścić je w folderze lokalnym lub sieciowym, aby użyć go jako źródła uaktualnień dla serwera administracyjnego 1. Jeżeli serwer administracyjny 2 ma wersję 13.2 lub wcześniejszą, włącz opcję **Pobierz aktualizacje za pomocą starego schematu** w zadaniu dla serwera administracyjnego 1.

Domyślnie opcja ta jest wyłączona.

- **Uruchom weryfikację aktualizacji**

  Serwer administracyjny pobiera uaktualnienia ze źródła, zapisuje je w tymczasowym repozytorium i uruchamia zadanie określone w polu **Zadanie weryfikacji uaktualnień**. Jeśli zadanie zakończy się pomyślnie, uaktualnienia są kopiowane z tymczasowego repozytorium do folderu współdzielonego na Serwerze administracyjnym, a następnie są rozsyłane do wszystkich urządzeń, dla których Serwer administracyjny pełni rolę źródła uaktualnień (zadania są uruchamiane zgodnie z opcją terminarza - **Po pobraniu nowych uaktualnień do repozytorium**). Zadanie pobierania uaktualnień do repozytorium zostaje zakończone dopiero po zakończeniu zadania *weryfikacji uaktualnień*.

  Domyślnie opcja ta jest wyłączona.

9. W oknie właściwości zadania, na zakładce **Terminarz** utwórz terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

   - **Uruchom zadanie:**

     Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

     - **Ręcznie**

       Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

       Domyślnie opcja ta jest zaznaczona.

     - **Co N minut**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

       Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

     - **Co N godzin**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

       Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

     - **Co N dni**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

       Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

     - **Według dni tygodnia**

       Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

       Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

     - **Co miesiąc**

       Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

       W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po ataku wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj automatycznego losowego opóźnienia dla zadań uruchamianych w przedziale**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

- **Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż**

  Po minięciu określonego czasu, zadanie jest zatrzymywane automatycznie, niezależnie od tego, czy zostało zakończone.

  Włącz tę opcję, jeśli chcesz przerwać (lub zatrzymać) zadania, których wykonanie zajmuje zbyt dużo czasu.

  Domyślnie opcja ta jest wyłączona. Domyślny czas wykonania zadania to 120 minut.

10. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

Podczas wykonywania zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* uaktualnienia baz danych i modułów programu są pobierane ze źródła uaktualnień i przechowywane w folderze współdzielonym Serwera administracyjnego. Jeśli tworzysz to zadanie dla grupy administracyjnej, zostanie ono zastosowane tylko do Agentów sieciowych umieszczonych w określonej grupie administracyjnej.

Uaktualnienia są rozsyłane do urządzeń klienckich i podrzędnych Serwerów administracyjnych z folderu współdzielonego Serwera administracyjnego.

Sprawdzanie pobranych uaktualnień

Przed zainstalowaniem aktualizacji na zarządzanych urządzeniach, w pierwszej kolejności możesz sprawdzić aktualizacje pod kątem łatwości obsługi i błędów poprzez zadanie *Weryfikacja aktualizacji*. Zadanie *Weryfikacja aktualizacji* jest wykonywane automatycznie jako część zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Serwer administracyjny pobierze uaktualnienia ze źródła, zapisze je w repozytorium tymczasowym i uruchomi zadanie *weryfikacji uaktualnień*. Jeżeli zadanie zakończy się powodzeniem, uaktualnienia zostaną skopiowane z repozytorium tymczasowego do folderu współdzielonego na serwerze administracyjnym. Zostaną one rozesłane do wszystkich urządzeń klienckich, dla których Serwer administracyjny jest źródłem uaktualnień.

Jeżeli zadanie *weryfikacji uaktualnień* wykaże niepoprawność uaktualnień znajdujących się w repozytorium tymczasowym lub podczas wykonywania *tego zadania* wystąpi błąd, uaktualnienia nie zostaną skopiowane do folderu współdzielonego. Serwer administracyjny zachowa poprzedni zestaw uaktualnień. Zaplanowane zadania wykonywane zgodnie z opcją terminarza **Po pobraniu nowych aktualizacji do repozytorium** również nie zostaną uruchomione. Te działania są wykonywane podczas następnego uruchomienia zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, jeśli skanowanie nowych uaktualnień przebiegło bez problemów.

Zestaw uaktualnień jest uważany za nieprawidłowy, jeżeli przynajmniej na jednym urządzeniu testującym jest spełniony jeden z następujących warunków:

- Wystąpił błąd zadania aktualizacji.
- Stan ochrony w czasie rzeczywistym aplikacji zabezpieczającej zmienił się po zastosowaniu uaktualnień.
- W trakcie wykonywania zadania skanowania na żądanie wykryto zainfekowany obiekt.
- Wystąpił błąd w funkcjonowaniu aplikacji Kaspersky.

Jeśli żaden z powyższych warunków nie wystąpił na żadnym urządzeniu testującym, zestaw uaktualnień jest uważany za poprawny, a zadanie *weryfikacji uaktualnień* uważa się za zakończone pomyślnie.

Zanim zaczniesz tworzyć zadanie *Weryfikacja aktualizacji*, zrealizuj wymagania wstępne:

1. Utwórz grupę administracyjną z kilkoma urządzeniami testowymi. Ta grupa będzie potrzebna do weryfikacji uaktualnień.

   Zaleca się korzystanie z urządzeń z najbardziej niezawodną ochroną i najpowszechniejszą konfiguracją aplikacji w całej sieci. Takie podejście zwiększa jakość i prawdopodobieństwo wykrycia wirusa podczas skanowania oraz minimalizuje ryzyko fałszywych alarmów. Jeśli na urządzeniach testujących zostaną wykryte wirusy, zadanie *weryfikacji uaktualnień* zakończy się niepowodzeniem.

2. Utwórz zadania aktualizacji i skanowania w poszukiwaniu złośliwego oprogramowania dla aplikacji obsługiwanej przez Kaspersky Security Center, na przykład Kaspersky Endpoint Security for Windows lub Kaspersky Security for Windows Server. Podczas tworzenia zadań aktualizacji i skanowania w poszukiwaniu złośliwego oprogramowania określ grupę administracyjną zawierającą urządzenia testowe.

   Zadanie *Weryfikacja aktualizacji* uruchamia kolejno zadania Aktualizacja i Skanowanie w poszukiwaniu szkodliwego oprogramowania na urządzeniach testowych, aby sprawdzić, czy wszystkie aktualizacje są prawidłowe. Ponadto podczas tworzenia zadania *Weryfikacja aktualizacji* musisz określić zadania Aktualizacja i Skanowanie w poszukiwaniu złośliwego oprogramowania.

3. Utwórz zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

W celu skonfigurowania Kaspersky Security Center do sprawdzania pobranych uaktualnień przed rozesłaniem ich na urządzenia klienckie:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij zadanie **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.
3. W otwartym oknie właściwości zadania przejdź do zakładki **Ustawienia aplikacji**, a następnie włącz opcję **Uruchom weryfikację aktualizacji**.
4. Jeśli zadanie *weryfikacji aktualizacji* istnieje, kliknij przycisk **Wybierz zadanie**. W oknie, które zostanie otwarte, wybierz zadanie *Weryfikacja aktualizacji* w grupie administracyjnej z urządzeniami testowymi.
5. Jeśli wcześniej nie utworzono zadania *Weryfikacja aktualizacji*, wykonaj następujące czynności:
   a. Kliknij przycisk **Nowe zadanie**.
   b. W otwartym kreatorze nowego zadania określ nazwę zadania, jeśli chcesz zmienić nazwę ustawienia wstępnego.
   c. Wybierz grupę administracyjną z urządzeniami testowymi, którą utworzono wcześniej.
   d. Najpierw wybierz zadanie aktualizacji wymaganej aplikacji obsługiwanej przez Kaspersky Security Center, a następnie wybierz zadanie skanowania w poszukiwaniu złośliwego oprogramowania.

      Następnie pojawiają się następujące opcje. Zalecamy pozostawienie ich włączonych:

      - **Uruchom urządzenie ponownie po aktualizacji baz danych**

        Po zaktualizowaniu antywirusowych baz danych na urządzeniu zalecamy ponowne uruchomienie urządzenia.

        Domyślnie opcja ta jest włączona.

      - **Sprawdź stan ochrony w czasie rzeczywistym po aktualizacji baz danych i ponownym uruchomieniu urządzenia**

        Jeżeli ta opcja jest włączona, zadanie *Weryfikacja aktualizacji* sprawdza, czy aktualizacje pobrane do repozytorium serwera administracyjnego są prawidłowe oraz czy poziom ochrony spadł po aktualizacji antywirusowej bazy danych i ponownym uruchomieniu urządzenia.

        Domyślnie opcja ta jest włączona.

   e. Określ konto, z którego zostanie uruchomione zadanie *Weryfikacja aktualizacji*. Możesz użyć swojego konta i pozostawić włączoną opcję **Konto domyślne**. Alternatywnie można określić, że zadanie powinno być uruchamiane na innym koncie, które ma niezbędne prawa dostępu. Aby to zrobić, wybierz opcję **Określ konto**, a następnie wprowadź poświadczenia tego konta.
6. Kliknij **Zapisz**, aby zamknąć okno właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

Automatyczna weryfikacja aktualizacji zostanie włączona. Teraz możesz uruchomić zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, które rozpocznie się od weryfikacji aktualizacji.

Tworzenie zadania Pobierz uaktualnienia do repozytoriów punktów dystrybucji

Zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji* działa tylko na urządzeniach punktów dystrybucji działających pod kontrolą systemu operacyjnego Windows. Urządzenia punktów dystrybucji działające pod kontrolą systemu operacyjnego Linux lub macOS nie mogą pobierać uaktualnień z serwerów aktualizacji Kaspersky. Jeśli w zakresie zadania znajduje się przynajmniej jedno urządzenie z systemem Linux lub macOS, zadanie będzie miało status *Nieudane*. Nawet wtedy, gdy zadanie zakończyło się pomyślnie na wszystkich urządzeniach z systemem Windows, zwróci błąd na pozostałych urządzeniach.

Możesz utworzyć zadanie *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla grupy administracyjnej. To zadanie będzie uruchamiane dla punktów dystrybucji znajdujących się w określonej grupie administracyjnej.

Możesz użyć tego zadania, na przykład, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktem(ami) dystrybucji jest droższy niż ruch sieciowy pomiędzy punktem(ami) dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do Internetu.

To zadanie jest wymagane do pobrania uaktualnień z serwerów aktualizacji Kaspersky do repozytoriów punktów dystrybucji. Lista aktualizacji obejmuje:

- Aktualizacje baz danych i modułów dla aplikacji zabezpieczających Kaspersky
- Aktualizacje komponentów Kaspersky Security Center
- Aktualizacje aplikacji zabezpieczających Kaspersky

Po pobraniu uaktualnień, mogą one zostać przesłane na zarządzane urządzenia.

Jeśli punkty dystrybucji łączą się z Internetem za pośrednictwem serwera proxy, należy określić odpowiednie ustawienia w zasadach Agenta sieciowego.

*W celu utworzenia zadania **Pobierz aktualizacje do repozytoriów punktów dystrybucji** dla wybranej grupy administracyjnej:*

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center, w polu **Typ zadania** wybierz **Pobierz aktualizacje do repozytoriów punktów dystrybucji**.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Wybierz przycisk opcji do określenia grupy administracyjnej, wyboru urządzeń lub urządzeń, do których stosowane jest zadanie.
6. W kroku **Zakończ tworzenie zadania**, jeśli chcesz zmienić domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

7. Kliknij przycisk **Utwórz**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

8. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

9. Na zakładce **Ustawienia aplikacji** okna właściwości zadania określ następujące ustawienia:

   - **Źródła aktualizacji**

     Jako źródła uaktualnień dla punktu dystrybucji można użyć następujących zasobów:

     - Serwery aktualizacji Kaspersky

       Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji.

       Opcja ta jest wybrana domyślnie.

     - Folder lokalny lub sieciowy

       Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

       > Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

   - **Folder do przechowywania aktualizacji**

     Ścieżka do określonego folderu na potrzeby przechowywania zapisanych aktualizacji. Możesz skopiować ścieżkę do określonego folderu do schowka. Nie możesz zmienić ścieżki do określonego folderu w przypadku zadania grupowego.

   - **Pobierz pliki diff**

     Ta opcja włącza funkcję pobierania plików diff.

     Domyślnie opcja ta jest wyłączona.

   - **Pobierz aktualizacje za pomocą starego schematu**

     Począwszy od wersji 14, Kaspersky Security Center pobiera aktualizacje baz danych i modułów oprogramowania przy użyciu nowego schematu. Aby aplikacja pobierała aktualizacje przy użyciu nowego schematu, źródło aktualizacji musi zawierać pliki aktualizacji z metadanymi zgodnymi z nowym schematem. Jeśli źródło aktualizacji zawiera pliki aktualizacji z metadanymi zgodnymi tylko ze starym schematem, włącz opcję **Pobierz aktualizacje za pomocą starego schematu**. W przeciwnym razie zadanie pobierania aktualizacji zakończy się niepowodzeniem.

     Na przykład musisz włączyć tę opcję, gdy folder lokalny lub sieciowy jest określony jako źródło aktualizacji, a pliki aktualizacji w tym folderze zostały pobrane przez jedną z następujących aplikacji:

     - Kaspersky Update Utility

       To narzędzie pobiera aktualizacje przy użyciu starego schematu.

- Kaspersky Security Center 13.2 lub wcześniejsza wersja

  Na przykład punkt dystrybucji jest skonfigurowany do pobierania aktualizacji z folderu lokalnego lub sieciowego. W takim przypadku aktualizacje można pobrać za pomocą serwera administracyjnego z połączeniem internetowym, a następnie umieścić je w folderze lokalnym w punkcie dystrybucji. Jeśli serwer administracyjny ma wersję 13.2 lub wcześniejszą, włącz opcję **Pobierz aktualizacje za pomocą starego schematu** w zadaniu *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

Domyślnie opcja ta jest wyłączona.

10. Utwórz terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- **Uruchom zadanie**

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - **Ręcznie**

    Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

    Domyślnie opcja ta jest zaznaczona.

  - **Co N minut**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

    Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

  - **Co N godzin**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

  - **Co N dni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

    Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Według dni tygodnia**

    Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

    Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

  - **Co miesiąc**

    Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

    W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

    Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

  - **Co miesiąc, w określone dni wybranych tygodni**

    Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

> Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

Można wybrać kilka dni tygodnia.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

- **Uruchom pominięte zadania**

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

Domyślnie opcja ta jest wyłączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj automatycznego losowego opóźnienia dla zadań uruchamianych w przedziale**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

11. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

    Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Po wykonaniu zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, aktualizacje baz danych i modułów aplikacji zostaną pobrane ze źródła uaktualnień i będą przechowywane w folderze współdzielonym. Pobrane uaktualnienia zostaną użyte tylko przez punkty dystrybucji, które znajdują się w określonej grupie administracyjnej i dla których nie ustawiono zadania pobierania aktualizacji.

Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center

Aktualizacje i poprawki dla Serwera administracyjnego mogą zostać zainstalowane tylko ręcznie, po uzyskaniu wyraźnego zatwierdzenia przez administratora.

Automatyczna instalacja uaktualnień i łat dla komponentów Kaspersky Security Center jest włączona domyślnie podczas instalacji Agenta sieciowego na urządzeniu. Możesz to wyłączyć podczas instalacji Agenta sieciowego lub wyłączyć później przy użyciu zasady.

W celu wyłączenia automatycznej aktualizacji i instalacji poprawek dla komponentów Kaspersky Security Center podczas lokalnej instalacji Agenta sieciowego na urządzeniu:

1. Uruchom lokalną instalację Agenta sieciowego na urządzeniu.
2. W kroku **Ustawienia zaawansowane** odznacz pole **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**.
3. Postępuj zgodnie z instrukcjami kreatora.

   Na urządzeniu zostanie zainstalowany Agent sieciowy z wyłączoną automatyczną aktualizacją i instalacją łat dla komponentów Kaspersky Security Center. Automatyczne aktualizowanie i instalowanie poprawek można włączyć w późniejszym czasie, korzystając z zasady.

W celu wyłączenia automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center podczas instalacji Agenta sieciowego na urządzeniu przy użyciu pakietu instalacyjnego:

1. W menu głównym przejdź do **Operacje** → **Repozytoria** → **Pakiety instalacyjne**.
2. Kliknij pakiet **Agent sieciowy Kaspersky Security Center <numer wersji>**.
3. W oknie właściwości otwórz zakładkę **Ustawienia**.
4. Wyłącz przycisk przełącznika **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**.

   Z tego pakietu zostanie zainstalowany Agent sieciowy z wyłączoną automatyczną aktualizacją i instalacją łat dla komponentów Kaspersky Security Center. Automatyczne aktualizowanie i instalowanie poprawek można włączyć w późniejszym czasie, korzystając z zasady.

Jeśli to pole zostało zaznaczone (lub odznaczone) podczas instalacji Agenta sieciowego na urządzeniu, możesz włączyć (lub wyłączyć) automatyczne aktualizowanie przy użyciu zasady Agenta sieciowa.

W celu włączenia lub wyłączenia automatycznego aktualizowania i instalowania poprawek dla składników Kaspersky Security Center przy użyciu zasady Agenta sieciowego:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Kliknij zasadę Agenta sieciowego.
3. W oknie ustawień zasady wybierz sekcję **Ustawienia aplikacji**.
4. W sekcji **Zarządzaj poprawkami i aktualizacjami** włącz lub wyłącz przycisk przełącznika **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**, aby włączyć lub wyłączyć automatyczne aktualizowanie i instalowanie łat.
5. Ustaw blokadę (🔒) dla tego przycisku przełącznika.

   Zasada zostanie zastosowana na wybranych urządzeniach, a automatyczne aktualizowanie i instalowanie poprawek dla komponentów Kaspersky Security Center zostanie włączone (lub wyłączone) na tych urządzeniach.

Pobieranie pakietu instalacyjnego dla Kaspersky Endpoint Security for Windows

Możesz skonfigurować automatyczne aktualizowanie baz danych i modułów aplikacji Kaspersky Endpoint Security for Windows na urządzeniach klienckich.

W celu skonfigurowania pobierania i automatycznej instalacji uaktualnień dla Kaspersky Endpoint Security for Windows na urządzeniach:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Endpoint Security for Windows, jako podtyp zadania wybierz **Aktualizacja**.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Wybierz obszar zadania.
6. Określ grupę administracyjną, wybór urządzeń lub urządzenia, do których stosowane jest zadanie.
7. W kroku **Zakończ tworzenie zadania**, jeśli chcesz zmienić domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
8. Kliknij przycisk **Utwórz**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.
9. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.
10. Na zakładce **Ustawienia aplikacji** okna właściwości zadania zdefiniuj ustawienia zadania aktualizacji w trybie lokalnym lub mobilnym:

    - **Tryb lokalny**: Połączenie jest nawiązywane między urządzeniem a Serwerem administracyjnym.
    - **Tryb mobilny**: Połączenie pomiędzy Kaspersky Security Center a urządzeniem nie jest nawiązywane (na przykład, jeśli urządzenie nie jest podłączone do internetu).
11. Włącz źródło aktualizacji, którego chcesz użyć do zaktualizowania baz danych i modułów aplikacji dla Kaspersky Endpoint Security for Windows. Jeśli jest to wymagane, zmień pozycje źródeł na liście, korzystając z przycisków **W górę** i **W dół**. Jeśli włączonych jest kilka źródeł aktualizacji, Kaspersky Endpoint Security for Windows próbuje nawiązać z nimi połączenie po kolei, rozpoczynając od góry listy, i wykonać zadanie aktualizacji, pobierając pakiet aktualizacyjny z pierwszego dostępnego źródła.
12. Włącz opcję **Zainstaluj zatwierdzone aktualizacje modułów aplikacji**, aby pobrać i zainstalować uaktualnienia modułów aplikacji wraz z bazami danych aplikacji.

Jeśli opcja jest włączona, Kaspersky Endpoint Security for Windows powiadamia użytkownika o dostępnych uaktualnieniach modułów aplikacji i włącza uaktualnienia modułów aplikacji do pakietu aktualizacyjnego podczas wykonywania zadania aktualizacji. Kaspersky Endpoint Security for Windows instaluje tylko te uaktualnienia, dla których ustawiłeś stan *Zatwierdzone*; zostaną zainstalowane lokalnie z poziomu interfejsu aplikacji lub poprzez Kaspersky Security Center.

Możesz także włączyć opcję **Automatycznie instaluj krytyczne aktualizacje modułów aplikacji**. Jeśli dla modułów aplikacji dostępne są jakiekolwiek aktualizacje, Kaspersky Endpoint Security for Windows automatycznie zainstaluje te ze stanem *Krytyczne*. Pozostałe aktualizacje zostaną zainstalowane, jak je zatwierdzisz.

Jeśli do zainstalowania uaktualnień modułów aplikacji wymagane jest przejrzenie i zaakceptowanie warunków Umowy licencyjnej i Polityki prywatności, aplikacja zainstaluje uaktualnienia po zaakceptowaniu warunków Umowy licencyjnej i Polityki prywatności przez użytkownika.

13. Zaznacz pole **Kopiuj uaktualnienia do folderu**, aby aplikacja zapisywała pobrane uaktualnienia w folderze, a następnie określ ścieżkę folderu.

14. Skonfiguruj terminarz zadania. Aby zapewnić dostarczanie aktualizacji na czas, zalecane jest włączenie opcji **Po pobraniu nowych uaktualnień do repozytorium**.

15. Kliknij **Zapisz**.

Podczas wykonywania zadania **Aktualizacja** aplikacja wysyła żądanie do serwerów aktualizacji Kaspersky.

Niektóre aktualizacje wymagają zainstalowania najnowszych wersji wtyczek zarządzających.

Zatwierdzanie i odrzucanie aktualizacji oprogramowania

Ustawienia zadania instalacji aktualizacji mogą wymagać zatwierdzenia aktualizacji, które mają zostać zainstalowane. Możesz zatwierdzić uaktualnienia, które muszą zostać zainstalowane, oraz odrzucić uaktualnienia, które nie muszą zostać zainstalowane.

Na przykład, możesz chcieć najpierw sprawdzić instalację aktualizacji w środowisku testowym i upewnić się, że nie wpływają negatywnie na działanie urządzeń, a następnie zezwolić na instalację tylko tych aktualizacji na urządzeniach klienckich.

Zatwierdzanie i odrzucanie aktualizacji jest dostępne tylko w przypadku Agenta sieciowego i aplikacji zarządzanych zainstalowanych na urządzeniach klienckich z systemem Windows. Bezproblemowa aktualizacja Serwera administracyjnego, Kaspersky Security Center Web Console i webowych wtyczek administracyjnych nie jest obsługiwana. Aby zaktualizować aplikacje, pobierz najnowsze wersje aplikacji z witryny internetowej Kaspersky, a następnie zainstaluj je ręcznie.

W celu zatwierdzenia lub odrzucenia jednej lub kilku aktualizacji:

1. W menu głównym przejdź do **Operacje → Aplikacje Kaspersky → Aktualizacje oprogramowania Kaspersky**.

   Zostanie wyświetlona lista dostępnych aktualizacji.

Aktualizacje zarządzanych aplikacji mogą wymagać zainstalowania określonej minimalnej wersji Kaspersky Security Center. Jeśli ta wersja jest nowsza niż aktualna wersja, te aktualizacje są wyświetlane, ale nie można ich zatwierdzić. Ponadto żadne pakiety instalacyjne nie mogą być tworzone z takich aktualizacji, dopóki nie zaktualizujesz Kaspersky Security Center. Zostaniesz poproszony o uaktualnienie instancji Kaspersky Security Center do wymaganej wersji minimalnej.

2. Wybierz uaktualnienia, które chcesz zatwierdzić lub odrzucić.

3. Kliknij **Zatwierdź**, aby zatwierdzić wybrane aktualizacje, lub **Odrzuć**, aby odrzucić wybrane aktualizacje.

   Domyślna wartość to *Niezdefiniowane*.

Aktualizacje, do których przypisałeś stan *Zatwierdzono*, są umieszczane w kolejce do instalacji.

Aktualizacje, do których przypisałeś stan *Odrzucono*, są odinstalowywane (jeśli to możliwe) ze wszystkich urządzeń, na których były wcześniej zainstalowane. Dodatkowo, nie zostaną one zainstalowane na innych urządzeniach w przyszłości.

Niektórych uaktualnień dla aplikacji firmy Kaspersky nie można odinstalować. Jeśli ustawiłeś dla nich stan *Odrzucono*, Kaspersky Security Center nie odinstaluje tych uaktualnień z urządzeń, na których były wcześniej zainstalowane. Jednakże te uaktualnienia nigdy nie zostaną zainstalowane na innych urządzeniach w przyszłości.

Jeśli ustawisz stan *Odrzucono* dla aktualizacji oprogramowania firm trzecich, te aktualizacje nie zostaną zainstalowane na urządzeniach, dla których planowane było ich zainstalowanie, ale jeszcze nie zostały zainstalowane. Uaktualnienia pozostaną na urządzeniach, na których zostały już zainstalowane. Jeśli musisz usunąć aktualizacje, możesz je usunąć ręcznie lokalnie.

Aktualizowanie Serwera administracyjnego

Aktualizacje Serwera administracyjnego można zainstalować przy użyciu Uaktualnij moduły Serwera administracyjnego.

W celu zainstalowania aktualizacji Serwera administracyjnego:

1. W menu głównym przejdź do **Operacje** → **Aplikacje Kaspersky** → **Aktualizacje oprogramowania Kaspersky**.

2. Usuń Uaktualnij moduły Serwera administracyjnego w jeden z następujących sposobów:

   - Kliknij nazwę aktualizacji Serwera administracyjnego na liście aktualizacji, a następnie w oknie, które zostanie otwarte, kliknij odnośnik **Uruchom kreatora aktualizacji Serwera administracyjnego**.

   - Kliknij odnośnik **Uruchom kreatora aktualizacji Serwera administracyjnego** w polu powiadomień w górnej części okna.

3. W oknie Uaktualnij moduły Serwera administracyjnego wybierz jedną z poniższych opcji, aby określić, kiedy zainstalować aktualizację:

   - **Zainstaluj teraz**. Wybierz tę opcję, jeśli chcesz zainstalować aktualizację teraz.
   - **Odrocz instalację**. Wybierz tę opcję, jeśli chcesz zainstalować aktualizację później. W takim przypadku zostanie wyświetlone powiadomienie o tej aktualizacji.
   - **Ignoruj aktualizację**. Wybierz tę opcję, jeśli nie chcesz instalować aktualizacji i nie chcesz otrzymywać powiadomień o tej aktualizacji.

4. Wybierz opcję **Utwórz kopię zapasową Serwera administracyjnego przed rozpoczęciem instalacji aktualizacji**, jeśli chcesz utworzyć kopię zapasową Serwera administracyjnego przed zainstalowaniem aktualizacji.

5. W celu zakończenia działania Kreatora kliknij przycisk **OK**.

W przypadku przerwania procesu tworzenia kopii zapasowej przerywany jest również proces instalacji aktualizacji.

Włączanie i wyłączanie trybu offline pobierania uaktualnień

Nie jest zalecane wyłączanie trybu offline pobierania uaktualnień. Wyłączenie tego trybu może spowodować błędy w dostarczeniu uaktualnień na urządzenia. W niektórych przypadkach specjalista z pomocy technicznej Kaspersky może zalecić wyłączenie opcji **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem**. Następnie upewnij się, że zadanie pobierania uaktualnień dla aplikacji firmy Kaspersky zostało skonfigurowane.

W celu włączenia lub wyłączenia trybu offline pobierania uaktualnień dla grupy administracyjnej:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.

2. Kliknij **Grupy**.

3. W strukturze grupy administracyjnej należy wybrać grupę administracyjną, dla której chcesz włączyć tryb offline pobierania uaktualnień.

4. Kliknij zasadę Agenta sieciowego.

   Zostanie otwarte okno właściwości zasady Agenta sieciowego.

   Domyślnie, ustawienia zasad podrzędnych są dziedziczone z zasad nadrzędnych i nie mogą być modyfikowane. Jeśli zasada, którą chcesz zmodyfikować, jest dziedziczona, w pierwszej kolejności powinieneś utworzyć nową zasadę dla Agenta sieciowego w żądanej grupie administracyjnej. W nowo utworzonej zasadzie możesz zmodyfikować ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

5. Na zakładce **Ustawienia aplikacji** wybierz sekcję **Zarządzaj poprawkami i aktualizacjami**.

6. Włącz lub wyłącz opcję **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)**, aby włączyć lub wyłączyć model offline dla pobierania uaktualnień.

   Domyślnie włączony jest tryb offline pobierania uaktualnień.

Tryb offline pobierania uaktualnień zostanie włączony lub wyłączony.

Aktualizowanie baz danych i modułów Kaspersky na urządzeniach offline

Aktualizowanie baz danych i modułów Kaspersky na zarządzanych urządzeniach jest ważnym zadaniem do utrzymania ochrony urządzeń przed wirusami i innymi zagrożeniami. Administratorzy zazwyczaj konfigurują regularne aktualizacje poprzez używanie repozytorium Serwera administracyjnego lub repozytoriów punktów dystrybucji.

Jeśli musisz aktualizować bazy danych i moduły na urządzeniu (lub grupie urządzeń), które nie jest połączone z Serwerem administracyjnym (głównym lub podrzędnym), punktem dystrybucji lub internetem, musisz użyć alternatywnych źródeł aktualizacji, takich jak serwer FTP lub folder lokalny. W tym przypadku musisz dostarczyć pliki żądanych aktualizacji przy użyciu masowego urządzenia przechowywania, takiego jak dysk flash lub zewnętrzny dysk twardy.

Możesz skopiować wymagane aktualizacje z:

- Serwera administracyjnego.

  Aby mieć pewność, że repozytorium Serwera administracyjnego zawiera aktualizacje wymagane dla aplikacji zabezpieczającej zainstalowanej na urządzeniu offline, przynajmniej na jednym z zarządzanych urządzeń online musi być zainstalowana ta sama aplikacja zabezpieczająca. Ta aplikacja musi być skonfigurowana do pobierania aktualizacji z repozytorium Serwera administracyjnego poprzez zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego.

- Dowolne urządzenie, na którym ta sama aplikacja zabezpieczająca jest zainstalowana i skonfigurowana do pobierania aktualizacji z repozytorium Serwera administracyjnego, repozytorium punktu dystrybucji lub bezpośrednie z serwerów aktualizacji Kaspersky.

Poniżej znajduje się przykład konfigurowania aktualizacji baz danych i modułów poprzez kopiowanie ich z repozytorium Serwera administracyjnego.

W celu zaktualizowania baz danych i modułów Kaspersky na urządzeniach offline:

1. Podłącz dysk wymienny do urządzenia, na którym jest zainstalowany Serwer administracyjny.

2. Skopiuj pliki aktualizacji na dysk wymienny.

   Domyślnie, aktualizacje znajdują się w następującej lokalizacji: \\<nazwa serwera>\KLSHARE\Updates.

   Alternatywnie możesz skonfigurować Kaspersky Security Center do regularnego kopiowania uaktualnień do folderu, który wybierzesz. W tym celu użyj opcji **Kopiuj pobrane aktualizacje do dodatkowych folderów** we właściwościach zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego. Jeśli dla tej opcji określisz folder znajdujący się na dysku flash lub wewnętrznym dysku twardym jako folder docelowy, to urządzenie masowego przechowywania będzie zawsze zawierało najnowszą wersję aktualizacji.

3. Na urządzeniach offline skonfiguruj aplikację zabezpieczającą (na przykład, Kaspersky Endpoint Security for Windows), aby pobierała uaktualnienia z folderu lokalnego lub zasobu współdzielonego, takiego jak serwer FTP lub folder współdzielony.

4. Skopiuj pliki aktualizacji z dysku wymiennego do folderu lokalnego lub zasobu współdzielonego, którego chcesz użyć jako źródła uaktualnień.

5. Na urządzeniu offline, które wymaga zainstalowania aktualizacji, uruchom zadanie aktualizacji Kaspersky Endpoint Security for Windows.

Po zakończeniu zadania aktualizacji, bazy danych i moduły Kaspersky są aktualne na urządzeniu.

Tworzenie kopii zapasowych i przywracanie wtyczek webowych

Kaspersky Security Center Web Console umożliwia wykonanie kopii zapasowej bieżącego stanu wtyczki webowej, aby móc później przywrócić zapisany stan. Na przykład, możesz utworzyć kopię zapasową wtyczki webowej przed aktualizacją jej do nowszej wersji. Po aktualizacji, jeśli nowsza wersja nie spełnia Twoich wymagań lub oczekiwań, możesz przywrócić poprzednią wersję wtyczki webowej z kopii zapasowej.

W celu utworzenia kopii zapasowej wtyczek webowych:

1. W menu głównym przejdź do **Ustawienia** → **Wtyczki sieciowe**.

2. W sekcji **Wtyczki sieciowe** wybierz wtyczki webowe, których kopię zapasową chcesz utworzyć, a następnie kliknij przycisk **Utwórz kopię zapasową**.

Kopia zapasowa wybranych wtyczek webowych zostanie utworzona. Utworzone kopie zapasowe można przeglądać w sekcji **Kopie zapasowe**.

W celu przywrócenia wtyczki webowej z kopii zapasowej:

1. W menu głównym przejdź do sekcji **Ustawienia** → **Kopie zapasowe**.

2. W sekcji **Kopie zapasowe** wybierz kopię zapasową wtyczki webowej, którą chcesz przywrócić, a następnie kliknij przycisk **Przywróć z kopii zapasowej**.

Wtyczka webowa zostanie przywrócona z wybranej kopii zapasowej.

Dostosowanie punktów dystrybucji i bram połączenia

Struktura grup administracyjnych w Kaspersky Security Center pełni następujące funkcje:

- Tworzy zakres zasad

  Istnieje alternatywny sposób stosowania odpowiednich ustawień na urządzeniach przy użyciu *profili zasad*. W tym przypadku ustawiasz zakres zasad ze znacznikami, lokalizacjami urządzeń w jednostkach organizacyjnych Active Directory, członkostwem w grupach zabezpieczeń Active Directory.

- Tworzy zakres zadań grupowych

  Istnieje sposób określania zakresu zadań grupowych, który nie jest oparty na hierarchii grup administracyjnych: korzystanie z zadań dla wyboru urządzeń oraz z zadań dla określonych urządzeń.

- Nadaje urządzeniom, wirtualnym Serwerom administracyjnym oraz podrzędnym Serwerom administracyjnym prawa dostępu
- Przypisuje punkty dystrybucji

Podczas tworzenia struktury grup administracyjnych należy wziąć pod uwagę topologię sieci organizacji dla optymalnego przydzielenia punktów dystrybucji. Optymalne przydzielenie punktów dystrybucji pozwala na zmniejszenie ruchu w sieci organizacji.

W zależności od schematu organizacyjnego oraz topologii sieci, w strukturze grup administracyjnych można zastosować następujące standardowe konfiguracje:

- Jedno biuro
- Wiele małych, zdalnych biur

Urządzenia pełniące rolę punktów dystrybucji muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

Standardowa konfiguracja punktów dystrybucji: Jedno biuro

W standardowej konfiguracji „jedno biuro" wszystkie urządzenia znajdują się w obrębie sieci organizacji i są dla siebie widoczne. Sieć organizacji może zawierać kilka oddzielnych części (sieci lub fragmentów sieci) połączonych ze sobą wąskimi kanałami.

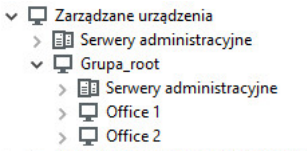
Dostępne są następujące metody tworzenia struktury grup administracyjnych:

- Tworzenie struktury grup administracyjnych z uwzględnieniem topologii sieci. Struktura grup administracyjnych nie musi odzwierciedlać topologii sieci z absolutną dokładnością. Wystarczy dopasowanie oddzielnych części sieci i pewnych grup administracyjnych. Możesz skorzystać z automatycznego przydzielenia punktów dystrybucji lub zrobić to ręcznie.
- Tworzenie struktury grup administracyjnych bez uwzględnienia topologii sieci. W tym przypadku należy wyłączyć automatyczne przydzielanie punktów dystrybucji, a następnie wskazać jedno lub kilka urządzeń jako punkty dystrybucji dla głównej grupy administracyjnej w każdej z oddzielnych części sieci, na przykład dla grupy **Zarządzane urządzenia**. Wszystkie punkty dystrybucji będą na tym samym poziomie i będą obejmować ten sam obszar, uwzględniając wszystkie urządzenia w sieci organizacji. W takim przypadku każdy z Agentów sieciowych połączy się z punktem dystrybucji o najkrótszej trasie. Trasę do punktu dystrybucji można ustalić za pomocą narzędzia tracert.

Standardowa konfiguracja punktów dystrybucji: Małe zdalne biura

Ta standardowa konfiguracja została utworzona z myślą o małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem internetu. Każde zdalne biuro znajduje się poza NAT, czyli połączenie jednego zdalnego biura z innym jest niemożliwe, gdyż biura są od siebie odizolowane.

Konfiguracja musi być odzwierciedlona w strukturze grup administracyjnych: dla każdego zdalnego biura musi zostać utworzona oddzielna grupa administracyjna (grupy **Office 1** i **Office 2** na rysunku poniżej).



Zdalne biura uwzględnione w strukturze grupy administracyjnej

Do każdej grupy administracyjnej odpowiadającej biuru należy przydzielić jeden lub kilka punktów dystrybucji. Punktami dystrybucji muszą być urządzenia w zdalnym biurze, które posiadają wystarczającą ilość wolnego miejsca na dysku. Urządzenia z grupy **Office 1** będą, na przykład, łączyć się z punktami dystrybucji przydzielonymi do grupy administracyjnej **Office 1**.

Jeśli niektórzy użytkownicy poruszają się między biurami ze swoimi laptopami, w każdym zdalnym biurze, dla grupy administracyjnej najwyższego poziomu (**Główna grupa dla biur** na poniższym rysunku) należy wskazać dwa lub więcej urządzeń jako punkty dystrybucji (oprócz już istniejących punktów dystrybucji).

Na przykład: Laptop znajduje się w grupie administracyjnej **Office 1**, a następnie zostaje fizycznie przeniesiony do biura, które odpowiada grupie administracyjnej **Office 2**. Po przeniesieniu laptopa, Agent sieciowy spróbuje połączyć się z punktami dystrybucji przypisanymi do grupy **Office 1**, ale te punkty dystrybucji są niedostępne. Następnie Agent sieciowy próbuje połączyć się z punktami dystrybucji, które zostały przypisane do **Głównej grupy dla biur**. Ponieważ zdalne biura są odizolowane od siebie, próby nawiązania połączenia z punktami dystrybucji przypisanymi do grupy administracyjnej **Główna grupa dla biur** zakończą się pomyślnie tylko wtedy, gdy Agent sieciowy spróbuje połączyć się z punktami dystrybucji w grupie **Office 2**. Oznacza to, że laptop pozostanie w grupie administracyjnej, która odpowiada pierwszemu biuru, ale będzie korzystał z punktu dystrybucji biura, w którym aktualnie się znajduje.

Informacje o przypisywaniu punktów dystrybucji

Możesz przypisać zarządzane urządzenie jako punkt dystrybucji ręcznie lub automatycznie.

Jeśli ręcznie przypiszesz zarządzane urządzenie jako punkt dystrybucji, możesz wybrać dowolne urządzenie w swojej sieci.

Jeśli przypiszesz punkty dystrybucji automatycznie, Kaspersky Security Center może wybrać tylko zarządzane urządzenie, które spełnia następujące warunki:

- Na urządzeniu jest przynajmniej 50 GB wolnej przestrzeni na dysku.
- Zarządzane urządzenie jest połączone bezpośrednio z Kaspersky Security Center (nie przez bramę).
- Zarządzane urządzenie nie jest laptopem.

> Jeśli w Twojej sieci nie ma urządzeń spełniających określone warunki, Kaspersky Security Center nie przypisze automatycznie żadnego urządzenia jako punktu dystrybucji.

Automatyczne przypisywanie punktów dystrybucji

Zalecane jest automatyczne przypisywanie punktów dystrybucji. W tym przypadku, Kaspersky Security Center sam wybierze urządzenia, które mają być punktami dystrybucji.

Urządzenia z systemem Microsoft Windows oparte na architekturze Arm nie mogą pełnić funkcji punktów dystrybucji.

Aby automatycznie przypisać punkty dystrybucji:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.

3. Wybierz opcję **Automatycznie przypisz punkty dystrybucji**.

   Jeśli włączone jest automatyczne wskazywanie urządzeń jako punktów dystrybucji, nie można ręcznie skonfigurować punktów dystrybucji, ani też zmodyfikować listy punktów dystrybucji.

4. Kliknij przycisk **Zapisz**.

Serwer administracyjny automatycznie przypisze i skonfiguruje punkty dystrybucji.

Ręczne przypisywanie punktów dystrybucji

Kaspersky Security Center umożliwia ręczne wskazanie urządzeń do pełnienia roli punktów dystrybucji.

Zalecane jest automatyczne przypisywanie punktów dystrybucji. W tym przypadku, Kaspersky Security Center sam wybierze urządzenia, które mają być punktami dystrybucji. Jednakże, jeśli z jakiegoś powodu musisz zrezygnować z automatycznego przypisywania punktów dystrybucji (na przykład, jeśli chcesz korzystać ze specjalnie wybranych serwerów), możesz ręcznie przypisać punkty dystrybucji po obliczeniu liczby i konfiguracji punktów dystrybucji.

Urządzenia pełniące rolę punktów dystrybucji muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

Urządzenia z systemem Microsoft Windows oparte na architekturze Arm nie mogą pełnić funkcji punktów dystrybucji.

W celu ręcznego wskazania urządzenia jako punktu dystrybucji:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.

3. Wybierz opcję **Ręcznie przypisz punkty dystrybucji**.

4. Kliknij przycisk **Przypisz**.

5. Wybierz urządzenie, które ma być punktem dystrybucji.

   Podczas wybierania urządzenia pamiętaj o zasadach działania punktów dystrybucji i wymaganiach ustawionych dla urządzenia pełniącego rolę punktu dystrybucji.

6. Wybierz grupę administracyjną, którą chcesz uwzględnić w obszarze wybranego punktu dystrybucji.

7. Kliknij przycisk **OK**.

   Dodany punkt dystrybucji będzie wyświetlany na liście punktów dystrybucji, w sekcji **Punkty dystrybucji**.

8. Na liście kliknij nowo dodany punkt dystrybucji, aby otworzyć jego okno właściwości.

9. Skonfiguruj punkt dystrybucji w oknie właściwości:

   - Sekcja **Ogólne** zawiera ustawienie interakcji pomiędzy punktem dystrybucji a urządzeniami klienckimi:

     - **Port SSL**

       Numer portu SSL do nawiązywania zaszyfrowanych połączeń między urządzeniami klienckimi a punktem dystrybucji przy użyciu SSL.

       Domyślnie wykorzystywany jest port 13000.

     - **Użyj multiemisji**

       Jeśli ta opcja jest włączona, multicasting IP będzie używany do automatycznego rozsyłania pakietów instalacyjnych na urządzenia klienckie w obrębie grupy.

       Multiemisja IP zmniejsza czas wymagany do zainstalowania aplikacji z pakietu instalacyjnego w grupie urządzeń klienckich, ale zwiększa czas instalacji, gdy instalujesz aplikację na jednym urządzeniu klienckim.

     - **Adres multiemisji IP**

       Adres IP, który będzie używany do multiemisji. Możesz zdefiniować adres IP z zakresu 224.0.0.0 – 239.255.255.255

       Domyślnie, Kaspersky Security Center automatycznie przypisze unikatowy adres IP multiemisji w obrębie danego zakresu.

     - **Numer portu multiemisji IP**

       Numer portu do multiemisji IP.

       Domyślnym numerem portu jest 15001. Jeśli jako punkt dystrybucji określono urządzenie, na którym działa Serwer administracyjny, domyślnie dla połączenia SSL używany jest port 13001.

     - **Adres punktu dystrybucji dla urządzeń zdalnych**

       Adres sieciowy, za pośrednictwem którego urządzenia zdalne łączą się z punktem dystrybucji.

- **Roześlij aktualizacje**

  Aktualizacje są dystrybuowane na zarządzane urządzenia z następujących źródeł:

  - Ten punkt dystrybucji, jeśli ta opcja jest włączona.
  - Inne punkty dystrybucji, Serwer administracyjny lub serwery aktualizacji Kaspersky, jeśli ta opcja jest wyłączona.

  Jeśli używasz punktów dystrybucji do wdrażania aktualizacji, możesz zmniejszyć ruch, ponieważ zmniejszasz liczbę pobrań. Możesz także odciążyć Serwer administracyjny i przenieść obciążenie między punktami dystrybucji. Możesz obliczyć liczbę punktów dystrybucji w Twojej sieci w celu optymalizacji ruchu i obciążenia.

  Jeśli wyłączysz tę opcję, liczba pobrań aktualizacji i obciążenia Serwera administracyjnego mogą wzrosnąć. Domyślnie opcja ta jest włączona.

- **Roześlij pakiety instalacyjne**

  Pakiety instalacyjne są dystrybuowane na zarządzane urządzenia z następujących źródeł:

  - Ten punkt dystrybucji, jeśli ta opcja jest włączona.
  - Inne punkty dystrybucji, Serwer administracyjny lub serwery aktualizacji Kaspersky, jeśli ta opcja jest wyłączona.

  Jeśli używasz punktów dystrybucji do wdrażania pakietów instalacyjnych, możesz zmniejszyć ruch, ponieważ zmniejszasz liczbę pobrań. Możesz także odciążyć Serwer administracyjny i przenieść obciążenie między punktami dystrybucji. Możesz obliczyć liczbę punktów dystrybucji w Twojej sieci w celu optymalizacji ruchu i obciążenia.

  Jeśli wyłączysz tę opcję, liczba pobrań pakietów instalacyjnych i obciążenie Serwera administracyjnego może wzrosnąć. Domyślnie opcja ta jest włączona.

- **Uruchom serwer push**

  W Kaspersky Security Center punkt dystrybucji może działać jako serwer push dla urządzeń zarządzanych za pośrednictwem protokołu mobilnego oraz zarządzanych za pośrednictwem agenta sieciowego. Na przykład, serwer push musi być włączony, jeśli chcesz mieć możliwość wymuszenia synchronizacji urządzeń KasperskyOS z Serwerem administracyjnym. Serwer push posiada ten sam obszar zarządzanych urządzeń jako punkt dystrybucji, na którym włączono serwer push. Jeśli posiadasz kilka punktów dystrybucji przypisanych dla tej samej grupy administracyjnej, możesz włączyć serwer push na każdym punkcie dystrybucji. W tym przypadku Serwer administracyjny rozkłada obciążenie między punkty dystrybucji.

- **Port serwera push**

  Numer portu serwera push. Możesz określić numer dowolnego zajętego portu.

- W sekcji **Zakres** określ obszar, w jakim punkt dystrybucji będzie rozsyłał uaktualnienia (grupy administracyjne i/lub lokalizacja sieciowa).

  Tylko urządzenia działające pod kontrolą systemu operacyjnego Windows mogą determinować swoją lokalizację sieciową. Lokalizacja sieciowa nie może zostać określona dla urządzeń z zainstalowanymi innymi systemami operacyjnymi.

- Jeżeli punkt dystrybucji działa na komputerze innym niż Serwer administracyjny, w sekcji **Źródło aktualizacji** możesz wybrać źródło aktualizacji dla punktu dystrybucji:

  - **Źródło aktualizacji**

    Wybierz źródło aktualizacji dla punktu dystrybucji:

    - Aby zezwolić punktowi dystrybucji na pobieranie uaktualnień z Serwera administracyjnego, zaznacz opcję **Pobierz z Serwera administracyjnego**.

    - Aby umożliwić punktowi dystrybucji otrzymywanie aktualizacji za pomocą zadania, wybierz **Użyj zadania pobierania aktualizacji**, a następnie określ zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

      - Jeśli takie zadanie już istnieje na urządzeniu, wybierz zadanie z listy.

      - Jeśli takie zadanie jeszcze nie istnieje na urządzeniu, kliknij łącze **Utwórz zadanie**, aby utworzyć zadanie. Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

  - **Pobierz pliki diff**

    Ta opcja włącza funkcję pobierania plików diff.

    Domyślnie opcja ta jest włączona.

- Jeśli Twoje punkty dystrybucji korzystają z serwera proxy podczas łączenia się z Internetem, w podsekcji **Ustawienia połączenia internetowego** możesz określić następujące ustawienia:

  - **Użyj serwera proxy**

    Jeśli to pole wyboru jest zaznaczone, do łączenia punktów dystrybucji z serwerami aktualizacji Kaspersky używany jest internetowy serwer proxy. W polach można skonfigurować połączenie z serwerem proxy.

    Domyślnie pole to nie jest zaznaczone.

  - **Adres serwera proxy**

    Adres serwera proxy.

  - **Numer portu**

    Numer portu używanego do nawiązywania połączenia.

  - **Pomiń serwer proxy dla adresów lokalnych**

    Jeśli ta opcja jest włączona, żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

    Domyślnie opcja ta jest wyłączona.

  - **Uwierzytelnianie na serwerze proxy**

    Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

    Domyślnie pole to nie jest zaznaczone.

  - **Nazwa użytkownika**

    Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy.

- **Hasło**

  Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

- W sekcji **KSN Proxy** możesz skonfigurować aplikację, aby używała punktu dystrybucji do przesyłania żądań KSN z zarządzanych urządzeń:

  - **Włącz KSN Proxy po stronie punktu dystrybucji**

    Usługa KSN proxy jest uruchamiana na urządzeniu, które jest używane jako punkt dystrybucji. Użyj tej funkcji do redystrybucji i optymalizacji ruchu w sieci.

    Punkt dystrybucji wysyła statystyki KSN, które zostały wymienione w Oświadczeniu Kaspersky Security Network, do Kaspersky.

    Domyślnie opcja ta jest wyłączona. Włączenie tej opcji działa, jeśli opcje **Użyj Serwera administracyjnego jako serwera proxy** i **Zgadzam się na korzystanie z Kaspersky Security Network** zostały włączone w oknie właściwości Serwera administracyjnego.

    Możesz przypisać węzeł klastra aktywny-pasywny do punktu dystrybucji i włączyć serwer proxy KSN na tym węźle.

  - **Przesyłaj żądania KSN do Serwera administracyjnego**

    Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do Serwera administracyjnego.

    Domyślnie opcja ta jest włączona.

  - **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**

    Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do chmury KSN lub KPSN. Żądania KSN wygenerowane na samym punkcie dystrybucji są także wysyłane bezpośrednio do chmury KSN lub KPSN.

    Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej), nie mogą uzyskać bezpośredniego dostępu do KPSN. Jeśli chcesz ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do KPSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji.

    Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 12 (lub późniejszej), mogą uzyskać bezpośredni dostęp do KPSN.

  - **Ignoruj ustawienia serwera proxy w przypadku łączenia z KPSN**

    Włącz tę opcję, jeśli skonfigurowałeś ustawienia serwera proxy we właściwościach punktu dystrybucji lub w zasadzie Agenta sieciowego, ale architektura Twojej sieci wymaga bezpośredniego korzystania z KPSN. W przeciwnym razie, żądania z zarządzanych aplikacji nie będą mogły dotrzeć do KPSN.

    Ta opcja jest dostępna, jeśli wybierzesz opcję **Dostęp do KSN Cloud/KPSN bezpośrednio przez Internet**.

  - **Port**

    Numer portu TCP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny numer portu to 13111.

  - **Użyj portu UDP**

    Jeśli chcesz, żeby zarządzane urządzenia nawiązywały połączenie z serwerem KSN proxy poprzez port UDP, włącz opcję **Użyj portu UDP** i określ numer portu UDP. Domyślnie opcja ta jest włączona.

- **Port UDP**

  Numer portu UDP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny port UDP do nawiązywania połączenia z serwerem KSN Proxy to 15111.

- Jeżeli punkt dystrybucji działa na komputerze innym niż Serwer administracyjny, w sekcji **Brama połączenia** możesz skonfigurować punkt dystrybucji tak, aby działał jako brama dla połączenia między instancjami Agenta sieciowego a Serwerem administracyjnym:

  - **Brama połączenia**

    Jeżeli bezpośrednie połączenie między Serwerem administracyjnym a Agentami sieciowymi nie może zostać nawiązane z powodu organizacji Twojej sieci, możesz użyć punktu dystrybucji, aby działał jako brama połączenia między Serwerem administracyjnym a Agentami sieciowymi.

    Włącz tę opcję, jeśli chcesz, aby punkt dystrybucji działał jako brama połączenia między Agentami sieciowymi a Serwerem administracyjnym. Domyślnie opcja ta jest wyłączona.

  - **Nawiąż połączenie z bramą z poziomu Serwera administracyjnego (jeśli brama znajduje się w DMZ)**

    Jeżeli Serwer administracyjny znajduje się poza strefą zdemilitaryzowaną (DMZ), w sieci lokalnej, Agenty sieciowe zainstalowane na zdalnych urządzeniach nie mogą łączyć się z Serwerem administracyjnym. Możesz użyć punktu dystrybucji jako bramy połączenia z odwrotną łącznością (Serwer administracyjny nawiązuje połączenie z punktem dystrybucji).

    Włącz tę opcję, jeśli chcesz połączyć Serwer administracyjny z bramą połączenia w strefie DMZ.

  - **Otwórz port lokalny dla Kaspersky Security Center Web Console**

    Włącz tę opcję, jeśli chcesz, aby brama połączenia w strefie DMZ otwierała port dla Web Console znajdujący się w strefie DMZ lub w Internecie. Określ numer portu, który będzie używany do połączenia z Web Console do punktu dystrybucji. Domyślny numer portu to 13299.

    Ta opcja jest dostępna, jeśli włączysz opcję **Nawiąż połączenie z bramą z poziomu Serwera administracyjnego (jeśli brama znajduje się w DMZ)**.

  Podczas podłączania urządzeń mobilnych do Serwera administracyjnego za pośrednictwem punktu dystrybucji pełniącego funkcję bramy połączenia można włączyć następujące opcje:

  - **Otwórz port dla urządzeń mobilnych (tylko uwierzytelnianie SSL Serwera administracyjnego)**

    Włącz tę opcję, jeśli potrzebujesz, aby brama połączenia otwierała port dla urządzeń mobilnych i określała numer portu, którego będą używać urządzenia mobilne do łączenia się z punktem dystrybucji. Domyślny numer portu to 13292. Urządzenie mobilne sprawdzi certyfikat Serwera administracyjnego. Podczas nawiązywania połączenia uwierzytelniany jest tylko Serwer administracyjny.

  - **Otwórz port dla urządzeń mobilnych (wzajemne uwierzytelnianie SSL)**

    Włącz tę opcję, jeśli potrzebujesz bramy połączenia, aby otworzyć port, który będzie używany do dwukierunkowej autoryzacji Serwera administracyjnego i urządzeń mobilnych. Urządzenie mobilne sprawdzi certyfikat Serwera administracyjnego, a Serwer administracyjny sprawdzi certyfikat urządzenia mobilnego. Określ następujące parametry:

    - Numer portu, którego urządzenia mobilne będą używać do łączenia się z punktem dystrybucji. Domyślny numer portu to 13293.

    - Nazwy domen DNS bramy połączenia, które będą używane przez urządzenia mobilne. Oddziel nazwy domen przecinkami. Określone nazwy domen zostaną uwzględnione w certyfikacie punktu dystrybucji. Jeśli nazwy domen używane przez urządzenia mobilne nie są zgodne z nazwą wspólną w certyfikacie punktu dystrybucji, urządzenia mobilne nie łączą się z punktem dystrybucji.

      Domyślną nazwą domeny DNS jest nazwa FQDN bramy połączenia.

W obu przypadkach certyfikaty są sprawdzane wyłącznie podczas nawiązywania sesji TLS w punkcie dystrybucji. Certyfikaty nie są przesyłane do sprawdzenia przez Serwer administracyjny. Po nawiązaniu sesji TLS z urządzeniem mobilnym punkt dystrybucji używa certyfikatu serwera administracyjnego w celu utworzenia tunelu umożliwiającego synchronizację między urządzeniem mobilnym a Serwerem administracyjnym. Jeśli otworzysz port dla dwukierunkowego uwierzytelniania SSL, jedynym sposobem na dystrybucję certyfikatu urządzenia mobilnego będzie użycie pakietu instalacyjnego.

- Skonfiguruj przeszukiwanie domen Windows, Active Directory i zakresów IP przez punkt dystrybucji:

  - **Domeny Windows**

    Możesz włączyć wykrywanie urządzeń dla domen Windows i ustawić terminarz dla wyszukiwania.

  - **Kontrolery domeny**

    Możesz włączyć przeszukiwanie sieci dla Active Directory i ustawić terminarz dla przeszukiwania.

    Jeśli korzystasz z punktu dystrybucji systemu Windows, możesz wybrać jedną z następujących opcji:

    - **Przeszukaj bieżącą domenę Active Directory**.
    - **Przeszukaj las domen Active Directory**.
    - **Przeszukaj tylko wybrane domeny Active Directory**. Jeśli wybierzesz tę opcję, dodaj jedną lub kilka domen Active Directory do listy.

    Jeśli korzystasz z punktu dystrybucji systemu Linux z zainstalowanym Agentem sieciowym w wersji 15, możesz odpytywać tylko domeny Active Directory, dla których określisz adres i poświadczenia użytkownika. Sondowanie bieżącej domeny Active Directory i lasu domeny Active Directory nie jest dostępne.

    Możesz włączyć wykrywanie urządzeń dla kontrolerów domeny.

    Jeśli wybierzesz opcję **Włącz przeszukiwanie sterowników domeny**, możesz wybrać kontrolery domeny do odpytywania, a także określić terminarz ich przeszukiwania.

    Jeśli korzystasz z punktu dystrybucji systemu Linux, w sekcji **Przeszukaj określone domeny** kliknij opcję **Dodaj**, a następnie określ adres i dane uwierzytelniające użytkownika kontrolera domeny.

    Jeśli korzystasz z punktu dystrybucji systemu Windows, możesz wybrać jedną z następujących opcji:

    - **Przeszukaj bieżącą domenę**
    - **Przeszukaj cały las domeny**
    - **Przeszukaj określone domeny**

  - **Zakresy IP**

    Możesz włączyć wykrywanie urządzeń dla zakresów IPv4 i sieci IPv6.

    Jeśli włączysz opcję **Włącz przeszukiwanie zakresów**, możesz dodać skanowane zakresy i skonfigurować dla nich terminarz. Możesz dodać zakresy IP do listy skanowanych zakresów.

    Jeśli włączysz opcję **Użyj Zeroconf do przeszukiwania sieci IPv6**, punkt dystrybucji automatycznie odpytuje sieć IPv6 za pomocą zero-configuration networking (zwany również *Zeroconf*). W takim przypadku określone zakresy adresów IP są ignorowane, ponieważ punkt dystrybucji przeszukuje całą sieć. Opcja **Użyj Zeroconf do przeszukiwania sieci IPv6** jest dostępna, jeśli w punkcie dystrybucji działa system Linux. Aby korzystać z odpytywania Zeroconf IPv6, musisz zainstalować narzędzie avahi-browse w punkcie dystrybucji.

- W sekcji **Zaawansowane** określ folder, którego punkt dystrybucji musi używać do przechowywania rozsyłanych danych:

  - **Użyj folderu domyślnego**

    Jeśli wybierzesz tę opcję, aplikacja użyje folderu instalacyjnego Agenta sieciowego na urządzeniu działającym jako punkt dystrybucji.

  - **Użyj określonego folderu**

    Jeśli wybierzesz tę opcję, w polu poniżej możesz określić ścieżkę dostępu do wybranego folderu. Może to być folder lokalny na urządzeniu działającym jako punkt dystrybucji lub folder na dowolnym urządzeniu w obrębie sieci korporacyjnej.

    Konto użytkownika używane na urządzeniu działającym jako punkt dystrybucji do uruchamiania Agenta sieciowego musi mieć uprawnienia do odczytu/zapisu określonego folderu.

10. Kliknij przycisk **OK**.

Wybrane urządzenia będą pełnić rolę punktów dystrybucji.

Modyfikowanie listy punktów dystrybucji dla grupy administracyjnej

Możesz wyświetlić listę punktów dystrybucji przypisanych do określonej grupy administracyjnej oraz zmodyfikować listę, dodając lub usuwając punkty dystrybucji.

W celu przejrzenia i zmodyfikowania listy punktów dystrybucji przypisanych do grupy administracyjnej:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
2. W polu **Bieżąca ścieżka** nad listą zarządzanych urządzeń kliknij łącze ścieżki.
3. W otwartym okienku po lewej stronie wybierz grupę administracyjną, dla której chcesz wyświetlić przypisane punkty dystrybucji.

   Spowoduje to włączenie pozycji menu **Punkty dystrybucji**.
4. W menu głównym przejdź do **Zasoby (urządzenia)** → **Punkty dystrybucji**.
5. Aby dodać nowe punkty dystrybucji dla grupy administracyjnej, kliknij przycisk **Przypisz** nad listą zarządzanych urządzeń i wybierz urządzenia z otwartego panelu.
6. Aby usunąć przypisane punkty dystrybucji, wybierz urządzenia z listy i kliknij przycisk **Cofnij przypisanie**.

W zależności od Twoich modyfikacji, nowe punkty dystrybucji są dodawane do listy lub istniejące punkty dystrybucji zostają usunięte z listy.

Wymuszona synchronizacja

Pomimo tego, że Kaspersky Security Center automatycznie synchronizuje stan, ustawienia, zadania i zasady dla zarządzanych urządzeń, w niektórych przypadkach możesz chcieć wymusić uruchomienie synchronizacji dla określonego urządzenia. Możesz uruchomić wymuszoną synchronizację dla następujących urządzeń:

- Urządzenia, na których jest zainstalowany Agent sieciowy
- Urządzenia działające pod kontrolą systemu operacyjnego KasperskyOS

  Przed uruchomieniem wymuszonej synchronizacji dla urządzenia KasperskyOS upewnij się, że urządzenie znajduje się w obszarze punktu dystrybucji oraz że serwer push jest włączony na punkcie dystrybucji.
- Urządzenia iOS
- Urządzenia Android

  Przed uruchomieniem wymuszonej synchronizacji dla urządzenia Android musisz skonfigurować Firebase Cloud Messaging.

Synchronizowanie pojedynczego urządzenia

W celu wymuszenia synchronizacji między Serwerem administracyjnym a zarządzanym urządzeniem:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
2. Kliknij nazwę urządzenia, które chcesz zsynchronizować z Serwerem administracyjnym.

   Zostanie otwarte okno właściwości na wybranej sekcji **Ogólne**.
3. Kliknij przycisk **Wymuś synchronizację**.

Aplikacja synchronizuje wybrane urządzenie z Serwerem administracyjnym.

Synchronizowanie kilku urządzeń

W celu wymuszenia synchronizacji między Serwerem administracyjnym a kilkoma zarządzanymi urządzeniami:

1. Otwórz listę urządzeń grupy administracyjnej lub wyboru urządzeń:
   - W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**, kliknij odnośnik ścieżki w polu **Bieżąca ścieżka** nad listą zarządzanych urządzeń, a następnie wybierz grupę administracyjną zawierającą urządzenia do synchronizacji.
   - Uruchom wybór urządzeń, aby przejrzeć listę urządzeń.
2. Zaznacz pola obok urządzeń, które chcesz zsynchronizować z Serwerem administracyjnym.

3. Nad listą zarządzanych urządzeń kliknij przycisk wielokropka (...), a następnie kliknij przycisk **Wymuś synchronizację**.

   Aplikacja synchronizuje wybrane urządzenia z Serwerem administracyjnym.

4. Na liście urządzeń sprawdź, czy czas ostatniego połączenia z Serwerem administracyjnym uległ zmianie dla wybranych urządzeń na bieżący czas. Jeśli czas nie został zmieniony, wówczas zmień zawartość strony, klikając przycisk **Odśwież**.

Wybrane urządzenia zostaną zsynchronizowane z Serwerem administracyjnym.

Przeglądanie czasu dostarczenia zasady

Po zmianie zasady dla aplikacji Kaspersky na Serwerze administracyjnym, administrator może sprawdzić, czy zmieniona zasada została dostarczona do określonego zarządzanego urządzenia. Zasada może zostać dostarczona podczas regularnej synchronizacji lub wymuszonej synchronizacji.

W celu sprawdzenia daty i godziny dostarczenia zasady aplikacji na zarządzane urządzenie:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
2. Kliknij nazwę urządzenia, które chcesz zsynchronizować z Serwerem administracyjnym.

   Zostanie otwarte okno właściwości na wybranej sekcji **Ogólne**.
3. Wybierz zakładkę **Aplikacje**.
4. Wybierz aplikację, dla której chcesz sprawdzić datę synchronizacji zasady.

   Zostanie otwarte okno zasady aplikacji na sekcji **Ogólne** i z wyświetloną datą i godziną dostarczenia zasady.

Włączanie serwera push

W Kaspersky Security Center punkt dystrybucji może działać jako serwer push dla urządzeń zarządzanych za pośrednictwem protokołu mobilnego oraz zarządzanych za pośrednictwem agenta sieciowego. Na przykład, serwer push musi być włączony, jeśli chcesz mieć możliwość wymuszenia synchronizacji urządzeń KasperskyOS z Serwerem administracyjnym. Serwer push posiada ten sam obszar zarządzanych urządzeń jako punkt dystrybucji, na którym włączono serwer push. Jeśli posiadasz kilka punktów dystrybucji przypisanych dla tej samej grupy administracyjnej, możesz włączyć serwer push na każdym punkcie dystrybucji. W tym przypadku Serwer administracyjny rozkłada obciążenie między punkty dystrybucji.

Punktów dystrybucji można używać jako serwerów push, aby zapewnić ciągłą łączność między zarządzanym urządzeniem a Serwerem administracyjnym. W przypadku niektórych operacji, takich jak uruchamianie i zatrzymywanie zadań lokalnych, odbieranie statystyk dla zarządzanej aplikacji lub tworzenie tunelu, wymagana jest ciągła łączność. Jeśli używasz punktu dystrybucji jako serwera push, nie musisz używać opcji **Nie odłączaj od Serwera administracyjnego** na zarządzanych urządzeniach lub wysyłaj pakiety do portu UDP Agenta sieciowego.

Serwer push obsługuje do 50 000 jednoczesnych połączeń.

W celu włączenia serwera push na punkcie dystrybucji:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.
3. Kliknij nazwę punktu dystrybucji, na którym chcesz włączyć serwer push.

   Spowoduje to otwarcie okna właściwości punktu dystrybucji.
4. W sekcji **Ogólne** włącz opcję **Uruchom serwer push**.
5. W polu **Port serwera push** wpisz numer portu. Możesz określić numer dowolnego zajętego portu.
6. W polu **Adres zdalnych hostów** określ adres IP lub nazwę urządzenia punktu dystrybucyjnego.
7. Kliknij przycisk **OK**.

Serwer push jest włączony na wybranym punkcie dystrybucyjnym.

Zarządzanie aplikacjami firm trzecich na urządzeniach klienckich

Ta sekcja opisuje funkcje Kaspersky Security Center, które dotyczą zarządzania aplikacjami firm trzecich zainstalowanymi na urządzeniach klienckich.

Instalowanie aktualizacji oprogramowania firm trzecich

Kaspersky Security Center umożliwia zarządzanie aktualizacjami oprogramowania firm trzecich, zainstalowanego na zarządzanych urządzeniach, oraz wyeliminowanie luk w aplikacjach Microsoft i produktach innych dostawców poprzez zainstalowanie żądanych aktualizacji.

Kaspersky Security Center wyszukuje aktualizacje za pośrednictwem zadania *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Serwer administracyjny pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania. Po przejrzeniu informacji o dostępnych aktualizacjach, możesz zainstalować je na urządzeniach.

> Kaspersky Security Center aktualizuje niektóre aplikacje poprzez usunięcie poprzedniej wersji aplikacji i instalację nowej.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Ze względów bezpieczeństwa wszelkie aktualizacje oprogramowania innych firm, które instalujesz za pomocą funkcji Zarządzanie lukami i poprawkami, są automatycznie skanowane w poszukiwaniu szkodliwego oprogramowania przez technologie firmy Kaspersky. Technologie te są używane do automatycznego sprawdzania plików i obejmują skanowanie antywirusowe, analizę statyczną, analizę dynamiczną, analizę zachowania w środowisku sandbox i uczenie maszynowe.

Eksperci firmy Kaspersky nie przeprowadzają ręcznej analizy aktualizacji oprogramowania innych firm, które są instalowane przez funkcję Zarządzanie lukami i poprawkami. Ponadto eksperci z firmy Kaspersky nie wyszukują luk (znanych lub nieznanych) ani nieudokumentowanych funkcji w takich aktualizacjach, a także nie przeprowadzają innych rodzajów analizy aktualizacji innych, niż określone w powyższym akapicie.

Zadania instalacji aktualizacji oprogramowania firm trzecich

Jeśli metadane aktualizacji oprogramowania firm trzecich są pobierane do repozytorium, możesz zainstalować aktualizacje na urządzeniach klienckich, korzystając z następujących zadań:

- Zadanie *Zainstaluj wymagane aktualizacje i napraw luki*

  Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do zainstalowania aktualizacji dla aplikacji firmy Microsoft, w tym aktualizacji dostarczonych przez usługę Windows Update, a także aktualizacji produktów innych producentów. Pamiętaj, że to zadanie może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami.

  Jeśli to zadanie zostanie zakończone, aktualizacje zostaną automatycznie zainstalowane na zarządzanych urządzeniach. Jeśli metadane nowych aktualizacji zostaną pobrane do repozytorium Serwera administracyjnego, Kaspersky Security Center sprawdzi, czy aktualizacje spełniają kryteria określone w regułach aktualizacji. Wszystkie nowe aktualizacje, które spełniają kryteria, zostaną pobrane i zainstalowane automatycznie przy kolejnym uruchomieniu zadania.

- Zadanie *Zainstaluj aktualizacje Windows Update*

  Zadanie *Zainstaluj aktualizacje Windows Update* nie wymaga licencji, ale może zostać użyte tylko do zainstalowania aktualizacji Windows Update.

  Jeśli to zadanie zostanie zakończone, zostaną zainstalowane tylko te aktualizacje, które zostały określone we właściwościach zadania. W przyszłości, jeśli będziesz chciał zainstalować nowe aktualizacje pobrane do repozytorium Serwera administracyjnego, będziesz musiał dodać wymagane aktualizacje do listy aktualizacji w istniejącym zadaniu lub utworzyć nowe zadanie Zainstaluj aktualizacje Windows Update.

Używanie Serwera administracyjnego jako serwera WSUS

Informacje o aktualizacjach dostępnych dla Microsoft Windows są dostępne poprzez usługę Windows Update. Serwer administracyjny może zostać użyty jako serwer Windows Server Update Services (WSUS). Aby użyć Serwera administracyjnego jako serwera WSUS, utwórz zadanie Wykonaj synchronizację Windows Update i wybierz opcję **Użyj Serwera administracyjnego jako serwera WSUS** w zasadzie Agenta sieciowego. Po skonfigurowaniu synchronizacji danych z Windows Update, Serwer administracyjny zapewnia aktualizacje dla usług Windows Update na urządzeniach w trybie scentralizowanym i z określoną częstotliwością.

Scenariusz: Aktualizowanie oprogramowania innej firmy

Ta sekcja oferuje scenariusz aktualizacji oprogramowania innej firmy, zainstalowanego na urządzeniach klienckich. Oprogramowanie firm trzecich obejmuje aplikacje firmy Microsoft oraz programy innych firm. Aktualizacje dla aplikacji firmy Microsoft są dostarczane przez usługę Windows Update.

Wymagania wstępne

Serwer administracyjny musi mieć połączenie z Internetem, aby zainstalować aktualizacje oprogramowania firm trzecich innego niż oprogramowanie firmy Microsoft.

Domyślnie połączenie internetowe w przypadku Serwera administracyjnego nie jest wymagane w celu instalowania aktualizacji oprogramowania firmy Microsoft na zarządzanych urządzeniach. Na przykład zarządzane urządzenia mogą pobierać aktualizacje oprogramowania firmy Microsoft bezpośrednio z serwerów Microsoft Update lub z systemu Windows Server z programem Microsoft Windows Server Update Services (WSUS) wdrożonymi w sieci organizacji. Serwer administracyjny musi być połączony z Internetem, jeśli jest on używany jako serwer WSUS.

Etapy

Aktualizowanie oprogramowania firm trzecich odbywa się w etapach:

1. **Wyszukiwanie wymaganych aktualizacji**

   Aby odnaleźć aktualizacje oprogramowania firm trzecich dla zarządzanych urządzeń, uruchom zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Kaspersky Security Center pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania.

   Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie przez Kreator wstępnej konfiguracji Serwera administracyjnego. Jeśli nie uruchomiono kreatora, utwórz zadanie lub uruchom Kreator wstępnej konfiguracji teraz.

   Dostępne instrukcje:

   - Konsola administracyjna: Skanowanie aplikacji w poszukiwaniu luk, Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
   - Kaspersky Security Center Web Console: Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji, Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

2. **Analizowanie listy wykrytych aktualizacji**

   Przejrzyj listę **Aktualizacje oprogramowania** i zdecyduj, które aktualizacje chcesz zainstalować. Aby przejrzeć szczegółowe informacje o każdej aktualizacji, kliknij nazwę aktualizacji na liście. Dla każdej aktualizacji na liście możesz także przejrzeć statystyki dotyczące instalacji aktualizacji na urządzeniach klienckich.

   Dostępne instrukcje:

   - Konsola administracyjna: Przeglądanie informacji o dostępnych aktualizacjach
   - Kaspersky Security Center Web Console: Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich

3. **Konfigurowanie instalacji aktualizacji**

   Jeśli Kaspersky Security Center odebrał listę aktualizacji oprogramowania firm trzecich, możesz zainstalować je na urządzeniach klienckich przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki* lub zadania *Zainstaluj aktualizacje Windows Update*. Utwórz jedno z tych zadań. Możesz utworzyć te zadania na zakładce **Zadania** lub korzystając z listy **Aktualizacje oprogramowania**.

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do zainstalowania aktualizacji dla aplikacji firmy Microsoft, w tym aktualizacji dostarczonych przez usługę Windows Update, a także aktualizacji produktów innych producentów. Pamiętaj, że to zadanie może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami.

Zadanie *Zainstaluj aktualizacje Windows Update* nie wymaga licencji, ale może zostać użyte tylko do zainstalowania aktualizacji Windows Update.

Aby zainstalować niektóre aktualizacje oprogramowania, należy zaakceptować Umowę licencyjną użytkownika końcowego (EULA) do zainstalowania oprogramowania. Jeśli odrzucisz Umowę licencyjną użytkownika końcowego, aktualizacja oprogramowania nie zostanie zainstalowana.

Możesz uruchomić zadanie instalacji aktualizacji zgodnie z terminarzem. Podczas określania terminarza zadania upewnij się, że zadanie instalacji aktualizacji jest uruchamiane po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

Dostępne instrukcje:

- Konsola administracyjna: Naprawianie luk w aplikacjach, Przeglądanie informacji o dostępnych aktualizacjach
- Kaspersky Security Center Web Console: Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki, Tworzenie zadania Zainstaluj aktualizacje Windows Update, Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich

4 Konfigurowanie terminarza zadań

Aby upewnić się, że lista aktualizacji jest zawsze aktualna, skonfiguruj terminarz zadania *Wyszukiwanie luk i wymaganych aktualizacji* tak, aby było uruchamiane automatycznie od czasu do czasu. Domyślnie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest ustawione na uruchamianie ręczne.

Jeśli utworzyłeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz skonfigurować terminarz tak, aby zadanie było uruchamiane z tą samą częstotliwością co zadanie *Wyszukiwanie luk i wymaganych aktualizacji* lub rzadziej. Podczas konfigurowania terminarza zadania *Zainstaluj aktualizacje Windows Update* należy pamiętać, że dla tego zadania konieczne jest zdefiniowanie listy aktualizacji za każdym razem przed uruchomieniem tego zadania.

Jeśli konfigurujesz terminarz uruchamiania zadań, upewnij się, że zadanie instalacji aktualizacji zostanie uruchomione po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

5 Zatwierdzanie i odrzucanie aktualizacji oprogramowania (opcjonalne)

Jeśli utworzyłeś zadanie Zainstaluj wymagane aktualizacje i napraw luki, możesz określić reguły instalacji aktualizacji we właściwościach zadania. Jeśli utworzyłeś zadanie Zainstaluj aktualizacje Windows Update, pomiń ten krok.

Dla każdej reguły możesz zdefiniować aktualizacje do zainstalowania w zależności od stanu aktualizacji: *Nie zdefiniowano*, *Zatwierdzono* lub *Odrzucono*. Na przykład, możesz utworzyć określone zadanie dla serwerów i ustawić regułę dla tego zadania, aby zezwolić na instalację tylko aktualizacji Windows Update i tylko tych, które posiadają stan *Zatwierdzono*. Po ręcznym ustawieniu stanu *Zatwierdzono* dla tych aktualizacji, które chcesz zainstalować. W tym przypadku aktualizacje Windows Update, które posiadają stan *Nie zdefiniowano* lub *Odrzucono*, nie będą zainstalowane na serwerach, które określiłeś w zadaniu.

Używanie stanu *Zatwierdzone* do zarządzania instalacją aktualizacji jest wystarczające dla małej ilości uaktualnień. Aby zainstalować kilka aktualizacji, użyj reguł, które możesz skonfigurować w zadaniu *Zainstaluj wymagane aktualizacje i napraw luki*. Zalecane jest ustawienie stanu *Zatwierdzone* tylko dla tych określonych aktualizacji, które nie spełniają kryteriów określonych w regułach. Jeśli ręcznie zatwierdzisz dużą liczbę aktualizacji, wydajność Serwera administracyjnego ulegnie zmniejszeniu i może doprowadzić do przeciążenia Serwera administracyjnego.

Domyślnie pobrane aktualizacje oprogramowania posiadają stan *Niezdefiniowane*. Możesz zmienić stan na *Zatwierdzono* lub *Odrzucono* na liście **Aktualizacje oprogramowania** list (**Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**).

Dostępne instrukcje:

- Konsola administracyjna: Zatwierdzanie i odrzucanie aktualizacji oprogramowania
- Kaspersky Security Center Web Console: Zatwierdzanie i odrzucanie aktualizacji oprogramowania innych firm

6. **Konfigurowanie Serwera administracyjnego do pracy jako serwer Windows Server Update Services (WSUS) (opcjonalne)**

   Domyślnie, aktualizacje Windows Update są pobierane na zarządzane urządzenia z serwerów Microsoft. Możesz zmienić to ustawienie, żeby używać Serwera administracyjnego jako serwera WSUS. W tym przypadku Serwer administracyjny synchronizuje dane aktualizacji z Windows Update w określonej częstotliwości i dostarcza aktualizacje w trybie scentralizowanym do Windows Update na urządzeniach w sieci.

   Aby użyć Serwera administracyjnego jako serwera WSUS, utwórz zadanie Wykonaj synchronizację Windows Update i zaznacz pole **Użyj Serwera administracyjnego jako serwera WSUS** w zasadzie Agenta sieciowego.

   Dostępne instrukcje:

   - Konsola administracyjna: Synchronizowanie aktualizacji z Windows Update z Serwerem administracyjnym, Konfigurowanie aktualizacji systemu Windows w zasadzie Agenta sieciowego
   - Kaspersky Security Center Web Console: Tworzenie zadania synchronizacji Windows Update

7. **Uruchamianie zadania instalacji aktualizacji**

   Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Zainstaluj aktualizacje Windows Update*. Jeśli uruchamiasz te zadania, aktualizacje są pobierane i instalowane na zarządzanych urządzeniach. Po zakończeniu zadania, upewnij się, że na liście zadań posiada stan *Zakończone pomyślnie*.

8. **Utwórz raport dotyczący wyników instalacji aktualizacji oprogramowania firm trzecich (opcjonalne)**

   Aby wyświetlić szczegółowe statystyki dotyczące instalacji aktualizacji, utwórz **Raport z wynikami instalacji aktualizacji oprogramowania firm trzecich**.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie i przeglądanie raportu
   - Kaspersky Security Center Web Console: Tworzenie i przeglądanie raportu

Wyniki

Jeśli utworzyłeś i skonfigurowałeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, aktualizacje są automatycznie instalowane na zarządzanych urządzeniach. Jeśli nowe aktualizacje zostaną pobrane do repozytorium Serwera administracyjnego, Kaspersky Security Center sprawdzi, czy spełniają kryteria określone w regułach aktualizacji. Wszystkie nowe aktualizacje, które spełniają kryteria, zostaną zainstalowane automatycznie przy kolejnym uruchomieniu zadania.

Jeśli utworzyłeś zadanie *Zainstaluj aktualizacje Windows Update*, instalowane są tylko te aktualizacje określone we właściwościach zadania *Zainstaluj aktualizacje Windows Update*. W przyszłości, jeśli będziesz chciał zainstalować nowe aktualizacje pobrane do repozytorium Serwera administracyjnego, będziesz musiał dodać wymagane aktualizacje do listy aktualizacji w istniejącym zadaniu lub utworzyć nowe zadanie *Zainstaluj aktualizacje Windows Update*.

Instalowanie aktualizacji oprogramowania firm trzecich

Możesz zainstalować aktualizacje oprogramowania firm trzecich na zarządzanych urządzeniach poprzez stworzenie i uruchomienie jednego z następujących zadań:

- *Zainstaluj wymagane aktualizacje i napraw luki*

  Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami. Możesz użyć tego zadania, aby zainstalować aktualizacje Windows Update dostarczone przez Microsoft oraz aktualizacje dla oprogramowania innych producentów.

- *Zainstaluj aktualizacje Windows*

  Możesz użyć zadania *Zainstaluj aktualizacje Windows* tylko do zainstalowania aktualizacji Windows Update.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Opcjonalnie możesz utworzyć zadanie instalacji wymaganych aktualizacji w następujący sposób:

- Otwierając listę aktualizacji i określając aktualizacje do zainstalowania.

  W rezultacie tworzone jest nowe zadanie instalacji wybranych aktualizacji. Istnieje możliwość dodania wybranych aktualizacji do istniejącego zadania.

- Uruchamiając kreator instalacji aktualizacji.

  kreator instalacji aktualizacji jest dostępny tylko dla licencji Zarządzanie lukami i poprawkami.

  Kreator upraszcza tworzenie i konfigurację zadania instalacji aktualizacji i pozwala wyeliminować tworzenie zbędnych zadań zawierających te same aktualizacje do zainstalowania.

Instalowanie aktualizacji oprogramowania innych firm przy użyciu listy aktualizacji

W celu zainstalowania aktualizacji oprogramowania firm trzecich, korzystając z listy aktualizacji:

1. Otwórz jedną z list aktualizacji:

   - Aby otworzyć ogólną listę aktualizacji, przejdź do **Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.

   - Aby otworzyć listę aktualizacji dla zarządzanego urządzenia, przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia** → <device name> → **Zaawansowane** → **Dostępne aktualizacje**.

   - Aby otworzyć listę aktualizacji dla określonej aplikacji, przejdź do **Operacje** → **Aplikacje innych firm** → **Rejestr aplikacji** → <application name> → **Dostępne aktualizacje**.

   Zostanie wyświetlona lista dostępnych aktualizacji.

2. Zaznacz pola obok aktualizacji, które chcesz zainstalować.

3. Kliknij przycisk **Zainstaluj aktualizacje**.

   Aby zainstalować niektóre aktualizacje oprogramowania, należy zaakceptować Umowę licencyjną użytkownika końcowego. Jeśli odrzucisz Umowę licencyjną użytkownika końcowego, aktualizacja oprogramowania nie zostanie zainstalowana.

4. Wybierz jedną z następujących opcji:

   - **Nowe zadanie**

     Zostanie uruchomiony Kreator tworzenia nowego zadania. Jeśli masz licencję Zarządzania lukami i poprawkami, domyślnie wybrany jest typ zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Jeśli nie masz licencji, wybrane jest zadanie *Zainstaluj aktualizacje Windows*. Aby zakończyć tworzenie zadania, postępuj zgodnie z instrukcjami kreatora.

   - **Zainstaluj aktualizację (dodaj regułę do określonego zadania)**

     Wybierz zadanie, do którego chcesz dodać wybrane aktualizacje. Jeśli masz licencję Zarządzania lukami i poprawkami, wybierz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*. Nowa reguła instalacji wybranych aktualizacji zostanie automatycznie dodana do wybranego zadania. Jeśli nie masz licencji, wybierz zadanie *Zainstaluj aktualizacje Windows*. Wybrane aktualizacje zostaną dodane do właściwości zadania.

     Zostanie otwarte okno właściwości zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Jeśli wybrałeś utworzenie nowego zadania, zadanie zostanie utworzone i wyświetlone na liście zadań, w sekcji **Zasoby (urządzenia)** → **Zadania**. Jeśli wybrałeś dodanie aktualizacji do istniejącego zadania, aktualizacje zostaną zapisane we właściwościach zadania.

Aby zainstalować aktualizacje dla oprogramowania innych firm, uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Zainstaluj aktualizacje Windows*. Możesz uruchomić jakiekolwiek z tych zadań ręcznie lub określić ustawienia terminarza we właściwościach zadania, które uruchomiłeś. Podczas określania terminarza zadania upewnij się, że zadanie instalacji aktualizacji jest uruchamiane po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

Instalowanie aktualizacji oprogramowania innych firm za pomocą Kreator naprawiania luk

kreator instalacji aktualizacji jest dostępny tylko dla licencji Zarządzanie lukami i poprawkami.

W celu utworzenia zadania instalacji aktualizacji oprogramowania firm trzecich, korzystając z Kreator naprawiania luk:

1. W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.

   Zostanie wyświetlona lista dostępnych aktualizacji.

2. Zaznacz pole obok aktualizacji, którą chcesz zainstalować.

3. Kliknij przycisk **Uruchom Kreatora instalacji aktualizacji**.

Zostanie uruchomiony kreator instalacji aktualizacji. Strona **Wybierz zadanie instalacji aktualizacji** wyświetla listę wszystkich istniejących zadań następujących typów:

- *Zainstaluj wymagane aktualizacje i napraw luki*
- *Zainstaluj aktualizacje Windows*
- *Napraw luki*

Nie możesz zmodyfikować zadań ostatnich dwóch typów, aby zainstalować nowe aktualizacje. Aby zainstalować nowe aktualizacje, możesz użyć tylko zadania *Zainstaluj wymagane aktualizacje i napraw luki*.

4. Jeśli chcesz, aby kreator wyświetlał tylko te zadania, które instalują wybraną aktualizację, włącz opcję **Wyświetl tylko zadania instalujące tę aktualizację**.

5. Wybierz, co chcesz zrobić:

   - Aby rozpocząć zadanie, zaznacz pole wyboru obok nazwy zadania, a następnie kliknij przycisk **Uruchom**.
   - Aby dodać nową regułę do istniejącego zadania:

     a. Zaznacz pole obok nazwy zadania i kliknij przycisk **Dodaj regułę**.

     b. Na wyświetlonej stronie skonfiguruj nową regułę:

     - **Reguła instalacji dla aktualizacji tej istotności**

       Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

       Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

       Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

       Domyślnie opcja ta jest wyłączona.

     - **Reguła instalacji aktualizacji tej istotności zgodnie z MSRC**

       Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

       Jeśli ta opcja jest włączona (dostępna tylko dla aktualizacji systemu Windows Update), aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

       Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

       Domyślnie opcja ta jest wyłączona.

     - **Reguła instalacji dla aktualizacji tego dostawcy**

       Ta opcja jest dostępna tylko dla aktualizacji aplikacji innych firm. Kaspersky Security Center instaluje tylko te aktualizacje, które odnoszą się do aplikacji stworzonych przez tego samego dostawcę co wybrana aktualizacja. Odrzucone aktualizacje i aktualizacje aplikacji stworzone przez innych dostawców nie są instalowane.

       Domyślnie opcja ta jest wyłączona.

- **Reguła instalacji dla aktualizacji typu**
- **Reguła instalacji dla wybranej aktualizacji**
- **Zatwierdź wybrane aktualizacje**

  Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

  Domyślnie opcja ta jest wyłączona.

- **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

  Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

  Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

  Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

  Domyślnie opcja ta jest włączona.

c. Kliknij przycisk **Dodaj**.

- W celu utworzenia zadania:

  a. Kliknij przycisk **Nowe zadanie**.

  b. Na wyświetlonej stronie skonfiguruj nową regułę:

  - **Reguła instalacji dla aktualizacji tej istotności**

    Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

    Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

    Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

    Domyślnie opcja ta jest wyłączona.

  - **Reguła instalacji aktualizacji tej istotności zgodnie z MSRC**

    Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

    Jeśli ta opcja jest włączona (dostępna tylko dla aktualizacji systemu Windows Update), aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

    Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

Domyślnie opcja ta jest wyłączona.

- **Reguła instalacji dla aktualizacji tego dostawcy**

  Ta opcja jest dostępna tylko dla aktualizacji aplikacji innych firm. Kaspersky Security Center instaluje tylko te aktualizacje, które odnoszą się do aplikacji stworzonych przez tego samego dostawcę co wybrana aktualizacja. Odrzucone aktualizacje i aktualizacje aplikacji stworzone przez innych dostawców nie są instalowane.

  Domyślnie opcja ta jest wyłączona.

- **Reguła instalacji dla aktualizacji typu**

- **Reguła instalacji dla wybranej aktualizacji**

- **Zatwierdź wybrane aktualizacje**

  Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

  Domyślnie opcja ta jest wyłączona.

- **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

  Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

  Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

  Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

  Domyślnie opcja ta jest włączona.

c. Kliknij przycisk **Dodaj**.

Jeśli wybrano rozpoczęcie zadania, możesz zamknąć kreatora. Zadanie zakończy się w tle. Dalsze działania nie są wymagane.

Jeśli wybrałeś dodanie reguły do istniejącego zadania, zostanie otwarte okno właściwości zadania. Nowa reguła została już dodana do właściwości zadania. Możesz przejrzeć lub zmodyfikować regułę lub ustawienia innego zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Jeśli chcesz utworzyć zadanie, kontynuuj tworzenie zadania w kreatorze tworzenia nowego zadania. Nowa reguła dodana w kreatorze instalacji aktualizacji zostanie wyświetlona w kreatorze tworzenia nowego zadania. Po zakończeniu pracy kreatora, do listy zadań zostanie dodane zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.

Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji

Za pośrednictwem zadania Wyszukiwanie luk i wymaganych aktualizacji program Kaspersky Security Center otrzymuje listy wykrytych luk i wymaganych aktualizacji dla oprogramowania firm trzecich, zainstalowanego na zarządzanych urządzeniach.

Zadanie Wyszukiwanie luk i wymaganych aktualizacji jest tworzone automatycznie po uruchomieniu kreatora wstępnej konfiguracji. Jeśli nie uruchamiałeś kreatora, możesz utworzyć zadanie ręcznie.

W celu utworzenia zadania Wyszukiwanie luk i wymaganych aktualizacji:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Wyszukiwanie luk i wymaganych aktualizacji**.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.
6. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
7. Kliknij przycisk **Utwórz**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.
8. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.
9. W oknie właściwości zadania określ ogólne ustawienia zadania.
10. Na zakładce **Ustawienia aplikacji** określ następujące ustawienia:

    - **Wyszukaj luki i aktualizacje wymienione przez firmę Microsoft**

      Podczas wyszukiwania luk i aktualizacji program Kaspersky Security Center używa informacji o stosowanych aktualizacjach firmy Microsoft ze źródła uaktualnień Microsoft, które są dostępne w danym momencie.

      Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft i aktualizacji aplikacji innych firm.

      Domyślnie opcja ta jest włączona.

      Informacje o opcjonalnych aktualizacjach Microsoft Windows nie są wysyłane do Serwera administracyjnego.

- **Połącz z serwerem aktualizacji, aby zaktualizować dane**

  Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem uaktualnień Microsoft. Następujące serwery mogą pełnić rolę źródeł aktualizacji Microsoft:

  - Serwer administracyjny Kaspersky Security Center (zapoznaj się z ustawieniami zasady Agenta sieciowego)
  - System Windows Server wdrożony w sieci Twojej organizacji wraz z programem Microsoft Windows Server Update Services (WSUS)
  - Serwery aktualizacji Microsoft

  Jeśli ta opcja jest włączona, agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem aktualizacji firmy Microsoft, aby odświeżyć informacje o stosowanych aktualizacjach Microsoft Windows.

  Jeśli ta opcja jest wyłączona, agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła aktualizacji firmy Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia.

  Nawiązywanie połączenia ze źródłem aktualizacji firmy Microsoft może zużywać dużo zasobów. Możesz chcieć wyłączyć tę opcję, jeśli ustawisz regularne nawiązywanie połączenia z tym źródłem uaktualnień w innym zadaniu lub we właściwościach zasady Agenta sieciowego, w sekcji **Aktualizacje oprogramowania i luki**. Jeśli nie chcesz wyłączyć tej opcji, następnie, aby zmniejszyć obciążenie Serwera, możesz skonfigurować terminarz zadania do losowego opóźnienia uruchomienia zadania w ciągu 360 minut.

  Domyślnie opcja ta jest włączona.

  Kombinacja następujących opcji ustawień zasady Agenta sieciowego definiuje tryb uzyskiwania aktualizacji:

  - Agent usługi Windows Update na zarządzanym urządzeniu łączy się z serwerem aktualizacji w celu pobierania aktualizacji tylko wtedy, gdy opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest włączona we właściwościach zadania *Wyszukiwanie luk i wymaganych aktualizacji*, a opcja **Tryb wyszukiwania aktualizacji systemu Windows** jest ustawiona na **Aktywny** w ustawieniach zasady Agenta sieciowego.
  - Jeśli nie potrzebujesz, aby Agent sieciowy nawiązał połączenie ze źródłem aktualizacji systemu Microsoft Windows i pobrał aktualizacje podczas wykonywania zadania *skanowania w poszukiwaniu luk*, możesz ustawić opcję **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, a opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** musi pozostać włączona. Dzięki temu możesz zaoszczędzić zasoby i wykorzystać wcześniej pobrane aktualizacje systemu Windows do skanowania w poszukiwaniu luk w zabezpieczeniach. Możesz użyć trybu pasywnego, jeśli skonfigurujesz otrzymywanie aktualizacji systemu Microsoft Windows w inny sposób. Jeśli odbieranie aktualizacji systemu Microsoft Windows nie zostało skonfigurowane w inny sposób, nie należy ustawiać opcji **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, ponieważ w takim przypadku informacje o aktualizacjach nigdy nie zostaną odebrane.
  - Bez względu na stan opcji **Połącz z serwerem aktualizacji, aby zaktualizować dane** (włączona lub wyłączona), jeśli opcja **Tryb wyszukiwania aktualizacji systemu Windows** zostanie ustawiona jako **Wyłączony**, Kaspersky Security Center nie żąda żadnych informacji o aktualizacjach.

- **Wyszukaj luki i aktualizacje innych firm wymienione przez firmę Kaspersky**

  Jeśli ta opcja jest włączona, Kaspersky Security Center wyszukuje luki i wymagane aktualizacje dla aplikacji firm trzecich (aplikacji producentów innych niż Kaspersky i Microsoft) w rejestrze systemu Windows i w folderach określonych pod **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**. Pełna lista obsługiwanych aplikacji firm trzecich jest zarządzana przez Kaspersky.

  Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie szuka luk i wymaganych uaktualnień dla aplikacji firm trzecich. Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft Windows i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

- **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**

  Foldery, w których Kaspersky Security Center wyszukuje aplikacje firm trzecich, które wymagają naprawienia luk i zainstalowania aktualizacji. Możesz użyć zmiennych systemowych.

  Określ foldery, w których zostaną zainstalowane aplikacje. Domyślnie, lista zawiera foldery systemowe, w których instalowana jest większość aplikacji.

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy zapisywanie plików śledzenia jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

11. Kliknij przycisk **Zapisz**.

Zadanie zostało utworzone i skonfigurowane.

Jeśli wyniki zadania zawierają ostrzeżenie o błędzie 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", możesz rozwiązać ten problem poprzez Rejestr systemu Windows.

Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie po uruchomieniu kreatora wstępnej konfiguracji. Jeśli nie uruchamiałeś kreatora, możesz utworzyć zadanie ręcznie.

Oprócz ogólnych ustawień zadania możesz określić następujące ustawienia podczas tworzenia zadania *Wyszukiwanie luk i wymaganych aktualizacji* lub później, podczas konfigurowania właściwości utworzonego zadania:

- **Wyszukaj luki i aktualizacje wymienione przez firmę Microsoft**

  Podczas wyszukiwania luk i aktualizacji program Kaspersky Security Center używa informacji o stosowanych aktualizacjach firmy Microsoft ze źródła uaktualnień Microsoft, które są dostępne w danym momencie.

  Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

  Informacje o opcjonalnych aktualizacjach Microsoft Windows nie są wysyłane do Serwera administracyjnego.

- **Połącz z serwerem aktualizacji, aby zaktualizować dane**

  Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem uaktualnień Microsoft. Następujące serwery mogą pełnić rolę źródeł aktualizacji Microsoft:

  - Serwer administracyjny Kaspersky Security Center (zapoznaj się z ustawieniami zasady Agenta sieciowego)
  - System Windows Server wdrożony w sieci Twojej organizacji wraz z programem Microsoft Windows Server Update Services (WSUS)
  - Serwery aktualizacji Microsoft

  Jeśli ta opcja jest włączona, agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem aktualizacji firmy Microsoft, aby odświeżyć informacje o stosowanych aktualizacjach Microsoft Windows.

  Jeśli ta opcja jest wyłączona, agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła aktualizacji firmy Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia.

  Nawiązywanie połączenia ze źródłem aktualizacji firmy Microsoft może zużywać dużo zasobów. Możesz chcieć wyłączyć tę opcję, jeśli ustawisz regularne nawiązywanie połączenia z tym źródłem uaktualnień w innym zadaniu lub we właściwościach zasady Agenta sieciowego, w sekcji **Aktualizacje oprogramowania i luki**. Jeśli nie chcesz wyłączyć tej opcji, następnie, aby zmniejszyć obciążenie Serwera, możesz skonfigurować terminarz zadania do losowego opóźnienia uruchomienia zadania w ciągu 360 minut.

  Domyślnie opcja ta jest włączona.

Kombinacja następujących opcji ustawień zasady Agenta sieciowego definiuje tryb uzyskiwania aktualizacji:

- Agent usługi Windows Update na zarządzanym urządzeniu łączy się z serwerem aktualizacji w celu pobierania aktualizacji tylko wtedy, gdy opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest włączona we właściwościach zadania *Wyszukiwanie luk i wymaganych aktualizacji*, a opcja **Tryb wyszukiwania aktualizacji systemu Windows** jest ustawiona na **Aktywny** w ustawieniach zasady Agenta sieciowego.

- Jeśli nie potrzebujesz, aby Agent sieciowy nawiązał połączenie ze źródłem aktualizacji systemu Microsoft Windows i pobrał aktualizacje podczas wykonywania zadania *skanowania w poszukiwaniu luk*, możesz ustawić opcję **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, a opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** musi pozostać włączona. Dzięki temu możesz zaoszczędzić zasoby i wykorzystać wcześniej pobrane aktualizacje systemu Windows do skanowania w poszukiwaniu luk w zabezpieczeniach. Możesz użyć trybu pasywnego, jeśli skonfigurujesz otrzymywanie aktualizacji systemu Microsoft Windows w inny sposób. Jeśli odbieranie aktualizacji systemu Microsoft Windows nie zostało skonfigurowane w inny sposób, nie należy ustawiać opcji **Tryb wyszukiwania aktualizacji systemu Windows** na **Pasywny**, ponieważ w takim przypadku informacje o aktualizacjach nigdy nie zostaną odebrane.

- Bez względu na stan opcji **Połącz z serwerem aktualizacji, aby zaktualizować dane** (włączona lub wyłączona), jeśli opcja **Tryb wyszukiwania aktualizacji systemu Windows** zostanie ustawiona jako **Wyłączony**, Kaspersky Security Center nie żąda żadnych informacji o aktualizacjach.

- **Wyszukaj luki i aktualizacje innych firm wymienione przez firmę Kaspersky**

  Jeśli ta opcja jest włączona, Kaspersky Security Center wyszukuje luki i wymagane aktualizacje dla aplikacji firm trzecich (aplikacji producentów innych niż Kaspersky i Microsoft) w rejestrze systemu Windows i w folderach określonych pod **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**. Pełna lista obsługiwanych aplikacji firm trzecich jest zarządzana przez Kaspersky.

  Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie szuka luk i wymaganych uaktualnień dla aplikacji firm trzecich. Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft Windows i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

- **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**

  Foldery, w których Kaspersky Security Center wyszukuje aplikacje firm trzecich, które wymagają naprawienia luk i zainstalowania aktualizacji. Możesz użyć zmiennych systemowych.

  Określ foldery, w których zostaną zainstalowane aplikacje. Domyślnie, lista zawiera foldery systemowe, w których instalowana jest większość aplikacji.

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy zapisywanie plików śledzenia jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

Zalecenia dotyczące terminarza zadania

Podczas tworzenia terminarza zadania *Wyszukiwanie luk i wymaganych aktualizacji* upewnij się, że włączone są dwie opcje: **Uruchom pominięte zadania** oraz **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Domyślnie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest ustawione na uruchamianie ręczne. Jeśli zasady obowiązujące w organizacji nakazują wyłączenie wszystkich urządzeń w tym czasie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* zostanie uruchomione, gdy urządzenia znowu zostaną włączone, czyli następnego dnia rano. Takie działanie nie jest wskazane, ponieważ wykrywanie luk może zwiększać zużycie procesora i obciążenie podsystemów dysku. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do aktualizacji i naprawy luk w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft, zainstalowanym na zarządzanych urządzeniach. To zadanie umożliwia zainstalowanie kilku aktualizacji i naprawę kilku luk zgodnie z pewnymi regułami.

W celu zainstalowania aktualizacji lub wyeliminowania luk za pomocą zadania *Zainstaluj wymagane aktualizacje i napraw luki*, możesz wykonać jedną z następujących czynności:

- Uruchom kreator instalacji aktualizacji lub Kreator naprawiania luk.
- Utwórz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.
- Dodaj regułę instalacji aktualizacji do istniejącego pliku *Zainstaluj wymagane aktualizacje i napraw luki* zadanie.

Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Zainstaluj wymagane aktualizacje i napraw luki**.

   Jeśli zadanie nie jest wyświetlane, sprawdź, czy Twoje konto ma uprawnienia **Odczyt**, **Modyfikuj** i **Wykonaj** dla obszaru funkcjonalnego **Zarządzanie systemem: Zarządzanie lukami w zabezpieczeniach i poprawkami**. Bez tych praw dostępu nie można utworzyć ani skonfigurować zadania *Zainstaluj wymagane aktualizacje i napraw luki*.

4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

5. Wybierz urządzenia, do których zadanie zostanie przypisane.

6. Określ zasady instalacji aktualizacji, a następnie określ następujące ustawienia:

   - **Uruchom instalację podczas ponownego uruchamiania lub wyłączania urządzenia**

     Jeśli ta opcja jest włączona, aktualizacje są instalowane po ponownym uruchomieniu lub zamknięciu urządzenia. W innym przypadku aktualizacje są instalowane zgodnie z terminarzem.

     Użyj tej opcji, jeśli instalowanie aktualizacji może wpłynąć na działanie urządzenia.

     Domyślnie opcja ta jest wyłączona.

   - **Zainstaluj wymagane ogólne składniki systemu**

     Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

     Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

     Domyślnie opcja ta jest wyłączona.

   - **Zezwól na instalację nowych wersji aplikacji podczas aktualizacji**

     Jeśli ta opcja jest włączona, aktualizacje są dozwolone, gdy powodują zainstalowanie nowej wersji aplikacji.

     Jeśli ta opcja jest wyłączona, aplikacja nie zostanie zaktualizowana. W takiej sytuacji możesz ręcznie zainstalować nowe wersje aplikacji lub użyć w tym celu innego zadania. Na przykład, możesz użyć tej opcji, jeśli struktura Twojej firmy nie jest obsługiwana przez nową wersję aplikacji lub jeśli chcesz sprawdzić aktualizację w infrastrukturze testowej.

     Domyślnie opcja ta jest włączona.

     > Aktualizowanie aplikacji może spowodować problemy z działaniem powiązanych aplikacji zainstalowanych na urządzeniach klienckich.

   - **Pobierz aktualizacje na urządzenie, ale ich nie instaluj**

     Jeśli ta opcja jest włączona, aplikacja pobierze uaktualnienia na urządzenie, ale nie zainstaluje ich automatycznie. Możesz ręcznie zainstalować pobrane aktualizacje.

     Aktualizacje Microsoft są pobierane do folderu systemowego Windows. Aktualizacje aplikacji firm trzecich (aplikacje innych producentów niż Kaspersky i Microsoft) są pobierane do folderu określonego w polu **Pobierz uaktualnienia do**.

     Jeśli ta opcja jest wyłączona, aktualizacje są instalowane na urządzeniu automatycznie.

     Domyślnie opcja ta jest wyłączona.

   - **Pobierz uaktualnienia do**

     Ten folder jest używany do pobierania aktualizacji aplikacji innych firm (aplikacji innych producentów niż Kaspersky i Microsoft).

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy zapisywanie plików śledzenia jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

7. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

  Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

  Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Czas oczekiwania przed wymuszeniem zamknięcia aplikacji dla zablokowanych sesji (min)**

  Wymuszone zamknięcie aplikacji ma miejsce, gdy urządzenie użytkownika jest zablokowane (automatycznie po określonym czasie nieaktywności lub ręcznie).

  Jeśli ta opcja jest włączona, wymuszone zamknięcie aplikacji na zablokowanym urządzeniu odbywa się po minięciu czasu określonego w polu wejściowym.

  Jeśli ta opcja jest wyłączona, aplikacje nie będą zamykane na zablokowanym urządzeniu.

  Domyślnie opcja ta jest wyłączona.

8. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

9. Kliknij przycisk **Zakończ**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

10. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

11. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.

12. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

Jeśli wyniki zadania zawierają ostrzeżenie o błędzie 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", możesz rozwiązać ten problem poprzez Rejestr systemu Windows.

Dodawanie reguł dla instalacji aktualizacji

Ta funkcja jest dostępna tylko w ramach licencji na Zarządzanie lukami i poprawkami.

Podczas instalowania aktualizacji oprogramowania lub naprawiania luk w oprogramowaniu przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki* należy określić zasady instalacji aktualizacji. Te reguły określają aktualizacje do zainstalowania oraz luki do wyeliminowania.

Dokładne ustawienia zależą od tego, czy dodajesz regułę dla wszystkich aktualizacji Windows Update lub aktualizacji aplikacji firm trzecich (aplikacje stworzone przez producentów oprogramowania innych niż Kaspersky i Microsoft) lub wszystkich aplikacji. Podczas dodawania reguły dla aktualizacji Windows Update lub aktualizacji aplikacji firm trzecich możesz wybrać określone aplikacje oraz wersje aplikacji, dla których chcesz zainstalować uaktualnienia. Podczas dodawani reguły dla wszystkich aktualizacji możesz wybrać określone uaktualnienia, które chcesz zainstalować, oraz luki, które chcesz wyeliminować poprzez zainstalowanie uaktualnień.

Regułę instalacji aktualizacji można dodać w następujący sposób:

- Dodając regułę podczas tworzenia nowego zadania Zainstaluj wymagane aktualizacje i napraw luki.
- Dodając regułę w zakładce **Ustawienia aplikacji** w oknie właściwości istniejącego zadania *Zainstaluj wymagane aktualizacje i napraw luki*.
- Za pomocą kreatora instalacji aktualizacji lub kreatora naprawiania luk.

W celu dodania nowej reguły dla wszystkich aktualizacji:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla wszystkich aktualizacji**.

3. W kroku **Kryteria ogólne** użyj list rozwijalnych do określenia następujących ustawień:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aktualizacje** wybierz aktualizacje, które mają zostać zainstalowane:

   - **Zainstaluj wszystkie pasujące aktualizacje**

     Zainstaluj aktualizacje oprogramowania, które spełniają kryteria określone w kroku **Kryteria ogólne**. Ta opcja jest wybrana domyślnie.

   - **Zainstaluj tylko aktualizacje z listy**

     Instalowane są tylko te aktualizacje oprogramowania, które wybierzesz ręcznie z listy. Ta lista zawiera wszystkie dostępne aktualizacje oprogramowania.

Na przykład, możesz wybrać określone aktualizacje w następujących przypadkach: aby sprawdzić ich instalację w środowisku testowym, aby zaktualizować tylko krytyczne aplikacje lub aby zaktualizować tylko określone aplikacje.

- **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

  Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

  Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

  Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

  Domyślnie opcja ta jest włączona.

5. W kroku **Luki** wybierz luki, które zostaną wyeliminowane poprzez zainstalowanie wybranych aktualizacji:

   - **Napraw wszystkie luki spełniające inne kryteria**

     Wyeliminuj wszystkie luki, które spełniają kryteria określone na stronie **Kryteria ogólne** kreatora. Ta opcja jest wybrana domyślnie.

   - **Napraw tylko luki z listy**

     Naprawione zostaną tylko te luki, które ręcznie wybierzesz z listy. Ta lista zawiera wszystkie wykryte luki.

     Na przykład, możesz wybrać określone luki w następujących przypadkach: aby sprawdzić ich eliminację w środowisku testowym, aby wyeliminować luki tylko w krytycznych aplikacjach lub aby wyeliminować luki tylko w określonych aplikacjach.

6. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

W celu dodania nowej reguły dla aktualizacji Windows Update:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji systemu Windows**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

   - **Napraw luki z priorytetem MSRC równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Kategorie aktualizacji** wybierz kategorie aktualizacji, które mają zostać zainstalowane. Te kategorie są takie same, jak w Microsoft Update Catalog. Domyślnie, zaznaczone są wszystkie kategorie.

6. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

W celu dodania nowej reguły dla aktualizacji aplikacji firm trzecich:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji firm trzecich**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.

     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.

     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji Ustawienia okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

Tworzenie zadania Zainstaluj aktualizacje Windows Update

Zadanie *Zainstaluj aktualizacje Windows* umożliwia zainstalowanie aktualizacji oprogramowania, dostarczonych przez usługę Windows Update na zarządzane urządzenia.

Jeśli nie masz licencji Zarządzania lukami i poprawkami, nie możesz tworzyć nowych zadań typu *Zainstaluj aktualizacje Windows*. Aby zainstalować nowe aktualizacje, możesz dodać je do istniejącego zadania *Zainstaluj aktualizacje Windows*. Zalecamy użycie zadania *Zainstaluj wymagane aktualizacje i napraw luki* zamiast zadania *Zainstaluj aktualizacje Windows*. Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* umożliwia automatyczne instalowanie wielu aktualizacji i naprawianie wielu luk w zabezpieczeniach, zgodnie z określonymi przez Ciebie regułami. Ponadto to zadanie umożliwia instalowanie aktualizacji od dostawców oprogramowania innych niż Microsoft.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

W celu utworzenia zadania Zainstaluj aktualizacje Windows Update:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Zainstaluj aktualizacje Windows**.
4. Określ nazwę tworzonego zadania.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.
6. Kliknij przycisk **Dodaj**.

   Zostanie otwarta lista aktualizacji.
7. Wybierz aktualizacje Windows Update, które chcesz zainstalować, a następnie kliknij **OK**.
8. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

   - **Nie uruchamiaj ponownie urządzenia**

     Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

   - **Uruchom urządzenie ponownie**

     Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

  Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

  Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

9. Określ ustawienia konta:

- **Konto domyślne**

  Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

  Domyślnie opcja ta jest zaznaczona.

- **Określ konto**

  Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

- **Konto**

  Konto, z poziomu którego zadanie jest uruchamiane.

- **Hasło**

  Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

10. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

11. Kliknij przycisk **Zakończ**.

    Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

12. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

13. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.

14. Kliknij przycisk **Zapisz**.

Zadanie zostało utworzone i skonfigurowane.

Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich

Możesz przejrzeć listę dostępnych aktualizacji dla oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft, zainstalowanego na urządzeniach klienckich.

W celu przejrzenia listy aktualizacji dostępnych dla aplikacji firm trzecich, zainstalowanych na urządzeniach klienckich:

W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.

Zostanie wyświetlona lista dostępnych aktualizacji.

Możesz określić filtr przeglądania listy aktualizacji oprogramowania. Kliknij ikonę **Filtr** () w prawym górnym rogu listy aktualizacji oprogramowania do zarządzania filtrem. Możesz także wybrać jeden z predefiniowanych filtrów z listy rozwijalnej **Wstępnie ustawione filtry** nad listą luk w oprogramowaniu.

W celu przejrzenia właściwości aktualizacji:

1. Kliknij nazwę żądanej aktualizacji oprogramowania.

2. Zostanie otwarte okno właściwości aktualizacji, wyświetlające informacje pogrupowane na następujących zakładkach:

   - **Ogólne**

     Ta zakładka wyświetla ogólne szczegóły wybranej aktualizacji:

     - Stan zatwierdzenia aktualizacji (można zmienić ręcznie, wybierają nowy stan na liście rozwijalnej)
     - Kategoria Windows Server Update Services (WSUS), do której należy aktualizacja
     - Data i godzina zarejestrowania aktualizacji

- Data i godzina utworzenia aktualizacji
- Istotność aktualizacji
- Wymagania instalacyjne: nałożone przez aktualizację
- Rodzina aplikacji, do której należy aktualizacja
- Aplikacja, do której stosowana jest aktualizacja
- Liczba rewizji aktualizacji

- **Atrybuty**

  Ta zakładka wyświetla zestaw atrybutów, których możesz użyć do uzyskania większej ilości informacji na temat wybranej aktualizacji. Ten zestaw różni się w zależności od tego, czy aktualizacja jest publikowana przez firmę Microsoft lub innego producenta.

  Zakładka wyświetla następujące informacje dla aktualizacji firmy Microsoft:

  - Poziom ważności aktualizacji zgodny z Microsoft Security Response Center (MSRC)
  - Odnośnik do artykułu w Bazie wiedzy Microsoft Knowledge Base opisujący aktualizację
  - Odnośnik do artykułu w biuletynie Microsoft Security Bulletin opisujący aktualizację
  - Identyfikator aktualizacji (ID)

  Zakładka wyświetla następujące informacje dla aktualizacji innej firmy:

  - Czy aktualizacja jest poprawką lub pełnym pakietem dystrybucyjnym
  - Język lokalizacji aktualizacji
  - Czy aktualizacja jest instalowana automatycznie lub ręcznie
  - Czy aktualizacja została wycofana po zastosowaniu
  - Odnośnik do pobrania aktualizacji

- **Urządzenia**

  Ta zakładka wyświetla listę urządzeń, na których zainstalowano wybraną aktualizację.

- **Naprawione luki**

  Ta zakładka wyświetla listę luk, które mogą zostać usunięte przez wybraną aktualizację.

- **Podział aktualizacji**

  Ta zakładka wyświetla możliwe podziały między różnymi aktualizacjami opublikowanymi dla tej samej aplikacji, czyli czy wybrana aktualizacja może zastąpić inne aktualizacje lub czy mogą zostać zastąpione przez inne aktualizacje (dostępne tylko dla aktualizacji Microsoft).

- **Zadania instalacji tej aktualizacji**

  Ta zakładka wyświetla listę zadań, których obszar obejmuje instalację wybranej aktualizacji. Zakładka umożliwia także utworzenie nowego zadania zdalnej instalacji dla aktualizacji.

W celu przejrzenia statystyk dotyczących instalacji aktualizacji:

1. Zaznacz pole obok żądanej aktualizacji oprogramowania.

2. Kliknij przycisk **Statystyki stanów instalacji aktualizacji**.

Zostanie wyświetlony wykres stanów instalacji aktualizacji. Kliknięcie stanu spowoduje otwarcie listy urządzeń, na których aktualizacja posiada wybrany stan.

Możesz przejrzeć informacje o dostępnych aktualizacjach oprogramowania dla programów firm trzecich, w tym programów firmy Microsoft, zainstalowanych na wybranym zarządzanym urządzeniu działającym pod kontrolą systemu Windows.

W celu przejrzenia listy aktualizacji dostępnych dla oprogramowania firm trzecich, zainstalowanych na wybranych zarządzanych urządzeniach:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń kliknij odnośnik z nazwą urządzenia, dla którego chcesz przejrzeć aktualizacje oprogramowania firm trzecich.

   Zostanie wyświetlone okno właściwości wybranego urządzenia.

3. W oknie właściwości wybranego urządzenia wybierz zakładkę **Zaawansowane**.

4. W lewej części okna wybierz sekcję **Dostępne aktualizacje**. Jeśli chcesz przejrzeć tylko zainstalowane aktualizacje, włącz opcję **Pokaż zainstalowane aktualizacje**.

Zostanie wyświetlona lista aktualizacji oprogramowania firm trzecich, dostępnych dla wybranego urządzenia.

Eksportowanie listy dostępnych aktualizacji oprogramowania do pliku

Możesz wyeksportować aktualizacje dla oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft, które jest aktualnie wyświetlane, do plików CSV lub TXT. Możesz użyć tych plików, na przykład, do wysłania ich do swojego menedżera ds. bezpieczeństwa informacji lub przechowywać je w celach statystycznych.

W celu wyeksportowania do pliku tekstowego listy aktualizacji dostępnych dla oprogramowania firm trzecich, zainstalowanego na wszystkich zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.

   Strona wyświetla listę aktualizacji dostępnych dla oprogramowania firm trzecich, zainstalowanego na wszystkich zarządzanych urządzeniach.

2. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj do pliku TXT** lub przycisk **Eksportuj do pliku CSV**.

Plik zawierający listę aktualizacji dostępnych dla oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft, zostanie pobrany na urządzenie, którego aktualnie używasz.

W celu wyeksportowania do pliku tekstowego listy aktualizacji dostępnych dla oprogramowania firm trzecich, zainstalowanego na wybranym zarządzanym urządzeniu:

1. Otwórz listę aktualizacji dostępnych dla oprogramowania firm trzecich na wybranym, zarządzanym urządzeniu.
2. Wybierz aktualizacje oprogramowania, które chcesz wyeksportować.

   Pomiń ten krok, jeśli chcesz wyeksportować pełną listę aktualizacji oprogramowania.

   Jeśli chcesz wyeksportować pełną listę aktualizacji oprogramowania, zostaną wyeksportowane tylko aktualizacje wyświetlające bieżącą stronę.

   Jeśli chcesz wyeksportować tylko zainstalowane aktualizacje, zaznacz pole **Pokaż zainstalowane aktualizacje**.
3. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj do pliku TXT** lub przycisk **Eksportuj do pliku CSV**.

Plik zawierający listę aktualizacji dla oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft, zainstalowanego na wybranym, zarządzanym urządzeniu, jest pobierany na aktualnie używane urządzenie.

Zatwierdzanie oraz odrzucanie aktualizacji oprogramowania firm trzecich

Jeśli konfigurujesz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz utworzyć regułę, która wymaga określonego stanu aktualizacji, które zostaną zainstalowane. Na przykład, reguła aktualizacji może zezwolić na instalację następujących elementów:

- Tylko zatwierdzonych aktualizacji
- Tylko zatwierdzonych i niezdefiniowanych aktualizacji
- Wszystkich aktualizacji niezależnie od stanu aktualizacji

Możesz zatwierdzić uaktualnienia, które muszą zostać zainstalowane, oraz odrzucić uaktualnienia, które nie muszą zostać zainstalowane.

Używanie stanu *Zatwierdzone* do zarządzania instalacją aktualizacji jest wystarczające dla małej ilości uaktualnień. Aby zainstalować kilka aktualizacji, użyj reguł, które możesz skonfigurować w zadaniu *Zainstaluj wymagane aktualizacje i napraw luki*. Zalecane jest ustawienie stanu *Zatwierdzone* tylko dla tych określonych aktualizacji, które nie spełniają kryteriów określonych w regułach. Jeśli ręcznie zatwierdzisz dużą liczbę aktualizacji, wydajność Serwera administracyjnego ulegnie zmniejszeniu i może doprowadzić do przeciążenia Serwera administracyjnego.

W celu zatwierdzenia lub odrzucenia jednej lub kilku aktualizacji:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Aktualizacje oprogramowania**.

   Zostanie wyświetlona lista dostępnych aktualizacji.
2. Wybierz uaktualnienia, które chcesz zatwierdzić lub odrzucić.
3. Kliknij **Zatwierdź**, aby zatwierdzić wybrane aktualizacje, lub **Odrzuć**, aby odrzucić wybrane aktualizacje.

   Domyślna wartość to *Niezdefiniowane*.

Wybrane aktualizacje posiadają stany, które zdefiniowałeś.

Istnieje również możliwość zmiany stanu zatwierdzenia we właściwościach określonej aktualizacji.

W celu zatwierdzenia lub odrzucenia aktualizacji w jej właściwościach:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Aktualizacje oprogramowania**.

   Zostanie wyświetlona lista dostępnych aktualizacji.

2. Kliknij nazwę aktualizacji, którą chcesz zatwierdzić lub odrzucić.

   Zostanie otwarte okno właściwości aktualizacji.

3. W sekcji **Ogólne** wybierz stan dla aktualizacji, zmieniając opcję **Stan zatwierdzenia aktualizacji**. Możesz wybrać stan *Zatwierdzono*, *Odrzucono* lub *Nie zdefiniowano*.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Wybrana aktualizacja posiada stan, który zdefiniowałeś.

Jeśli ustawisz stan **Odrzucono** dla aktualizacji oprogramowania firm trzecich, te aktualizacje nie zostaną zainstalowane na urządzeniach, dla których planowane było ich zainstalowanie, ale jeszcze nie zostały zainstalowane. Uaktualnienia pozostaną na urządzeniach, na których zostały już zainstalowane. Jeśli musisz je usunąć, możesz je usunąć ręcznie lokalnie.

Tworzenie zadania Wykonaj synchronizację Windows Update

Zadanie *Wykonaj synchronizację Windows Update* jest dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

Zadanie *Wykonaj synchronizację Windows Update* jest wymagane, jeśli chcesz używać serwera administracyjnego jako serwera WSUS. W tym przypadku serwer administracyjny pobiera aktualizacje Windows do bazy danych i dostarcza aktualizacje Windows Update na urządzeniach klienckich w trybie scentralizowanym za pośrednictwem Agentów sieciowych. Jeśli sieć nie wykorzystuje serwera WSUS, każde urządzenie klienckie pobiera aktualizacje Microsoft niezależnie z zewnętrznych serwerów.

Zadanie *Wykonaj synchronizację Windows Update* pobiera tylko metadane z serwerów Microsoft. Kaspersky Security Center pobiera aktualizacje po uruchomieniu zadania instalacji aktualizacji i tylko te aktualizacje, które wybrałeś do instalacji.

Podczas wykonywania zadania **Wykonaj synchronizację Windows Update** aplikacja pobiera listę bieżących aktualizacji z serwera aktualizacji Microsoft. Następnie, Kaspersky Security Center tworzy listę aktualizacji, które są przestarzałe. Przy kolejnym uruchomieniu zadania **Wyszukiwanie luk i wymaganych aktualizacji** program Kaspersky Security Center oznaczy wszystkie przestarzałe aktualizacje i ustawi dla nich czas usunięcia. Przy kolejnym uruchomieniu zadania **Wykonaj synchronizację Windows Update** wszystkie aktualizacje, które zostały oznaczone do usunięcia 30 dni wcześniej, zostaną usunięte. Kaspersky Security Center sprawdza także obecność przestarzałych aktualizacji, które zostały oznaczone do usunięcia ponad 180 dni temu, a następnie usuwa te starsze aktualizacje.

Jeśli zadanie **Wykonaj synchronizację Windows Update** zostanie zakończone, a przestarzałe aktualizacje zostaną usunięte, baza danych może wciąż posiadać kody skrótów odnoszące się do plików usuniętych aktualizacji, a także odpowiednie pliki w plikach %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (jeśli zostały pobrane wcześniej). Możesz uruchomić zadanie **Konserwacja Serwera administracyjnego**, aby usunąć te przestarzałe wpisy z bazy danych oraz odpowiednich plików.

W celu utworzenia zadania Wykonaj synchronizację Windows Update:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Wykonaj synchronizację Windows Update**.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Włącz opcję **Pobierz ekspresowe pliki instalacyjne** jeśli chcesz, aby pliki ekspresowej aktualizacji były pobierane podczas uruchamiania zadania.

   Jeśli Kaspersky Security Center synchronizuje aktualizacje z Microsoft Windows Update Servers, informacje o wszystkich plikach są zapisywane w bazie danych Serwera administracyjnego. Wszystkie pliki niezbędne dla aktualizacji zostają także pobrane na dysk podczas interakcji z Windows Update Agent. Kaspersky Security Center zapisuje informacje o plikach aktualizacji ekspresowej w bazie danych i pobiera je, gdy jest to konieczne. Pobranie plików aktualizacji ekspresowej prowadzi do zmniejszenia wolnego miejsca na dysku.

   Aby uniknąć zmniejszenia ilości wolnego miejsca na dysku oraz zmniejszyć ruch sieciowy, wyłącz opcję **Pobierz ekspresowe pliki instalacyjne**.
6. Wybierz aplikacje, dla których chcesz pobrać aktualizacje.

   Jeśli pole **Wszystkie aplikacje** jest zaznaczone, uaktualnienia będą pobierane dla wszystkich istniejących aplikacji, a także dla wszystkich aplikacji, które mogą zostać wydane w przyszłości.
7. Wybierz kategorie aktualizacji, które chcesz pobrać na serwer administracyjny.

   Jeśli pole **Wszystkie kategorie** jest zaznaczone, uaktualnienia będą pobierane dla wszystkich istniejących kategorii uaktualnień, a także dla wszystkich kategorii, które mogą pojawić się w przyszłości.
8. Wybierz języki lokalizacji aktualizacji, które chcesz pobrać na Serwer administracyjny. Wybierz jedną z następujących opcji:

   - **Pobierz wszystkie języki, wraz z nowymi**

     Jeśli ta opcja jest zaznaczona, na Serwer administracyjny zostaną pobrane wszystkie wersje językowe aktualizacji. Domyślnie opcja ta jest zaznaczona.

   - **Pobierz wybrane języki**

     Jeśli ta opcja jest zaznaczona, z listy wersji językowych możesz wybrać te, które powinny zostać pobrane na Serwer administracyjny.
9. Określ, które konto ma być używane podczas uruchamiania zadania. Wybierz jedną z następujących opcji:

   - **Konto domyślne**

     Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

     Domyślnie opcja ta jest zaznaczona.

   - **Określ konto**

     Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

10. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

11. Kliknij przycisk **Zakończ**.

    Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

12. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

13. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.

14. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

Automatyczne aktualizowanie aplikacji innych firm

Niektóre aplikacje innych firm mogą być aktualizowane automatycznie. Producent aplikacji definiuje, czy aplikacja obsługuje funkcję automatycznej aktualizacji. Jeśli aplikacja innej firmy, zainstalowana na zarządzanym urządzeniu, obsługuje automatyczną aktualizację, możesz określić ustawienie automatycznej aktualizacji we właściwościach aplikacji. Po zmianie ustawienia automatycznej aktualizacji Agenty sieciowe stosują nowe ustawienie na każdym zarządzanym urządzeniu, na którym jest zainstalowana aplikacja.

Ustawienie automatycznej aktualizacji jest niezależne od innych obiektów i ustawień funkcji Zarządzanie lukami i poprawkami. Na przykład, to ustawienie nie zależy od stanu zatwierdzenia aktualizacji ani od zadań instalacji aktualizacji, takich jak *Zainstaluj wymagane aktualizacje i napraw luki*, *Zainstaluj aktualizacje Windows* oraz *Napraw luki*.

W celu skonfigurowania ustawienia automatycznej aktualizacji dla aplikacji innej firmy:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Rejestr aplikacji**.

2. Kliknij nazwę aplikacji, dla której chcesz zmienić ustawienie automatycznej aktualizacji.

   Aby uprościć wyszukiwanie, możesz przefiltrować listę według kolumny **Stan aktualizacji automatycznych**.

   Zostanie otwarte okno właściwości aplikacji.

3. W sekcji **Ogólne** wybierz wartość dla następującego ustawienia:

   Stan aktualizacji automatycznych

   Wybierz jedną z następujących opcji:

   - **Nie zdefiniowano**

     Funkcja automatycznej aktualizacji jest wyłączona. Kaspersky Security Center instaluje aktualizacje aplikacji innej firmy, korzystając z zadań: *Zainstaluj wymagane aktualizacje i napraw luki*, *Zainstaluj aktualizacje Windows* i *Napraw luki*.

   - **Dozwolony**

     Jak tylko wydawca opublikuje aktualizację dla aplikacji, ta aktualizacja jest automatycznie instalowana na zarządzanych urządzeniach. Dodatkowe działania nie są wymagane.

- **Zablokowano**

  Aktualizacje aplikacji nie są instalowane automatycznie. Kaspersky Security Center instaluje aktualizacje aplikacji innej firmy, korzystając z zadań: *Zainstaluj wymagane aktualizacje i napraw luki*, *Zainstaluj aktualizacje Windows* i *Napraw luki*.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Ustawienie automatycznej aktualizacji jest stosowane do wybranej aplikacji.

Eliminowanie luk w oprogramowaniu innych firm

Ta sekcja opisuje funkcje Kaspersky Security Center, które dotyczą eliminowania luk w oprogramowaniu zainstalowanym na zarządzanych urządzeniach.

Scenariusz: Wyszukiwanie i usuwanie luk w oprogramowaniu firm trzecich

Ta sekcja zawiera scenariusz wyszukiwania i naprawiania luk na zarządzanych urządzeniach działających pod kontrolą systemu Windows. Możesz znaleźć i naprawić luki w oprogramowaniu w systemie operacyjnym oraz w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft.

Wymagania wstępne

- Kaspersky Security Center zostanie wdrożony w Twojej organizacji.
- W Twojej organizacji znajdują się zarządzane urządzenia działające pod kontrolą systemu Windows.
- Połączenie internetowe w przypadku Serwera administracyjnego jest wymagane, aby można było wykonywać następujące zadania:
  - Sporządzanie listy zalecanych poprawek dla luk w oprogramowaniu firmy Microsoft. Lista jest tworzona i regularnie aktualizowana przez specjalistów z Kaspersky.
  - Naprawianie luk w oprogramowaniu firm trzecich innym niż oprogramowanie firmy Microsoft.

Etapy

Wyszukiwanie i naprawianie luk w oprogramowaniu odbywa się w etapach:

1. **Skanowanie luk w oprogramowaniu zainstalowanym na zarządzanych urządzeniach**

   Aby odszukać luki w oprogramowaniu zainstalowanym na zarządzanych urządzeniach, uruchom zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Kaspersky Security Center pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania.

Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Jeśli nie uruchamiałeś kreatora, uruchom go teraz lub utwórz zadanie ręcznie.

Dostępne instrukcje:

- Konsola administracyjna: Skanowanie aplikacji w poszukiwaniu luk, Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
- Kaspersky Security Center Web Console: Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji, Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

2. **Analizowanie listy wykrytych luk w oprogramowaniu**

Przejrzyj listę **Luki w oprogramowaniu** i zdecyduj, które luki mają zostać naprawione. Aby przejrzeć szczegółowe informacje o każdej luce, kliknij nazwę luki na liście. Dla każdej luki na liście możesz także przejrzeć statystyki dotyczące luki na zarządzanych urządzeniach.

Dostępne instrukcje:

- Konsola administracyjna: Przeglądanie informacji o lukach w oprogramowaniu, Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach
- Kaspersky Security Center Web Console: Przeglądanie informacji o lukach w oprogramowaniu, Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach

3. **Konfigurowanie naprawy luk**

Jeśli luki w oprogramowaniu zostaną wykryte, możesz naprawić luki w oprogramowaniu na zarządzanych urządzeniach, korzystając z zadania *Zainstaluj wymagane aktualizacje i napraw luki* lub zadania *Napraw luki*.

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do aktualizacji i naprawy luk w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft, zainstalowanym na zarządzanych urządzeniach. To zadanie umożliwia zainstalowanie kilku aktualizacji i naprawę kilku luk zgodnie z pewnymi regułami. Pamiętaj, że to zadanie może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami. Aby naprawić luki w oprogramowaniu, zadanie *Zainstaluj wymagane aktualizacje i napraw luki* używa zalecanych aktualizacji oprogramowania.

Zadanie *Napraw luki* nie wymaga opcji licencjonowania dla funkcji Zarządzanie lukami i poprawkami. Aby użyć tego zadania, należy ręcznie określić poprawki użytkownika dla luk w programach innych firm, wymienionych w ustawieniach zadania. Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla programów innych firm.

Możesz uruchomić Kreator naprawiania luk, który tworzy jedno z tych zadań automatycznie, lub możesz utworzyć jedno z tych zadań ręcznie.

Dostępne instrukcje:

- Konsola administracyjna: Wybieranie poprawek użytkownika dla luk w programach innych firm, Naprawianie luk w aplikacjach
- Kaspersky Security Center Web Console: Wybieranie poprawek użytkownika dla luk w programach innych firm, Naprawianie luk w programach innych firm, Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki

4. **Konfigurowanie terminarza zadań**

Aby upewnić się, że lista luk jest zawsze aktualna, skonfiguruj zadanie *Wyszukiwanie luk i wymaganych aktualizacji* tak, aby było uruchamiane automatycznie od czasu do czasu. Zalecana przeciętna częstotliwość uruchamiania to raz na tydzień.

Jeśli utworzyłeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz skonfigurować terminarz tak, aby zadanie było uruchamiane z tą samą częstotliwością co zadanie *Wyszukiwanie luk i wymaganych aktualizacji* lub rzadziej. Podczas ustawiania terminarza zadania *Napraw luki* należy pamiętać, żeby wybrać poprawki dla oprogramowania Microsoft lub określić poprawki użytkownika dla oprogramowania innych firm za każdym razem przed rozpoczęciem zadania.

Jeśli konfigurujesz terminarz uruchamiania zadania, upewnij się, że zadanie naprawy luki zostanie uruchomione po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

5. **Ignorowanie luk w oprogramowaniu (opcjonalne)**

   Jeśli chcesz, możesz zignorować luki w oprogramowaniu na wszystkich zarządzanych urządzeniach lub tylko na wybranych zarządzanych urządzeniach.

   Dostępne instrukcje:

   - Konsola administracyjna: Ignorowanie luk w oprogramowaniu
   - Kaspersky Security Center Web Console: Ignorowanie luk w oprogramowaniu

6. **Uruchamianie zadania naprawy luk**

   Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Napraw lukę*. Po zakończeniu zadania, upewnij się, że na liście zadań posiada stan *Zakończone pomyślnie*.

7. **Utwórz raport dotyczący wyników naprawy luk w oprogramowaniu (opcjonalne)**

   Aby wyświetlić szczegółowe statystyki dotyczące naprawy luk, wygeneruj Raport o lukach. Raport wyświetla informacje o lukach w oprogramowaniu, które nie zostały naprawione. Dzięki temu możesz wiedzieć o wyszukiwaniu i naprawie luk w programach innych firm, w tym w oprogramowaniu firmy Microsoft, w swojej organizacji.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie i przeglądanie raportu
   - Kaspersky Security Center Web Console: Tworzenie i przeglądanie raportu

8. **Sprawdzanie konfiguracji wyszukiwania i naprawy luk w programach innych firm**

   Upewnij się, że wykonałeś następujące czynności:

   - Uzyskałeś i przejrzałeś listę luk w oprogramowaniu na zarządzanych urządzeniach
   - Zignorowałeś luki w oprogramowaniu, jeśli chciałeś
   - Skonfigurowałeś zadanie naprawy luk
   - Skonfigurowałeś terminarz zadań wyszukiwania i naprawy luk w oprogramowaniu, aby były uruchamianie po kolei
   - Sprawdziłeś, czy zadanie naprawy luk w oprogramowaniu zostało uruchomione

Wyniki

Jeśli utworzyłeś i skonfigurowałeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, luki zostają naprawione na zarządzanych urządzeniach automatycznie. Jeśli zadanie zostaje uruchomione, zestawia listę dostępnych aktualizacji oprogramowania z regułami określonymi w ustawieniach zadania. Wszystkie aktualizacje oprogramowania, które spełniają kryteria w regułach, zostaną pobrane do repozytorium Serwera administracyjnego i zostaną zainstalowane w celu naprawy luk w oprogramowaniu.

Jeśli utworzyłeś zadanie *Napraw luki*, naprawione zostaną tylko luki w oprogramowaniu firmy Microsoft.

Informacje o wyszukiwaniu i eliminowaniu luk w oprogramowaniu

Kaspersky Security Center wykrywa i naprawia luki w oprogramowaniu na zarządzanych urządzeniach działających pod kontrolą systemów operacyjnych z rodziny Microsoft Windows. Luki są wykrywane w systemie operacyjnym i w oprogramowaniu innych firm, w tym w oprogramowaniu firmy Microsoft.

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), przy czym funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Wyszukiwanie luk w oprogramowaniu

Aby znaleźć luki w oprogramowaniu, Kaspersky Security Center wykorzystuje znaki charakterystyczne z bazy danych znanych zagrożeń. Ta baza danych jest tworzona przez specjalistów z Kaspersky. Zawiera informacje o lukach, takie jak opis luki, data wykrycia luki, priorytet luki. Szczegóły dotyczące luk w oprogramowaniu można znaleźć na stronie internetowej Kaspersky.

Kaspersky Security Center wykorzystuje zadanie *Wyszukiwanie luk i wymaganych aktualizacji* do wykrywania luk w oprogramowaniu.

W niektórych przypadkach luki w zabezpieczeniach wykryte w systemie operacyjnym Microsoft Windows można naprawić, korzystając z jednej z następujących metod:

- Instalowanie aktualizacji systemu operacyjnego.
- Aktualizacja systemu operacyjnego do nowszej wersji (na przykład z Windows 10 do Windows 11).

W tym scenariuszu Kaspersky Security Center wyświetla dwa wpisy dla tej samej luki w zabezpieczeniach.

Naprawianie luk w oprogramowaniu

Aby naprawić luki w oprogramowaniu, Kaspersky Security Center używa aktualizacji oprogramowania opublikowanych przez producentów oprogramowania. Metadane aktualizacji oprogramowania są pobierane z repozytorium Serwera administracyjnego w wyniku uruchomienia następującego zadania:

- *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. To zadanie jest przeznaczone do pobrania metadanych aktualizacji dla Kaspersky i oprogramowania firm trzecich. To zadanie jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Możesz ręcznie utworzyć zadanie Pobierz uaktualnienia do repozytorium Serwera administracyjnego.

- *Wykonaj synchronizację Windows Update*. To zadanie jest przeznaczone do pobrania metadanych aktualizacji dla oprogramowania firmy Microsoft.

Aktualizacje oprogramowania eliminujące luki mogą być w postaci pełnych pakietów dystrybucyjnych lub poprawek. Aktualizacje oprogramowania, które eliminują luki w oprogramowaniu, nazywane są *poprawkami*. *Zalecane poprawki* to takie poprawki, które są zalecane do zainstalowania przez specjalistów z Kaspersky. *Poprawki użytkownika* to takie poprawki, które są ręcznie określane do zainstalowania przez użytkowników. Aby zainstalować poprawkę użytkownika, należy utworzyć pakiet instalacyjny zawierający tę poprawkę.

Jeśli posiadasz licencję dla Kaspersky Security Center z funkcją Zarządzanie lukami i poprawkami, aby usunąć luki w oprogramowaniu, możesz użyć zadania *Zainstaluj wymagane aktualizacje i napraw luki*. To zadanie automatycznie eliminuje kilka luk poprzez zainstalowanie zalecanych poprawek. Dla tego zadania można ręcznie skonfigurować pewne reguły do naprawy kilku luk.

Jeśli nie posiadasz licencji dla Kaspersky Security Center z funkcją Zarządzanie lukami i poprawkami, aby usunąć luki w oprogramowaniu, możesz użyć zadania *Napraw luki*. Korzystając z tego zadania, możesz wyeliminować luki poprzez zainstalowanie zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla innych programów innych firm.

Ze względów bezpieczeństwa wszelkie aktualizacje oprogramowania innych firm, które instalujesz za pomocą funkcji Zarządzanie lukami i poprawkami, są automatycznie skanowane w poszukiwaniu szkodliwego oprogramowania przez technologie firmy Kaspersky. Technologie te są używane do automatycznego sprawdzania plików i obejmują skanowanie antywirusowe, analizę statyczną, analizę dynamiczną, analizę zachowania w środowisku sandbox i uczenie maszynowe.

Eksperci firmy Kaspersky nie przeprowadzają ręcznej analizy aktualizacji oprogramowania innych firm, które są instalowane przez funkcję Zarządzanie lukami i poprawkami. Ponadto eksperci z firmy Kaspersky nie wyszukują luk (znanych lub nieznanych) ani nieudokumentowanych funkcji w takich aktualizacjach, a także nie przeprowadzają innych rodzajów analizy aktualizacji innych, niż określone w powyższym akapicie.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Aby naprawić niektóre luki w oprogramowaniu, należy zaakceptować Umowę licencyjną użytkownika końcowego (EULA) dla instalowanego oprogramowania, jeśli wymagane jest zaakceptowanie Umowy licencyjnej. Jeśli odrzucisz Umowę licencyjną użytkownika końcowego, luka w oprogramowaniu nie zostanie wyeliminowana.

Eliminowanie luk w oprogramowaniu innych firm

Po uzyskaniu listy luk w oprogramowaniu możliwe jest wyeliminowanie luk w oprogramowaniu na zarządzanych urządzeniach działających pod kontrolą systemu Windows. Luki w oprogramowaniu w systemie operacyjnym i oprogramowaniu innych firm, w tym w oprogramowaniu firmy Microsoft, można naprawić, tworząc i uruchamiając zadanie *Napraw luki* lub zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Opcjonalnie możesz utworzyć zadanie naprawiania luk w oprogramowaniu w następujący sposób:

- Otwierając listę luk i określając, które luki należy naprawić.

  W rezultacie powstaje nowe zadanie naprawy luk w oprogramowaniu. Istnieje możliwość dodania wybranych luk do istniejącego zadania.

- Uruchamiając Kreator naprawiania luk.

  Funkcje kreatora naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

  Kreator upraszcza tworzenie i konfigurację zadania naprawy luki w zabezpieczeniach i pozwala wyeliminować tworzenie zbędnych zadań zawierających te same aktualizacje do zainstalowania.

Naprawianie luk w oprogramowaniu przy użyciu listy luk w zabezpieczeniach

W celu wyeliminowania luk w oprogramowaniu:

1. Otwórz jedną z list luk:

   - Aby otworzyć ogólną listę luk, w menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.
   - Aby otworzyć listę luk dla zarządzanego urządzenia, w menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia** → <device name> → **Zaawansowane** → **Luki w oprogramowaniu**.
   - Aby otworzyć listę luk dla określonej aplikacji, w menu głównym przejdź do **Operacje** → **Aplikacje innych firm** → **Rejestr aplikacji** → <application name> → **Luki**.

   Zostanie wyświetlona lista luk w oprogramowaniu innych firm.

2. Wybierz jedną lub więcej luk na liście, a następnie kliknij przycisk **Napraw lukę**.

   Jeśli brakuje zalecanej aktualizacji oprogramowania do naprawy jednej z wybranych luk, zostanie wyświetlony odpowiedni komunikat.

   Aby naprawić niektóre luki w oprogramowaniu, należy zaakceptować Umowę licencyjną użytkownika końcowego (EULA), dla instalowanego oprogramowania jeśli wymagane jest zaakceptowanie Umowy licencyjnej. Jeśli odrzucisz Umowę licencyjną użytkownika końcowego, luka w oprogramowaniu nie zostanie wyeliminowana.

3. Wybierz jedną z następujących opcji:

   - **Nowe zadanie**

     Zostanie uruchomiony Kreator tworzenia nowego zadania. Jeśli masz licencję Zarządzania lukami i poprawkami, domyślnie wybrany jest typ zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Jeśli nie masz licencji, domyślnie wybrany jest typ zadania *Napraw luki*. Aby zakończyć tworzenie zadania, postępuj zgodnie z instrukcjami kreatora.

   - **Napraw lukę (dodaj regułę do określonego zadania)**

     Wybierz zadanie, do którego chcesz dodać wybrane luki. Jeśli masz licencję Zarządzania lukami i poprawkami, wybierz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*. Nowa reguła eliminacji wybranych luk zostanie automatycznie dodania do wybranego zadania. Jeśli nie masz licencji, wybierz zadanie *Napraw luki*. Wybrane luki zostaną dodane do właściwości zadania.

     Zostanie otwarte okno właściwości zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

   Jeśli wybrałeś utworzenie nowego zadania, zadanie zostanie utworzone i wyświetlone na liście zadań, w sekcji **Zasoby (urządzenia)** → **Zadania**. Jeśli wybrałeś dodanie luk do istniejącego zadania, luki zostaną zapisane we właściwościach zadania.

Aby wyeliminować luki w oprogramowaniu firm trzecich, uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Napraw luki*. Jeśli utworzyłeś zadanie *Napraw luki*, powinieneś ręcznie określić aktualizacje oprogramowania w celu naprawy luk w oprogramowaniu, wymienionych w ustawieniach zadania.

Naprawianie luk w oprogramowaniu przy użyciu kreatora naprawiania luk

Funkcje kreatora naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

Aby naprawić luki w oprogramowaniu przy użyciu kreatora naprawiania luk:

1. W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.

   Zostanie wyświetlona lista luk w oprogramowaniu innych firm, zainstalowanym na zarządzanych urządzeniach.

2. Zaznacz pole obok luki, który chcesz wyeliminować.

3. Kliknij przycisk **Uruchom kreatora naprawiania luk**.

   Zostanie uruchomiony Kreator naprawiania luk. Strona **Wybierz zadanie naprawiania luk** wyświetla listę wszystkich istniejących zadań następujących typów:

   - *Zainstaluj wymagane aktualizacje i napraw luki*
   - *Zainstaluj aktualizacje Windows*
   - *Napraw luki*

   Nie można zmodyfikować ostatnich dwóch typów zadań, aby zainstalować nowe aktualizacje. Aby zainstalować nowe aktualizacje, możesz użyć tylko zadania *Zainstaluj wymagane aktualizacje i napraw luki*.

4. Jeśli chcesz, aby kreator wyświetlał tylko te zadania, które usuwają wybraną lukę, włącz opcję **Pokaż tylko zadania naprawiające tę lukę**.

5. Wybierz, co chcesz zrobić:

- Aby rozpocząć zadanie, zaznacz pole wyboru obok nazwy zadania, a następnie kliknij przycisk **Uruchom**.
- Aby dodać nową regułę do istniejącego zadania:

  a. Zaznacz pole obok nazwy zadania i kliknij przycisk **Dodaj regułę**.

  b. Na wyświetlonej stronie skonfiguruj nową regułę:

  - **Reguła dla naprawiania luk tego priorytetu**

    Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

    Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

    Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

    Domyślnie opcja ta jest wyłączona.

  - **Reguła naprawiania luk za pomocą aktualizacji tego samego typu, co aktualizacja zdefiniowana jako zalecana dla wybranej luki** (dostępna tylko dla luk w oprogramowaniu Microsoft)
  - **Reguła naprawiania luk w aplikacjach według wybranego dostawcy** (dostępne tylko dla luk w oprogramowaniu innych firm)
  - **Reguła naprawiania luk we wszystkich wersjach wybranej aplikacji** (dostępne tylko dla luk w oprogramowaniu innych firm)
  - **Reguła naprawiania wybranej luki**
  - **Akceptuj aktualizacje, które naprawiają tę lukę**

    Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

    Domyślnie opcja ta jest wyłączona.

  c. Kliknij przycisk **Dodaj**.

- W celu utworzenia zadania:

  a. Kliknij przycisk **Nowe zadanie**.

  b. Na wyświetlonej stronie skonfiguruj nową regułę:

  - **Reguła dla naprawiania luk tego priorytetu**

    Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

    Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

Domyślnie opcja ta jest wyłączona.

- **Reguła naprawiania luk za pomocą aktualizacji tego samego typu, co aktualizacja zdefiniowana jako zalecana dla wybranej luki** (dostępna tylko dla luk w oprogramowaniu Microsoft)
- **Reguła naprawiania luk w aplikacjach według wybranego dostawcy** (dostępne tylko dla luk w oprogramowaniu innych firm)
- **Reguła naprawiania luk we wszystkich wersjach wybranej aplikacji** (dostępne tylko dla luk w oprogramowaniu innych firm)
- **Reguła naprawiania wybranej luki**
- **Akceptuj aktualizacje, które naprawiają tę lukę**

  Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

  Domyślnie opcja ta jest wyłączona.

c. Kliknij przycisk **Dodaj**.

Jeśli wybrano rozpoczęcie zadania, możesz zamknąć kreatora. Zadanie zakończy się w tle. Dalsze działania nie są wymagane.

Jeśli wybrałeś dodanie reguły do istniejącego zadania, zostanie otwarte okno właściwości zadania. Nowa reguła została już dodana do właściwości zadania. Możesz przejrzeć lub zmodyfikować regułę lub ustawienia innego zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Jeśli chcesz utworzyć zadanie, kontynuuj tworzenie zadania w kreatorze tworzenia nowego zadania. Nowa reguła dodana w kreatorze naprawiania luk zostanie wyświetlona w kreatorze tworzenia nowego zadania. Po zakończeniu pracy kreatora, do listy zadań zostanie dodane zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.

Tworzenie zadania Napraw luki

Zadanie *Napraw luki* pozwala naprawić luki w oprogramowaniu na zarządzanych urządzeniach z systemem Windows. Możesz naprawić luki w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft.

Jeśli nie masz licencji Zarządzania lukami i poprawkami, nie możesz tworzyć nowych zadań typu *Napraw luki*. Aby naprawić nowe luki, możesz dodać je do istniejącego zadania *Napraw luki*. Zalecamy użycie zadania *Zainstaluj wymagane aktualizacje i napraw luki* zamiast zadania *Napraw luki*. Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* umożliwia automatyczne instalowanie wielu aktualizacji i naprawianie wielu luk w zabezpieczeniach, zgodnie z określonymi przez Ciebie regułami.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

W celu utworzenia zadania Napraw luki:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Napraw luki**.
4. Określ nazwę tworzonego zadania.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.
6. Kliknij przycisk **Dodaj**.

   Zostanie otwarta lista luk.
7. Wybierz luki, które chcesz naprawić, a następnie kliknij **OK**.

   Luki w oprogramowaniu firmy Microsoft zwykle zawierają zalecane poprawki. Nie są wymagane żadne dodatkowe czynności. W przypadku luk w zabezpieczeniach oprogramowania innych producentów należy najpierw określić poprawkę użytkownika dla każdej luki, którą chcesz naprawić. Następnie będzie można dodać te luki do zadania *Napraw luki*.
8. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

   - **Nie uruchamiaj ponownie urządzenia**

     Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

   - **Uruchom urządzenie ponownie**

     Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

   - **Pytaj użytkownika o akcję**

     Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

     Domyślnie opcja ta jest zaznaczona.

   - **Ponawiaj pytanie co (min)**

     Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany, aplikacja nie zezwoli na ponowne uruchomienie urządzenia.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

9. Określ ustawienia konta:

   - **Konto domyślne**

     Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

     Domyślnie opcja ta jest zaznaczona.

   - **Określ konto**

     Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

   - **Konto**

     Konto, z poziomu którego zadanie jest uruchamiane.

   - **Hasło**

     Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

10. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

11. Kliknij przycisk **Zakończ**.

    Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

12. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

13. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.

14. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki

> Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do aktualizacji i naprawy luk w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft, zainstalowanym na zarządzanych urządzeniach. To zadanie umożliwia zainstalowanie kilku aktualizacji i naprawę kilku luk zgodnie z pewnymi regułami.

W celu zainstalowania aktualizacji lub wyeliminowania luk za pomocą zadania *Zainstaluj wymagane aktualizacje i napraw luki*, możesz wykonać jedną z następujących czynności:

- Uruchom kreator instalacji aktualizacji lub Kreator naprawiania luk.
- Utwórz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.
- Dodaj regułę instalacji aktualizacji do istniejącego pliku *Zainstaluj wymagane aktualizacje i napraw luki* zadanie.

Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Zainstaluj wymagane aktualizacje i napraw luki**.

   Jeśli zadanie nie jest wyświetlane, sprawdź, czy Twoje konto ma uprawnienia **Odczyt**, **Modyfikuj** i **Wykonaj** dla obszaru funkcjonalnego **Zarządzanie systemem: Zarządzanie lukami w zabezpieczeniach i poprawkami**. Bez tych praw dostępu nie można utworzyć ani skonfigurować zadania *Zainstaluj wymagane aktualizacje i napraw luki*.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.
6. Określ zasady instalacji aktualizacji, a następnie określ następujące ustawienia:

   - **Uruchom instalację podczas ponownego uruchamiania lub wyłączania urządzenia**

     Jeśli ta opcja jest włączona, aktualizacje są instalowane po ponownym uruchomieniu lub zamknięciu urządzenia. W innym przypadku aktualizacje są instalowane zgodnie z terminarzem.

     Użyj tej opcji, jeśli instalowanie aktualizacji może wpłynąć na działanie urządzenia.

     Domyślnie opcja ta jest wyłączona.

- **Zainstaluj wymagane ogólne składniki systemu**

  Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

  Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

  Domyślnie opcja ta jest wyłączona.

- **Zezwól na instalację nowych wersji aplikacji podczas aktualizacji**

  Jeśli ta opcja jest włączona, aktualizacje są dozwolone, gdy powodują zainstalowanie nowej wersji aplikacji.

  Jeśli ta opcja jest wyłączona, aplikacja nie zostanie zaktualizowana. W takiej sytuacji możesz ręcznie zainstalować nowe wersje aplikacji lub użyć w tym celu innego zadania. Na przykład, możesz użyć tej opcji, jeśli struktura Twojej firmy nie jest obsługiwana przez nową wersję aplikacji lub jeśli chcesz sprawdzić aktualizację w infrastrukturze testowej.

  Domyślnie opcja ta jest włączona.

  > Aktualizowanie aplikacji może spowodować problemy z działaniem powiązanych aplikacji zainstalowanych na urządzeniach klienckich.

- **Pobierz aktualizacje na urządzenie, ale ich nie instaluj**

  Jeśli ta opcja jest włączona, aplikacja pobierze uaktualnienia na urządzenie, ale nie zainstaluje ich automatycznie. Możesz ręcznie zainstalować pobrane aktualizacje.

  Aktualizacje Microsoft są pobierane do folderu systemowego Windows. Aktualizacje aplikacji firm trzecich (aplikacje innych producentów niż Kaspersky i Microsoft) są pobierane do folderu określonego w polu **Pobierz uaktualnienia do**.

  Jeśli ta opcja jest wyłączona, aktualizacje są instalowane na urządzeniu automatycznie.

  Domyślnie opcja ta jest wyłączona.

- **Pobierz uaktualnienia do**

  Ten folder jest używany do pobierania aktualizacji aplikacji innych firm (aplikacji innych producentów niż Kaspersky i Microsoft).

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy zapisywanie plików śledzenia jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

7. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

  Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

  Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Czas oczekiwania przed wymuszeniem zamknięcia aplikacji dla zablokowanych sesji (min)**

  Wymuszone zamknięcie aplikacji ma miejsce, gdy urządzenie użytkownika jest zablokowane (automatycznie po określonym czasie nieaktywności lub ręcznie).

  Jeśli ta opcja jest włączona, wymuszone zamknięcie aplikacji na zablokowanym urządzeniu odbywa się po minięciu czasu określonego w polu wejściowym.

  Jeśli ta opcja jest wyłączona, aplikacje nie będą zamykane na zablokowanym urządzeniu.

  Domyślnie opcja ta jest wyłączona.

8. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

9. Kliknij przycisk **Zakończ**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

10. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

11. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.

12. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

Jeśli wyniki zadania zawierają ostrzeżenie o błędzie 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", możesz rozwiązać ten problem poprzez Rejestr systemu Windows.

Dodawanie reguł dla instalacji aktualizacji

Ta funkcja jest dostępna tylko w ramach licencji na Zarządzanie lukami i poprawkami.

Podczas instalowania aktualizacji oprogramowania lub naprawiania luk w oprogramowaniu przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki* należy określić zasady instalacji aktualizacji. Te reguły określają aktualizacje do zainstalowania oraz luki do wyeliminowania.

Dokładne ustawienia zależą od tego, czy dodajesz regułę dla wszystkich aktualizacji Windows Update lub aktualizacji aplikacji firm trzecich (aplikacje stworzone przez producentów oprogramowania innych niż Kaspersky i Microsoft) lub wszystkich aplikacji. Podczas dodawania reguły dla aktualizacji Windows Update lub aktualizacji aplikacji firm trzecich możesz wybrać określone aplikacje oraz wersje aplikacji, dla których chcesz zainstalować uaktualnienia. Podczas dodawani reguły dla wszystkich aktualizacji możesz wybrać określone uaktualnienia, które chcesz zainstalować, oraz luki, które chcesz wyeliminować poprzez zainstalowanie uaktualnień.

Regułę instalacji aktualizacji można dodać w następujący sposób:

- Dodając regułę podczas tworzenia nowego zadania Zainstaluj wymagane aktualizacje i napraw luki.
- Dodając regułę w zakładce **Ustawienia aplikacji** w oknie właściwości istniejącego zadania *Zainstaluj wymagane aktualizacje i napraw luki*.
- Za pomocą kreatora instalacji aktualizacji lub kreatora naprawiania luk.

W celu dodania nowej reguły dla wszystkich aktualizacji:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla wszystkich aktualizacji**.

3. W kroku **Kryteria ogólne** użyj list rozwijalnych do określenia następujących ustawień:

- **Zbiór uaktualnień do zainstalowania**

  Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

  - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
  - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
  - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

- **Napraw luki z priorytetem równym lub większym niż**

  Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

  Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

  Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

  Domyślnie opcja ta jest wyłączona.

4. W kroku **Aktualizacje** wybierz aktualizacje, które mają zostać zainstalowane:

- **Zainstaluj wszystkie pasujące aktualizacje**

  Zainstaluj aktualizacje oprogramowania, które spełniają kryteria określone w kroku **Kryteria ogólne**. Ta opcja jest wybrana domyślnie.

- **Zainstaluj tylko aktualizacje z listy**

  Instalowane są tylko te aktualizacje oprogramowania, które wybierzesz ręcznie z listy. Ta lista zawiera wszystkie dostępne aktualizacje oprogramowania.

  Na przykład, możesz wybrać określone aktualizacje w następujących przypadkach: aby sprawdzić ich instalację w środowisku testowym, aby zaktualizować tylko krytyczne aplikacje lub aby zaktualizować tylko określone aplikacje.

  - **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

    Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

    Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

    Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

Domyślnie opcja ta jest włączona.

5. W kroku **Luki** wybierz luki, które zostaną wyeliminowane poprzez zainstalowanie wybranych aktualizacji:

   - **Napraw wszystkie luki spełniające inne kryteria**

     Wyeliminuj wszystkie luki, które spełniają kryteria określone na stronie **Kryteria ogólne** kreatora. Ta opcja jest wybrana domyślnie.

   - **Napraw tylko luki z listy**

     Naprawione zostaną tylko te luki, które ręcznie wybierzesz z listy. Ta lista zawiera wszystkie wykryte luki.

     Na przykład, możesz wybrać określone luki w następujących przypadkach: aby sprawdzić ich eliminację w środowisku testowym, aby wyeliminować luki tylko w krytycznych aplikacjach lub aby wyeliminować luki tylko w określonych aplikacjach.

6. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

W celu dodania nowej reguły dla aktualizacji Windows Update:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji systemu Windows**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

- **Napraw luki z priorytetem MSRC równym lub większym niż**

  Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

  Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

  Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

  Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Kategorie aktualizacji** wybierz kategorie aktualizacji, które mają zostać zainstalowane. Te kategorie są takie same, jak w Microsoft Update Catalog. Domyślnie, zaznaczone są wszystkie kategorie.

6. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

W celu dodania nowej reguły dla aktualizacji aplikacji firm trzecich:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji firm trzecich**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.

     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.

     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji Ustawienia okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

Wybieranie poprawek użytkownika dla luk w programach innych firm

Aby użyć zadania *Napraw luki*, należy ręcznie określić aktualizacje oprogramowania do naprawy luk w programach innych firm, wymienionych w ustawieniach zadania. Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla innych programów innych firm. *Poprawki użytkownika* to aktualizacje oprogramowania do naprawy luk, które administrator ręcznie określa do zainstalowania.

W celu wybrania poprawek użytkownika dla luk w programach firm trzecich:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Luki w oprogramowaniu**.

   Strona wyświetla listę luk w oprogramowaniu wykrytych na urządzeniach klienckich.

2. Na liście luk w oprogramowaniu kliknij odnośnik z nazwą luki w oprogramowaniu, dla której chcesz określić poprawkę użytkownika.

   Zostanie otwarte okno właściwości luki.

3. W lewej części okna wybierz sekcję **Poprawki użytkownika i inne poprawki**.

   Zostanie wyświetlona lista poprawek użytkownika dla wybranej luki w oprogramowaniu.

4. Kliknij **Dodaj**.

   Zostanie wyświetlona lista dostępnych pakietów instalacyjnych. Lista wyświetlonych pakietów instalacyjnych odpowiada liście **Operacje → Repozytoria → Pakiety instalacyjne**. Jeśli nie utworzono pakietu instalacyjnego zawierającego poprawkę użytkownika dla wybranej luki, możesz utworzyć pakiet teraz, uruchamiając Kreator tworzenia nowego pakietu.

5. Wybierz pakiet (lub pakiety) instalacyjny zawierający poprawkę użytkownika (lub poprawki użytkownika) dla luki w oprogramowaniu innych firm.

6. Kliknij **Zapisz**.

Zostaną określone pakiety instalacyjne zawierające poprawki użytkownika dla luki w oprogramowaniu. Jeśli zadanie jest uruchamiane *Napraw luki*, pakiet instalacyjny zostanie zainstalowany, a luka w oprogramowaniu zostanie wyeliminowana.

Przeglądanie informacji o lukach w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach

Po przeskanowaniu oprogramowaniu na zarządzanych urządzeniach w poszukiwaniu luk, możesz przejrzeć listę luk w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach. Jeśli uruchomisz zadanie dla hierarchii Serwerów administracyjnych, możesz wyświetlić listę zarządzanych urządzeń z wykrytymi lukami tylko dla wybranego Serwera administracyjnego.

W celu przejrzenia listy luk w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach:

W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.

Strona wyświetla listę luk w oprogramowaniu wykrytych na urządzeniach klienckich.

Możesz także wygenerować i przejrzeć Raport o lukach.

Możesz określić filtr przeglądania listy luk w oprogramowaniu. Kliknij ikonę **Filtr** ( ) w prawym górnym rogu listy luk w oprogramowaniu do zarządzania filtrem. Możesz także wybrać jeden z predefiniowanych filtrów z listy rozwijalnej **Wstępnie ustawione filtry** nad listą luk w oprogramowaniu.

Możesz uzyskać szczegółowe informacje o dowolnej luce z listy.

W celu uzyskania informacji o luce w oprogramowaniu:

Na liście luk w oprogramowaniu kliknij odnośnik z nazwą luki.

Zostanie otwarte okno właściwości luki w oprogramowaniu.

Przeglądanie informacji o lukach w oprogramowaniu wykrytych na wybranym zarządzanym urządzeniu

Możesz przejrzeć informacje o lukach w oprogramowaniu, wykrytych na wybranym zarządzanym urządzeniu działającym pod kontrolą systemu Windows.

W celu wyeksportowania listy luk w oprogramowaniu, wykrytych na wybranym zarządzanym urządzeniu:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń kliknij odnośnik z nazwą urządzenia, dla którego chcesz przejrzeć wykryte luki w oprogramowaniu.

   Zostanie wyświetlone okno właściwości wybranego urządzenia.

3. W oknie właściwości wybranego urządzenia wybierz zakładkę **Zaawansowane**.

4. W lewej części okna wybierz sekcję **Luki w oprogramowaniu**.

Zostanie wyświetlona lista luk w oprogramowaniu, wykrytych na wybranym, zarządzanym urządzeniu.

W celu przejrzenia właściwości wybranej luki w oprogramowaniu:

Kliknij odnośnik z nazwą luki w oprogramowaniu na liście luk w oprogramowaniu.

Zostanie otwarte okno właściwości wybranej luki w oprogramowaniu.

Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach

Statystyki dla każdej luki w oprogramowaniu możesz przejrzeć na zarządzanych urządzeniach. Statystyki są przedstawiane w postaci wykresu. Wykres wyświetla liczbę urządzeń z następującymi stanami:

- *Zignorowano na: <liczba urządzeń>*. Stan jest przypisywany, jeśli we właściwościach luki ręcznie ustawiono opcję ignorowania luki.
- *Naprawiono na: <liczba urządzeń>*. Ten stan jest przypisywany, jeśli zadanie naprawy luki zostało zakończone pomyślnie.
- *Naprawa zaplanowana na: <liczba urządzeń>*. Stan jest przypisywany, jeśli utworzono zadanie naprawy luki, ale zadanie nie zostało jeszcze wykonane.
- *Zastosowano poprawkę na: <liczba urządzeń>*. Stan jest przypisywany, jeśli ręcznie wybrano aktualizację oprogramowania do naprawy luki, ale ta aktualizacja oprogramowania nie naprawiła luki.
- *Naprawa wymagana na: <liczba urządzeń>*. Ten stan jest przypisywany, jeśli luka została naprawiona tylko na niektórych zarządzanych urządzeniach i wymagana jest naprawa luki na większej liczbie zarządzanych urządzeń.

W celu sprawdzenia statystyk dotyczących luki na zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Luki w oprogramowaniu**.

   Strona wyświetla listę luk w aplikacjach wykrytych na zarządzanych urządzeniach.

2. Zaznacz pole obok żądanej luki.
3. Kliknij przycisk **Statystyki luk na urządzeniach**.

   Zostanie wyświetlony wykres stanów luk. Kliknięcie stanu spowoduje otwarcie listy urządzeń, na których luka posiada wybrany stan.

Eksportowanie listy luk w oprogramowaniu do pliku

Wyświetloną listę luk możesz wyeksportować do plików CSV lub TXT. Możesz użyć tych plików, na przykład, do wysłania ich do swojego menedżera ds. bezpieczeństwa informacji lub przechowywać je w celach statystycznych.

W celu wyeksportowania listy luk w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach do pliku tekstowy:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Luki w oprogramowaniu**.

   Strona wyświetla listę luk w aplikacjach wykrytych na zarządzanych urządzeniach.

2. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj do pliku TXT** lub przycisk **Eksportuj do pliku CSV**.

Plik zawierający listę luk w oprogramowaniu zostanie pobrany na urządzenie, którego aktualnie używasz.

W celu wyeksportowania listy luk w oprogramowaniu, wykrytych na wybranym zarządzanym urządzeniu, do pliku tekstowego:

1. Otwórz listę luk w oprogramowaniu wykrytych na wybranym zarządzanym urządzeniu.

2. Wybierz luki w oprogramowaniu, które chcesz wyeksportować.

   Pomiń ten krok, jeśli chcesz wyeksportować pełną listę luk w oprogramowaniu wykrytych na zarządzanym urządzeniu.

   Jeśli chcesz wyeksportować pełną listę luk w oprogramowaniu, wykrytych na zarządzanym urządzeniu, wyeksportowane zostaną tylko luki wyświetlane na bieżącej stronie.

3. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj do pliku TXT** lub przycisk **Eksportuj do pliku CSV**.

Plik zawierający listę luk w oprogramowaniu, wykrytych na wybranym zarządzanym urządzeniu, zostanie pobrany na urządzenie, którego używasz w danym momencie.

Ignorowanie luk w oprogramowaniu

Możesz zignorować luki w oprogramowaniu, które mają zostać naprawione. Przyczyny zignorowania luk w oprogramowaniu mogą być, na przykład, następujące:

- Nie uważasz luki w oprogramowaniu za krytyczną dla swojej organizacji.
- Rozumiesz, poprawka luki w oprogramowaniu może uszkodzić dane związane z oprogramowaniem, które wymagało naprawy luki.
- Jesteś pewien, że luka w oprogramowaniu nie jest niebezpieczna dla sieci w Twojej organizacji, ponieważ używasz innych środków ochrony swoich zarządzanych urządzeń.

Możesz zignorować lukę w oprogramowaniu na wszystkich zarządzanych urządzeniach lub tylko na wybranych zarządzanych urządzeniach.

W celu zignorowania luki w oprogramowaniu na wszystkich zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Luki w oprogramowaniu**.

   Strona wyświetla listę luk w oprogramowaniu wykrytych na zarządzanych urządzeniach.

2. Na liście luk w oprogramowaniu kliknij odnośnik z nazwą luki w oprogramowaniu, którą chcesz zignorować.

   Zostanie otwarte okno właściwości luk w oprogramowaniu.

3. Na zakładce **Ogólne** włącz opcję **Ignoruj lukę**.
4. Kliknij przycisk **Zapisz**.

   Okno właściwości luk w oprogramowaniu zostanie zamknięte.

Luka w oprogramowaniu zostanie zignorowana na wszystkich zarządzanych urządzeniach.

W celu zignorowania luki w oprogramowaniu na wybranym zarządzanym urządzeniu:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.
2. Na liście zarządzanych urządzeń kliknij odnośnik z nazwą urządzenia, na którym chcesz zignorować lukę w oprogramowaniu.

   Zostanie otwarte okno właściwości urządzenia.
3. W oknie właściwości urządzenia wybierz zakładkę **Zaawansowane**.
4. W lewej części okna wybierz sekcję **Luki w oprogramowaniu**.

   Zostanie wyświetlona lista luk w oprogramowaniu wykrytych na urządzeniu.
5. Na liście luk w oprogramowaniu wybierz lukę, którą chcesz zignorować na wybranym urządzeniu.

   Zostanie otwarte okno właściwości luk w oprogramowaniu.
6. W oknie właściwości luki w oprogramowaniu, na zakładce **Ogólne** włącz opcję **Ignoruj lukę**.
7. Kliknij przycisk **Zapisz**.

   Okno właściwości luk w oprogramowaniu zostanie zamknięte.
8. Zamknij okno właściwości urządzenia.

Luka w oprogramowaniu zostanie zignorowana na wybranym urządzeniu.

Zignorowana luka w oprogramowaniu nie zostanie naprawiona po zakończeniu wykonywania zadania *Napraw luki* lub zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Możesz wykluczyć zignorowane luki w oprogramowaniu z listy luk z użyciem filtra.

Zarządzanie aplikacjami uruchomionymi na urządzeniach klienckich

Ta sekcja opisuje funkcje Kaspersky Security Center, które dotyczą zarządzania uruchamianiem aplikacji na urządzeniach klienckich.

Korzystanie z Kontroli aplikacji do zarządzania plikami wykonywalnymi

Możesz użyć komponentu Kontrola aplikacji, aby zezwolić lub zablokować uruchamianie plików wykonywalnych na urządzeniach użytkowników. Komponent Kontrola aplikacji obsługuje systemy operacyjne oparte na systemie Windows i Linux.

W systemach operacyjnych opartych na systemie Linux komponent Kontrola aplikacji jest dostępny od wersji Kaspersky Endpoint Security 11.2 for Linux. Komponent ten jest również dostępny w Kaspersky Embedded Systems Security for Windows w wersji 3.0 i nowszych.

Wymagania wstępne

- Kaspersky Security Center zostanie wdrożony w Twojej organizacji.
- Zasada Kaspersky Endpoint Security for Windows lub Kaspersky Endpoint Security for Linux została utworzona i jest aktywna.
- Zasada Kaspersky Embedded Systems Security for Windows lub Kaspersky Embedded Systems Security for Linux została utworzona i jest aktywna.

Etapy

Scenariusz korzystania z Kontroli aplikacji podzielony jest na etapy:

1. **Tworzenie i przeglądanie listy plików wykonywalnych na urządzeniach klienckich**

   Ten etap pomaga w odnalezieniu plików wykonywalnych, które znajdują się na zarządzanych urządzeniach. Przejrzyj listę plików wykonywalnych i porównaj ją z listami dozwolonych i zabronionych plików wykonywalnych. Ograniczenia dotyczące użycia plików wykonywalnych mogą być związane z polityką bezpieczeństwa informacji, obowiązującej w Twojej organizacji.

   Dostępne instrukcje:

   - Konsola administracyjna: Inwentaryzacja plików wykonywalnych
   - Kaspersky Security Center Web Console: Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

2. **Tworzenie kategorii dla plików wykonywalnych używanych w Twojej organizacji**

   Przeanalizuj listy plików wykonywalnych, przechowywanych na zarządzanych urządzeniach. Na podstawie analizy utwórz kategorie dla plików wykonywalnych. Zalecane jest utworzenie kategorii „Aplikacje do pracy”, która obejmuje standardowy zestaw plików wykonywalnych używanych w Twojej organizacji. Jeśli różne grupy bezpieczeństwa używają własnych zestawów plików wykonywalnych w swojej pracy, oddzielna kategoria może zostać utworzona dla każdej grupy bezpieczeństwa.

Dostępne instrukcje:

- Konsola administracyjna: Tworzenie kategorii aplikacji z zawartością dodaną ręcznie, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranych urządzeń, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranego folderu.
- Kaspersky Security Center Web Console: Tworzenie kategorii aplikacji z zawartością dodaną ręcznie, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranych urządzeń, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranego folderu.

3. **Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security**

   Skonfiguruj komponent Kontrola aplikacji w zasadzie Kaspersky Endpoint Security, korzystając z kategorii aplikacji, które utworzono w poprzednim kroku.

   Dostępne instrukcje:

   - Konsola administracyjna: Konfigurowanie zarządzania uruchamianiem aplikacji na urządzeniach klienckich
   - Kaspersky Security Center Web Console: Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows

4. **Konfigurowanie Kontroli aplikacji w zasadzie aplikacji Kaspersky Embedded Systems Security**

   Skonfiguruj komponent Kontrola aplikacji w zasadach Kaspersky Embedded Systems Security for Windows, korzystając z kategorii, które utworzyłeś/-aś. Aby uzyskać więcej informacji na temat komponentu Kontrola aplikacji, zapoznaj się z Pomocą Kaspersky Embedded Systems Security for Windows lub Pomocą Kaspersky Embedded Systems Security for Linux.

   Jeśli używasz dużej liczby reguł, może wystąpić błąd podczas ładowania zasady. Maksymalny rozmiar żądania w bajtach można zwiększyć, korzystając z następujących poleceń:

   - W przypadku żądania JSON:

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
     ```

   - W przypadku żądania HTTP:

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
     ```

     Gdzie `<max_request_size>` to maksymalny rozmiar żądania w bajtach (na przykład `200000000`).

5. **Włączanie komponentu Kontrola aplikacji w trybie testowym**

   Aby zapewnić, że reguły Kontroli aplikacji nie będą blokowały plików wykonywalnych wymaganych do pracy użytkownika, zalecane jest włączenie testowania reguł Kontroli aplikacji i analizowanie ich działania po utworzeniu nowych reguł. Po włączeniu testowania, Kaspersky Endpoint Security for Windows lub Kaspersky Embedded Systems Security nie zablokuje plików wykonywalnych, których uruchamianie jest zablokowane przez reguły Kontroli aplikacji, ale zamiast tego wyśle powiadomienia o ich uruchomieniu do Serwera administracyjnego.

   Podczas testowania reguł Kontroli aplikacji zalecane jest wykonanie następujących działań:

   - Określenie okresu testowania. Okres testowania może wahać się od siedmiu dni do dwóch miesięcy.
   - Sprawdź zdarzenia wynikające z testowania działania Kontroli aplikacji.

   Wskazówki jak postępować dla Kaspersky Security Center Web Console: Konfigurowanie komponentu Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Windows. Postępuj zgodnie z tymi instrukcjami i włącz opcję **Tryb testowy** w procesie konfiguracji.

6. **Zmienianie ustawień kategorii komponentu Kontrola aplikacji**

Jeśli to konieczne, wprowadź zmiany w ustawieniach Kontroli aplikacji. W oparciu o wyniki testu, możesz dodać pliki wykonywalne związane ze zdarzeniami komponentu Kontrola aplikacji do kategorii z zawartością dodaną ręcznie.

Dostępne instrukcje:

- Konsola administracyjna: Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji
- Kaspersky Security Center Web Console: Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

7. **Stosowanie reguł Kontroli aplikacji w trybie działania**

   Po przetestowaniu reguł Kontroli aplikacji i zakończeniu konfiguracji kategorii możesz zastosować reguły Kontroli aplikacji w trybie działania.

   Wskazówki jak postępować dla Kaspersky Security Center Web Console: Konfigurowanie komponentu Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Windows. Postępuj zgodnie z tymi instrukcjami i wyłącz opcję **Tryb testowy** w procesie konfiguracji.

8. **Weryfikowanie konfiguracji Kontroli aplikacji**

   Upewnij się, że wykonałeś następujące czynności:

   - Utworzono kategorie dla plików wykonywalnych.
   - Skonfigurowano Kontrolę aplikacji przy użyciu kategorii.
   - Zastosowałeś reguły Kontroli aplikacji w trybie działania.

Wyniki

Po zakończeniu scenariusza uruchamianie plików wykonywalnych na zarządzanych urządzeniach jest kontrolowane. Użytkownicy mogą uruchamiać tylko te pliki wykonywalne, które są dozwolone w Twojej organizacji, a nie mogą uruchamiać plików wykonywalnych, które są zabronione w Twojej organizacji.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Pomoc Kaspersky Embedded Systems Security for Windows
- Pomoc Kaspersky Embedded Systems Security for Linux

Tryby i kategorie Kontroli aplikacji

Komponent Kontrola aplikacji monitoruje próby uruchomienia plików wykonywalnych przez użytkowników. Za pomocą reguł Kontroli aplikacji możesz kontrolować uruchamianie plików wykonywalnych.

Komponent Kontrola aplikacji jest dostępny w programach Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security 11.2 for Linux i nowszych wersjach oraz Kaspersky Security for Virtualization Light Agent. Wszystkie instrukcje w tej sekcji opisują konfigurację Kontroli aplikacji dla Kaspersky Endpoint Security for Windows.

Uruchamianie plików wykonywalnych, których ustawienia nie odpowiadają żadnym regułom Kontroli aplikacji, jest regulowane przez wybrany tryb działania komponentu:

- *Lista zablokowanych*. Tryb jest używany, jeśli chcesz zezwolić na uruchamianie wszystkich plików wykonywalnych, za wyjątkiem plików określonych w regułach blokowania. Ten tryb jest wybrany domyślnie.
- *Lista zezwolonych*. Tryb jest używany, jeśli chcesz zablokować uruchamianie wszystkich plików wykonywalnych, z wyjątkiem plików określonych w regułach zezwalania.

Reguły Kontroli aplikacji są implementowane poprzez kategorie plików wykonywalnych. W Kaspersky Security Center istnieją trzy typy kategorii aplikacji:

- Ręcznie dodana kategoria z zawartością. Definiujesz warunki, na przykład, metadane plików, wartość skrótu pliku, certyfikat pliku, kategorię KL, ścieżkę do pliku, aby uwzględniać pliki wykonywalne w kategorii.
- Kategoria zawierająca pliki wykonywalne z wybranych urządzeń. Określasz urządzenie, którego pliki wykonywalne są automatycznie uwzględniane w kategorii.
- Kategoria zawierająca pliki wykonywalne z wybranego folderu. Określasz folder, z którego pliki wykonywalne mają zostać automatycznie uwzględnione w kategorii.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Pomoc Kaspersky Embedded Systems Security for Windows
- Pomoc Kaspersky Embedded Systems Security for Linux

Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

Listę plików wykonywalnych przechowywanych na urządzeniach klienckich można uzyskać w jeden z następujących sposobów:

- Włączenie powiadomień o uruchomieniu aplikacji w zasadach Kaspersky Endpoint Security.
- Tworzenie zadania inwentaryzacji.

Włączenie powiadomień o uruchomieniu aplikacji w zasadach Kaspersky Endpoint Security

Aby włączyć powiadomienia o uruchomieniu aplikacji:

1. Otwórz ustawienia zasad Kaspersky Endpoint Security, a następnie przejdź do **Ustawienia ogólne** → **Raporty i pliki danych**.
2. W grupie ustawień **Przesyłania danych do Serwera administracyjnego** zaznacz pole wyboru **Informacje o uruchomionych aplikacjach** i zapisz zmiany.

   Gdy użytkownik próbuje uruchomić pliki wykonywalne, informacje o tych plikach są dodawane do listy plików wykonywalnych na urządzeniu klienckim. Kaspersky Endpoint Security wysyła te informacje do Agenta sieciowego, a następnie Agent sieciowy wysyła je do Serwera administracyjnego.

Tworzenie zadania inwentaryzacji

Funkcja inwentaryzacji plików wykonywalnych jest dostępna dla następujących aplikacji:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux w wersji 11.2 i nowszych
- Kaspersky Security for Virtualization 4.0 Light Agent i nowsze wersje

Możesz zmniejszyć obciążenie bazy danych, jednocześnie uzyskując informacje o zainstalowanych aplikacjach. Aby zaoszczędzić miejsce, uruchom zadanie inwentaryzacji na urządzeniach referencyjnych, na których jest zainstalowany standardowy zestaw oprogramowania. Preferowana liczba urządzeń to od 1 do 3.

Zdecydowanie nie zalecamy uruchamiania zadania inwentaryzacji w przypadku korzystania z następujących baz danych: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (wszystkie edycje).

W celu utworzenia zadania dla plików wykonywalnych na urządzeniach klienckich:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.

   Zostanie wyświetlona lista zadań.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.

3. Na stronie **Ustawienia nowych zadań**, z listy rozwijanej **Aplikacja** wybierz Kaspersky Endpoint Security for Windows lub Kaspersky Endpoint Security for Linux, w zależności od typu systemu operacyjnego urządzeń klienckich.

4. Z listy rozwijalnej **Typ zadania** wybierz **Inwentaryzacja**.

5. Na stronie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**.

   Po zakończeniu działania Kreatora tworzenia nowego zadania, zostaje utworzone i skonfigurowane zadanie **Inwentaryzacja**. Jeśli chcesz, możesz zmienić ustawienia dla utworzonego zadania. Nowo utworzone zadanie będzie wyświetlane na liście zadań.

Szczegółowy opis zadania inwentaryzacji znajduje się w następujących Pomocach:

- Pomoc Kaspersky Endpoint Security for Windows
- Pomoc Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Po wykonaniu zadania **Inwentaryzacja**, zostaje utworzona lista plików wykonywalnych przechowywanych na zarządzanych urządzeniach i możesz przejrzeć listę.

Podczas inwentaryzacji mogą zostać wykryte pliki wykonywalne w następujących formatach (w zależności od opcji wybranej we właściwościach zadania inwentaryzacji): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR i HTML.

Przeglądanie listy plików wykonywalnych, przechowywanych na zarządzanych urządzeniach

W celu przejrzenia listy plików wykonywalnych przechowywanych na urządzeniach klienckich:

W menu głównym przejdź do **Operacje → Aplikacje innych firm → Pliki wykonywalne**.

Strona wyświetla listę plików wykonywalnych przechowywanych na urządzeniach klienckich.

W razie potrzeby możesz wysłać plik wykonywalny zarządzanego urządzenia na urządzenie, na którym otwarta jest Kaspersky Security Center Web Console.

Aby wysłać plik wykonywalny:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Pliki wykonywalne**.

2. Zaznacz odnośnik do pliku wykonywalnego, który chcesz wysłać.

3. W oknie, które zostanie otwarte, przejdź do sekcji **Urządzenia**, a następnie zaznacz pole wyboru zarządzanego urządzenia, z którego chcesz wysłać plik wykonywalny.

   Przed wysłaniem pliku wykonywalnego upewnij się, że zarządzane urządzenie ma bezpośrednie połączenie z Serwerem administracyjnym, zaznaczając pole wyboru **Nie odłączaj od Serwera administracyjnego**.

4. Kliknij przycisk **Wyślij**.

   Wybrany plik wykonywalny zostanie pobrany w celu dalszego wysłania na urządzenie, na którym otwarta jest Kaspersky Security Center Web Console.

Tworzenie kategorii aplikacji z zawartością dodaną ręcznie

Możesz określić zestaw kryteriów jako szablon plików wykonywalnych, dla których chcesz zezwolić na lub zablokować uruchamianie w Twojej organizacji. W oparciu o pliki wykonywalne odpowiadające kryteriom, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii aplikacji z zawartością dodaną ręcznie:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Kategorie aplikacji**.

   Zostanie wyświetlona strona z listą kategorii aplikacji.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. W kroku **Wybierz metodę tworzenia kategorii** wybierz opcję **Kategoria z zawartością dodaną ręcznie. Dane plików wykonywalnych są dodawane do tej kategorii ręcznie**.

4. W kroku **Warunki** kliknij przycisk **Dodaj**, aby dodać kryterium warunku do uwzględnienia plików w tworzonej kategorii.

5. W kroku **Kryteria warunku** wybierz typ reguły dla tworzenia kategorii z listy:

   - **Z kategorii KL**

     Jeśli ta opcja jest zaznaczona, możesz określić kategorię aplikacji Kaspersky jako warunek dodania aplikacji do kategorii użytkownika. Aplikacje z określonej kategorii Kaspersky zostaną dodane do kategorii użytkownika dla aplikacji.

   - **Wybierz certyfikat z repozytorium**

     Jeśli ta opcja jest zaznaczona, możesz określić certyfikaty z repozytorium. Warunek kategorii obejmuje tylko pliki wykonywalne podpisane określonym certyfikatem.

     Certyfikaty są dodawane do repozytorium, jeśli utworzono i uruchomiono zadanie inwentaryzacji lub zaznaczono pole wyboru **Informacje o uruchomionych aplikacjach** w profilu Kaspersky Endpoint Security. Możesz wykonać obie czynności.

     Informacje o certyfikatach można wyodrębnić tylko z plików wykonywalnych w formacie PE (.exe, .dll, .sys).

- **Określ ścieżkę do aplikacji (maski są obsługiwane)**

  Jeżeli ta opcja zostanie zaznaczona, możesz określić ścieżkę do pliku lub folderu na urządzeniu klienckim zawierający pliki wykonywalne, które zostaną dodane do kategorii użytkownika dla aplikacji. Można użyć wyrażeń regularnych, takich jak *C:\path_to_exe*.*, na przykład: *C:\Program Files\Internet Explorer*.*

- **Dysk wymienny**

  Jeżeli ta opcja jest zaznaczona, możesz określić typ nośnika (dowolny dysk lub dysk wymienny), na którym aplikacja jest uruchomiona. Aplikacje, które były uruchomione na wybranym typie urządzenia, zostaną dodane do kategorii użytkownika dla aplikacji.

- **Suma kontrolna, metadane lub certyfikat**:

  - **Wybierz z listy plików wykonywalnych**

    Jeśli ta opcja jest zaznaczona, możesz wskazać na liście plików wykonywalnych na urządzeniu klienckim te aplikacje, które chcesz dodać do kategorii.

  - **Wybierz z rejestru aplikacji**

    Jeśli ta opcja jest wybrana, zostanie wyświetlony rejestr aplikacji. Po wybraniu aplikacji z rejestru otwiera się okno z parametrami wypełnionymi metadanymi wybranej aplikacji:

    - Nazwa pliku.
    - Wersja pliku. Możesz określić dokładną wartość wersji lub opisać warunek, na przykład „większy niż 5.0”.
    - Nazwa aplikacji.
    - Wersja aplikacji. Możesz określić dokładną wartość wersji lub opisać warunek, na przykład „większy niż 5.0”.
    - Producent.

    Należy pamiętać, że zablokowane zostanie wyłącznie uruchomienie plików wykonywalnych spełniających określone parametry, a nie uruchomienie wybranej aplikacji. Jeśli wybrane metadane aplikacji odpowiadają metadanym pliku wykonywalnego uruchamianego po uruchomieniu aplikacji, możesz przejść do następnego kroku. W przeciwnym razie należy ręcznie zmienić wartości, aby odpowiadały metadanym pliku wykonywalnego.

  - **Określ ręcznie**

    Jeśli ta opcja jest zaznaczona, możesz określić hash pliku lub metadane lub certyfikat jako warunek dodawania aplikacji do kategorii użytkownika.

    Suma kontrolna pliku

    W zależności od wersji aplikacji zabezpieczającej, zainstalowanej na urządzeniach w sieci, musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w tej kategorii. Informacje o wartościach sumy kontrolnej obliczonych przez funkcje skrótu są przechowywane w bazie danych Serwera administracyjnego.

    SHA256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono luk, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje obsługują obliczanie SHA256. Obliczanie funkcji skrótu MD5 jest obsługiwane przez wszystkie wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w kategorii:

- Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowanych w Twojej sieci to Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowsze wersje, zaznacz pole **SHA256**. Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Może to spowodować błędy w działaniu aplikacji zabezpieczającej. W takim przypadku można użyć kryptograficznej funkcji skrótu MD5 dla plików kategorii.

- Jeśli w Twojej sieci są zainstalowane wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, wybierz **Suma kontrolna MD5**. Nie można dodać kategorii, która została utworzona na podstawie kryterium sumy kontrolnej MD5 pliku wykonywalnego dla Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowszych wersji. W takim przypadku można użyć kryptograficznej funkcji skrótu SHA256 dla plików kategorii.

- Jeśli różne urządzenia w Twojej sieci używają zarówno wcześniejszych, jak i nowszych wersji Kaspersky Endpoint Security 10, zaznacz zarówno pole **SHA256**, jak i pole wyboru skrótu **Suma kontrolna MD5**.

Metadane

Jeśli ta opcja jest wybrana, możesz określić metadane pliku jako nazwę pliku, wersję pliku, producenta. Warunek kategorii obejmuje tylko pliki wykonywalne z takimi samymi metadanymi.

Certyfikat

Jeśli ta opcja jest zaznaczona, możesz określić certyfikaty z repozytorium. Warunek kategorii obejmuje tylko pliki wykonywalne podpisane określonym certyfikatem.

Certyfikaty są dodawane do repozytorium, jeśli utworzono i uruchomiono zadanie inwentaryzacji lub zaznaczono pole wyboru **Informacje o uruchomionych aplikacjach** w profilu Kaspersky Endpoint Security. Możesz wykonać obie czynności.

- **Z pliku lub z pakietu MSI/zarchiwizowanego folderu**

  Jeśli ta opcja jest zaznaczona, możesz określić plik instalatora MSI jako warunek dodania aplikacji do kategorii użytkownika. Metadane instalatora aplikacji zostaną przesłane do Serwera administracyjnego. Aplikacje, dla których metadane instalatora są takie same jak dla określonego instalatora MSI, zostaną dodane do kategorii użytkownika dla aplikacji.

Wybrane kryterium zostanie dodane do listy warunków.

Możesz dodać tyle kryteriów tworzenia kategorii aplikacji, ile potrzebujesz.

6. W kroku **Wykluczenia** kliknij przycisk **Dodaj**, aby dodać kryterium warunku wykluczenia w celu wykluczenia plików z tworzonej kategorii.

7. W kroku **Kryteria warunku** wybierz typ reguły z listy w taki sam sposób, w jaki wybierałeś typ reguły dla tworzenia kategorii.

Jeśli kreator zakończy działanie, zostanie utworzona kategoria aplikacji. Jest wyświetlana na liście kategorii aplikacji. Po skonfigurowaniu Kontroli aplikacji możesz użyć utworzonej kategorii aplikacji.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

- Pomoc Kaspersky Embedded Systems Security for Windows
- Pomoc Kaspersky Embedded Systems Security for Linux

Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń

Możesz użyć plików wykonywalnych z wybranych urządzeń jako szablonu plików wykonywalnych, które chcesz zablokować lub na które chcesz zezwolić. W oparciu o pliki wykonywalne z wybranych urządzeń, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

Aby pobrać listę plików wykonywalnych z urządzeń:

1. Upewnij się, że została utworzona i jest aktywna zasada Kaspersky Endpoint Security for Windows lub Kaspersky Endpoint Security for Linux. Włącz komponent Kontrola aplikacji w zasadzie.
2. Uzyskaj listę plików wykonywalnych przechowywanych na urządzeniach klienckich.

Aby utworzyć kategorię aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Kategorie aplikacji**.

   Zostanie wyświetlona strona z listą kategorii.
2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.
3. W kroku **Wybierz metodę tworzenia kategorii** określ nazwę kategorii i wybierz opcję **Kategoria zawierająca pliki wykonywalne znajdujące się na wybranych urządzeniach. Takie pliki wykonywalne są przetwarzane automatycznie, a ich metryki są dodawane do kategorii**.
4. Kliknij **Dodaj**.
5. W otwartym oknie wybierz urządzenie lub urządzenia, których pliki wykonywalne będą używane do tworzenia kategorii aplikacji.
6. Określ następujące ustawienia:

   - **Algorytm obliczania wartości sumy kontrolnej**

     W zależności od wersji aplikacji zabezpieczającej, zainstalowanej na urządzeniach w sieci, musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w tej kategorii. Informacje o wartościach sumy kontrolnej obliczonych przez funkcje skrótu są przechowywane w bazie danych Serwera administracyjnego.

     SHA256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono luk, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje obsługują obliczanie SHA256. Obliczanie funkcji skrótu MD5 jest obsługiwane przez wszystkie wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w kategorii:

- Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowanych w Twojej sieci to Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowsze wersje, zaznacz pole **SHA256**. Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Może to spowodować błędy w działaniu aplikacji zabezpieczającej. W takim przypadku można użyć kryptograficznej funkcji skrótu MD5 dla plików kategorii.

- Jeśli w Twojej sieci są zainstalowane wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, wybierz **Suma kontrolna MD5**. Nie można dodać kategorii, która została utworzona na podstawie kryterium sumy kontrolnej MD5 pliku wykonywalnego dla Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowszych wersji. W takim przypadku można użyć kryptograficznej funkcji skrótu SHA256 dla plików kategorii.

Jeśli różne urządzenia w Twojej sieci używają zarówno wcześniejszych, jak i nowszych wersji Kaspersky Endpoint Security 10, zaznacz zarówno pole **SHA256**, jak i pole wyboru skrótu **Suma kontrolna MD5**.

Pole **Oblicz SHA256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje)** jest zaznaczone domyślnie.

Pole **Przelicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane w wersjach starszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** jest odznaczone domyślnie.

- **Synchronizuj dane z repozytorium Serwera administracyjnego**

  Wybierz tę opcję, jeśli chcesz, żeby Serwer administracyjny okresowo sprawdzał zmiany w określonym folderze (lub folderach).

  Domyślnie opcja ta jest wyłączona.

  Jeśli włączysz tę opcję, określ przedział czasu (w godzinach), aby sprawdzić zmiany w określonym folderze (folderach). Domyślnie przedział czasu skanowania wynosi 24 godziny.

- **Typ pliku**

  W tej sekcji możesz określić typ pliku, który jest używany do tworzenia kategorii aplikacji.

  Wszystkie pliki. Wszystkie pliki są brane pod uwagę podczas tworzenia kategorii. Domyślnie opcja ta jest zaznaczona.

  Tylko pliki spoza kategorii aplikacji. Tylko pliki poza kategoriami aplikacji są brane pod uwagę podczas tworzenia kategorii.

- **Foldery**

  W tej sekcji możesz określić, które foldery z wybranego urządzenia (urządzeń) zawierają pliki używane do tworzenia kategorii aplikacji.

  Wszystkie foldery. Wszystkie foldery są brane pod uwagę podczas tworzenia kategorii. Domyślnie opcja ta jest zaznaczona.

  Określony folder. Tylko określony folder jest brany pod uwagę podczas tworzenia kategorii. Jeśli wybierzesz tę opcję, musisz określić ścieżkę do folderu.

Po zakończeniu działania kreatora tworzona jest kategoria plików wykonywalnych. Jest wyświetlana na liście kategorii. W przypadku konfigurowania Kontroli aplikacji możesz użyć utworzonej kategorii.

Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranego folderu

Możesz użyć plików wykonywalnych z wybranego folderu jako standardu plików wykonywalnych, które chcesz zablokować lub na które chcesz zezwolić w swojej organizacji. W oparciu o pliki wykonywalne z wybranego folderu, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii, która zawiera pliki wykonywalne z wybranego folderu:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Kategorie aplikacji**.

   Zostanie wyświetlona strona z listą kategorii.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

3. W kroku **Wybierz metodę tworzenia kategorii** kreatora określ nazwę kategorii i wybierz opcję **Kategoria, która zawiera pliki wykonywalne z określonego folderu. Pliki wykonywalne aplikacji skopiowane do określonego folderu są przetwarzane automatycznie, a ich metryki są dodawane do kategorii**.

4. Określ folder, którego pliki wykonywalne zostaną użyte do utworzenia kategorii.

5. Określ następujące ustawienia:

   - **Uwzględnij w tej kategorii biblioteki dołączane dynamicznie (DLL)**

     Kategoria aplikacji zawiera biblioteki dołączane dynamicznie (pliki w formacie DLL), a składnik Kontrola aplikacji rejestruje akcje takich bibliotek działających w systemie. Włączenie plików DLL do kategorii może obniżyć wydajność Kaspersky Security Center.

     Domyślnie pole to nie jest zaznaczone.

   - **Uwzględnij w tej kategorii dane skryptów**

     Kategoria aplikacji zawiera dane o skryptach, a skrypty nie są blokowane przez moduł Ochrona WWW. Włączenie danych skryptów do kategorii może obniżyć wydajność Kaspersky Security Center.

     Domyślnie pole to nie jest zaznaczone.

   - **Algorytm obliczania wartości sumy kontrolnej**: **Oblicz sumy SHA256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze) / Oblicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane przez starsze wersje niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

     W zależności od wersji aplikacji zabezpieczającej, zainstalowanej na urządzeniach w sieci, musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w tej kategorii. Informacje o wartościach sumy kontrolnej obliczonych przez funkcje skrótu są przechowywane w bazie danych Serwera administracyjnego.

     SHA256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono luk, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje obsługują obliczanie SHA256. Obliczanie funkcji skrótu MD5 jest obsługiwane przez wszystkie wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w kategorii:

- Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowanych w Twojej sieci to Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowsze wersje, zaznacz pole **SHA256**. Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Może to spowodować błędy w działaniu aplikacji zabezpieczającej. W takim przypadku można użyć kryptograficznej funkcji skrótu MD5 dla plików kategorii.

- Jeśli w Twojej sieci są zainstalowane wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, wybierz **Suma kontrolna MD5**. Nie można dodać kategorii, która została utworzona na podstawie kryterium sumy kontrolnej MD5 pliku wykonywalnego dla Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowszych wersji. W takim przypadku można użyć kryptograficznej funkcji skrótu SHA256 dla plików kategorii.

Jeśli różne urządzenia w Twojej sieci używają zarówno wcześniejszych, jak i nowszych wersji Kaspersky Endpoint Security 10, zaznacz zarówno pole **SHA256**, jak i pole wyboru skrótu **Suma kontrolna MD5**.

Pole **Oblicz SHA256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje)** jest zaznaczone domyślnie.

Pole **Oblicz MD5 plików należących do tej kategorii (obsługiwane w wersjach starszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** jest odznaczone domyślnie.

- **Wymuś skanowanie folderu pod kątem zmian**

  Jeśli ta opcja jest włączona, aplikacja regularnie sprawdza folder dodawania zawartości kategorii na obecność zmian. Możesz określić częstotliwość skanowań (w godzinach) w polu wejściowym znajdującym się obok pola do zaznaczenia. Domyślnie przedział czasu między wymuszonymi skanowaniami wynosi 24 godziny.

  Jeśli ta opcja jest wyłączona, aplikacja nie wymusza skanowania folderu. Serwer podejmie próbę uzyskania dostępu do plików, jeśli zostały zmodyfikowane, dodane lub usunięte.

  Domyślnie opcja ta jest wyłączona.

Po zakończeniu działania kreatora tworzona jest kategoria plików wykonywalnych. Jest wyświetlana na liście kategorii. Podczas konfiguracji Kontroli aplikacji możesz użyć kategorii.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Pomoc Kaspersky Embedded Systems Security for Windows
- Pomoc Kaspersky Embedded Systems Security for Linux

Przeglądanie listy kategorii aplikacji

Możesz przejrzeć listę konfigurowanych kategorii plików wykonywalnych i ustawień każdej kategorii.

W celu przejrzenia listy kategorii aplikacji:

W menu głównym przejdź do **Operacje → Aplikacje innych firm → Kategorie aplikacji**.

Zostanie wyświetlona strona z listą kategorii.

W celu przejrzenia właściwości kategorii aplikacji:

Kliknij nazwę kategorii.

Zostanie wyświetlone okno właściwości kategorii. Właściwości zostaną pogrupowane na kilku zakładkach.

Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

Po skonfigurowaniu Kontroli aplikacji w zasadach Kaspersky Endpoint Security for Windows, na liście zdarzeń zostaną wyświetlone następujące zdarzenia:

- **Zablokowano uruchomienie aplikacji** (zdarzenie *Krytyczne*). To zdarzenie jest wyświetlane, jeśli skonfigurowałeś Kontrolę aplikacji do stosowania reguł.
- **Zablokowane uruchomienie aplikacji w trybie testowym** (zdarzenie *Informacje*). To zdarzenie jest wyświetlane, jeśli skonfigurowałeś Kontrolę aplikacji do testowania reguł.
- **Wiadomość do administratora o zakazie uruchamiania aplikacji** (zdarzenie *ostrzegawcze*). To zdarzenie jest wyświetlane, jeśli skonfigurowałeś Kontrolę aplikacji do stosowania reguł i użytkownik zażądał dostępu do aplikacji, która jest zablokowana podczas uruchamiania.

Zalecane jest utworzenie wyborów zdarzeń, aby przeglądać zdarzenia dotyczące działania Kontroli aplikacji.

Możesz dodać pliki wykonywalne dotyczące zdarzeń Kontroli aplikacji do istniejącej kategorii aplikacji lub do nowej kategorii aplikacji. Możesz dodać pliki wykonywalne tylko do kategorii aplikacji z zawartością dodaną ręcznie.

W celu dodania plików wykonywalnych związanych ze zdarzeniami Kontroli aplikacji do kategorii aplikacji:

1. W menu głównym przejdź do **Monitorowanie i raportowanie → Wybory zdarzeń**.

   Zostanie wyświetlona lista wyborów zdarzeń.

2. Wybierz wybór zdarzeń, aby przeglądać zdarzenia związane z Kontrolą aplikacji oraz uruchomić ten wybór zdarzeń.

   Jeśli nie utworzyłeś wyboru zdarzeń dotyczącego Kontroli aplikacji, możesz wybrać i uruchomić predefiniowany wybór, na przykład, **Ostatnie zdarzenia**.

   Zostanie wyświetlona lista zdarzeń.

3. Wybierz zdarzenia, których skojarzone pliki wykonywalne chcesz dodać do kategorii aplikacji, a następnie kliknij przycisk **Przypisz do kategorii**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

4. W kroku kreatora określ odpowiednie ustawienia:

   - W sekcji **Akcja na pliku wykonywalnym związanym ze zdarzeniem** wybierz jedną z następujących opcji:

     - **Dodaj do nowej kategorii aplikacji**

       Wybierz tę opcję, jeśli chcesz utworzyć nową kategorię aplikacji w oparciu o pliki wykonywalne dotyczące zdarzeń.

       Domyślnie opcja ta jest zaznaczona.

Jeśli wybrałeś tę opcję, określ nową nazwę kategorii.

- **Dodaj do istniejącej kategorii aplikacji**

  Wybierz tę opcję, jeśli chcesz dodać pliki wykonywalne dotyczące zdarzeń do istniejącej kategorii aplikacji.

  Domyślnie ta opcja nie jest zaznaczona.

  Jeśli wybrałeś tę opcję, wybierz kategorię aplikacji z zawartością dodaną ręcznie, do której chcesz dodać pliki wykonywalne.

- W sekcji **Typ reguły** wybierz jedną z następujących opcji:

  - **Reguły dodawania do włączeń**

  - **Reguły dodawania do wykluczeń**

- W sekcji **Parametr użyty jako warunek** wybierz jedną z następujących opcji:

  - **Szczegóły certyfikatu (lub sumy kontrolne SHA256 dla plików bez certyfikatu)**

    Pliki mogą być podpisane certyfikatem. Kilka plików może być podpisanych tym samym certyfikatem. Na przykład, różne wersje tej samej aplikacji mogą być podpisane tym samym certyfikatem lub kilka różnych aplikacji od tego samego producenta może być podpisanych tym samym certyfikatem. Jeśli wybierzesz certyfikat, kilka wersji aplikacji lub kilka aplikacji od tego samego producenta może zostać przydzielonych do kategorii.

    Każdy plik posiada swoją unikatową funkcję skrótu SHA256. Jeśli wybierzesz funkcję skrótu SHA256, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

    Wybierz tę opcję, jeśli chcesz dodać do reguł kategorii szczegóły certyfikatu pliku wykonywalnego (lub funkcję skrótu SHA256 dla plików bez certyfikatu).

    Domyślnie opcja ta jest zaznaczona.

  - **Szczegóły certyfikatu (pliki bez certyfikatu zostaną pominięte)**

    Pliki mogą być podpisane certyfikatem. Kilka plików może być podpisanych tym samym certyfikatem. Na przykład, różne wersje tej samej aplikacji mogą być podpisane tym samym certyfikatem lub kilka różnych aplikacji od tego samego producenta może być podpisanych tym samym certyfikatem. Jeśli wybierzesz certyfikat, kilka wersji aplikacji lub kilka aplikacji od tego samego producenta może zostać przydzielonych do kategorii.

    Wybierz tę opcję, jeśli chcesz dodać szczegóły certyfikatu pliku wykonywalnego do reguł kategorii. Jeśli plik wykonywalny nie posiada certyfikatu, ten plik zostanie pominięty. Do kategorii nie zostaną dodane żadne informacje o tym pliku.

  - **Tylko SHA256 (pliki bez sumy kontrolnej zostaną pominięte)**

    Każdy plik posiada swoją unikatową funkcję skrótu SHA256. Jeśli wybierzesz funkcję skrótu SHA256, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

    Wybierz tę opcję, jeśli chcesz dodać tylko szczegóły funkcji skrótu SHA256 pliku wykonywalnego.

  - **Tylko MD5 (tryb wycofany, wyłącznie dla wersji Kaspersky Endpoint Security 10 Service Pack 1)**

    Każdy plik posiada swoją unikatową funkcję skrótu MD5. Jeśli wybierzesz funkcję skrótu MD5, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

    Wybierz tę opcję, jeśli chcesz dodać tylko szczegóły funkcji skrótu MD5 pliku wykonywalnego. Obliczanie funkcji skrótu MD5 jest obsługiwane w Kaspersky Endpoint Security 10 Service Pack 1 for Windows i późniejszych wersjach.

5. Kliknij **OK**.

   Jeśli kreator zakończy działanie, pliki wykonywalne dotyczące zdarzeń Kontroli aplikacji są dodawane do istniejącej kategorii aplikacji lub do nowej kategorii aplikacji. Możesz przejrzeć ustawienia kategorii aplikacji, które zmodyfikowałeś lub utworzyłeś.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Pomoc Kaspersky Embedded Systems Security for Windows
- Pomoc Kaspersky Embedded Systems Security for Linux

Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows

Po utworzeniu kategorii Kontroli aplikacji możesz użyć ich do konfigurowania Kontroli aplikacji w zasadach Kaspersky Endpoint Security for Windows.

W celu skonfigurowania Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.

   Zostanie wyświetlona lista zasad.

2. Kliknij zasadę **Kaspersky Endpoint Security for Windows**.

   Zostanie otwarte okno ustawień zasady.

3. Przejdź do **Ustawienia aplikacji** → **Kontrola bezpieczeństwa** → Kontrola **aplikacji**.

   Zostanie wyświetlone okno **Kontrola aplikacji** z ustawieniami Kontroli aplikacji.

4. Opcja **Kontrola aplikacji** jest domyślnie włączona. Upewnij się, że przycisk przełączania **WYŁĄCZONA Kontroli aplikacji** jest ustawiony w pozycji wyłączonej.

5. W ustawieniach blokowania **Ustawienia Kontroli aplikacji** włącz tryb działania, aby zastosować reguły Kontroli aplikacji i zezwól Kaspersky Endpoint Security for Windows na blokowanie uruchamiania aplikacji.

   Jeśli chcesz przetestować reguły Kontroli aplikacji, w sekcji **Ustawienia Kontroli aplikacji** włącz tryb testowy. W trybie testowym Kaspersky Endpoint Security for Windows nie blokuje uruchamiania aplikacji, ale rejestruje informacje o wyzwolonych regułach w raporcie. Kliknij łącze **Wyświetl raport**, aby wyświetlić te informacje.

6. Włącz opcję **Kontrola wczytywania modułów DLL**, jeśli chcesz, żeby program Kaspersky Endpoint Security for Windows monitorował wczytywanie modułów DLL, gdy aplikacje są uruchamiane przez użytkowników.

   Informacje o module i aplikacji, która wczytuje moduł, zostaną zapisane w raporcie.

   Kaspersky Endpoint Security for Windows monitoruje tylko moduły DLL i sterowniki wczytywane po wybraniu opcji **Kontrola wczytywania modułów DLL**. Uruchom ponownie urządzenie po wybraniu opcji **Kontrola wczytywania modułów DLL**, jeśli chcesz, żeby program Kaspersky Endpoint Security for Windows monitorował wszystkie moduły DLL i sterowniki, w tym te wczytywane przed uruchomieniem Kaspersky Endpoint Security for Windows.

7. (Opcjonalne) W sekcji **Szablony wiadomości** zmień szablon wiadomości, która jest wyświetlana po zablokowaniu możliwości uruchomienia aplikacji, oraz szablon wiadomości e-mail, która jest wysyłana do Ciebie.

8. W ustawieniach sekcji **Tryb Kontroli aplikacji** wybierz tryb **Lista zablokowanych** lub **Lista zezwolonych**.

   Domyślnie, wybrany jest tryb **Lista zablokowanych**.

9. Kliknij odnośnik **Ustawienia list reguł**.

   Zostanie otwarte okno **Lista zablokowanych i lista zezwolonych**, w którym można dodać kategorię aplikacji. Domyślnie, wybrana jest zakładka **Lista zablokowanych**, jeśli wybrany jest tryb **Lista zablokowanych** lub wybrana jest zakładka **Lista zezwolonych**, jeśli wybrany jest tryb **Lista zezwolonych**.

10. W oknie **Lista zablokowanych i lista zezwolonych** kliknij przycisk **Dodaj**.

    Zostanie otwarte okno **Reguła Kontroli aplikacji**.

11. Kliknij łącze **Wybierz kategorię**.

    Zostanie otwarte okno **Kategoria aplikacji**.

12. Dodaj kategorię (lub kategorie) aplikacji, które utworzyłeś wcześniej.

    Możesz edytować ustawienia utworzonej kategorii, klikając przycisk **Edytuj**.

    Możesz utworzyć nową kategorię, klikając przycisk **Dodaj**.

    Możesz usunąć kategorię z listy, klikając przycisk **Usuń**.

13. Po zakończeniu tworzenia listy kategorii aplikacji, kliknij przycisk **OK**.

    Okno **Kategoria aplikacji** zostanie zamknięte.

14. W oknie reguły **Kontrola aplikacji**, w sekcji **Użytkownicy i ich uprawnienia** utwórz listę użytkowników i grup użytkowników do zastosowania reguły Kontroli aplikacji.

15. Aby zapisać ustawienia i zamknąć okno **Reguła Kontroli aplikacji**, kliknij przycisk **OK**.

16. Aby zapisać ustawienia i zamknąć okno **Lista zablokowanych i lista zezwolonych**, kliknij przycisk **OK**.

17. Aby zapisać ustawienia i zamknąć okno **Kontrola aplikacji**, kliknij przycisk **OK**.

18. Zamknij okno z ustawieniami zasady Kaspersky Endpoint Security for Windows.

Kontrola aplikacji została skonfigurowana. Po przeniesieniu zasady na urządzenia klienckie, możliwe jest zarządzanie uruchamianiem plików wykonywalnych.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Pomoc Kaspersky Embedded Systems Security for Windows
- Pomoc Kaspersky Embedded Systems Security for Linux

Uzyskiwanie i przeglądanie listy aplikacji zainstalowanych na urządzeniach klienckich

Kaspersky Security Center przeprowadza inwentaryzację wszystkich programów zainstalowanych na zarządzanych urządzeniach klienckich działających pod kontrolą systemu Linux i Windows.

Agent sieciowy tworzy listę aplikacji zainstalowanych na urządzeniu, a następnie wysyła ją do Serwera administracyjnego. Aktualizacja listy aplikacji przez Agenta sieciowego zajmuje około 10–15 minut.

W przypadku urządzeń klienckich z systemem Windows Agent sieciowy otrzymuje większość informacji o zainstalowanych aplikacjach z rejestru systemu Windows. W przypadku urządzeń klienckich opartych na systemie Linux menedżery pakietów dostarczają Agentowi sieciowemu informacje o zainstalowanych aplikacjach.

Jeśli aplikacja z sekcji **Rejestr aplikacji** została wykryta na urządzeniu z systemem Linux, właściwości aplikacji nie zawierają informacji o powiązanych plikach wykonywalnych.

W celu przejrzenia listy aplikacji zainstalowanych na zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje** → **Aplikacje innych firm** → **Rejestr aplikacji**.

   Strona wyświetla tabelę z aplikacjami zainstalowanymi na zarządzanych urządzeniach. Wybierz aplikację, aby wyświetlić jej właściwości, na przykład nazwę dostawcy, numer wersji, listę plików wykonywalnych, listę urządzeń, na których aplikacja jest zainstalowana, listę dostępnych aktualizacji oprogramowania oraz listę wykrytych luk w oprogramowaniu.

2. Możesz grupować i filtrować dane tabeli z zainstalowanymi aplikacjami w następujący sposób:

   - Kliknij ikonę ustawień ( ) w prawym górnym rogu tabeli.

     W wywołanym menu **Ustawienia kolumn** wybierz kolumny, które mają być wyświetlane w tabeli. Aby wyświetlić typ systemu operacyjnego urządzeń klienckich, na których zainstalowana jest aplikacja, wybierz kolumnę **Typ systemu operacyjnego**.

   - Kliknij ikonę filtra ( ) w prawym górnym rogu tabeli, a następnie określić i zastosować kryterium filtrowania w wywołanym menu.

     Zostanie wyświetlona przefiltrowana tabela zainstalowanych aplikacji.

Aby wyświetlić listę aplikacji zainstalowanych na określonym zarządzanym urządzeniu,

W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia** → **<nazwa urządzenia>** → **Zaawansowane** → **Rejestr aplikacji**. Z tego menu możesz wyeksportować listę aplikacji do pliku CSV lub pliku TXT.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Pomoc Kaspersky Embedded Systems Security for Windows
- Pomoc Kaspersky Embedded Systems Security for Linux

Tworzenie pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky

Kaspersky Security Center Web Console pozwala na zdalną instalację aplikacji firm trzecich przy użyciu pakietów instalacyjnych. Takie aplikacje innych firm są zawarte w dedykowanej bazie danych Kaspersky. Baza danych jest tworzona automatycznie, gdy uruchamiasz zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* po raz pierwszy.

W celu utworzenia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**.
2. Kliknij przycisk **Dodaj**.
3. Na otwartej stronie Kreatora nowego pakietu wybierz opcję **Wybierz aplikację z bazy danych Kaspersky do utworzenia pakietu instalacyjnego**, a następnie kliknij **Dalej**.
4. Na liście aplikacji, która zostanie otwarta, wybierz odpowiednią aplikację, a następnie kliknij **Dalej**.
5. Wybierz odpowiedni język lokalizacji z listy rozwijanej, a następnie kliknij **Dalej**.

   Ten krok jest wyświetlany tylko wtedy, gdy aplikacja umożliwia wybór opcji językowych.

6. Jeśli pojawi się monit o zaakceptowanie umowy licencyjnej na instalację, na stronie **Umowa licencyjna użytkownika końcowego**, która zostanie otwarta, kliknij odnośnik, aby przeczytać umowę licencyjną w witrynie internetowej dostawcy, a następnie wybierz pole wyboru **Potwierdzam, że w pełni przeczytałem(-am), rozumiem i akceptuję warunki niniejszej Umowy licencyjnej użytkownika końcowego**.
7. Na stronie **Nazwa nowego pakietu instalacyjnego**, która zostanie otwarta, w polu **Nazwa pakietu** wprowadź nazwę pakietu instalacyjnego i kliknij **Dalej**.

Poczekaj, aż nowo utworzony pakiet instalacyjny zostanie przesłany na Serwer administracyjny. Jeśli Kreator tworzenia nowego pakietu wyświetla wiadomość informującą, że proces tworzenia pakietu zakończył się pomyślnie, kliknij **Zakończ**.

Nowo utworzony pakiet instalacyjny pojawi się na liście pakietów instalacyjnych. Możesz wybrać ten pakiet podczas tworzenia lub ponownego konfigurowania zadania *Zdalna instalacja aplikacji*.

Przeglądanie i modyfikowanie ustawienia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky

Jeśli poprzednio utworzyłeś jakiekolwiek pakiety instalacyjne aplikacji innych firm znajdujące się w bazie danych Kaspersky, możesz przejrzeć i zmodyfikować ustawienia tych pakietów.

Modyfikowanie ustawień pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky jest dostępne tylko w licencji Zarządzanie lukami i poprawkami.

W celu przejrzenia i zmodyfikowania ustawień pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**.
2. Na otwartej liście pakietów instalacyjnych kliknij nazwę odpowiedniego pakietu.
3. Na otwartej stronie właściwości zmodyfikuj ustawienia (jeśli jest to konieczne).
4. Kliknij przycisk **Zapisz**.

Zmodyfikowane ustawienia zostaną zapisane.

Ustawienia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky

Ustawienia pakietu instalacyjnego aplikacji innej firmy są pogrupowane na następujących zakładkach:

Tylko część ustawień wymienionych poniżej jest wyświetlana domyślnie, więc możesz dodać odpowiednie kolumny, klikając przycisk **Filtr** i wybierając nazwy odpowiednich kolumn z listy.

- Zakładka **Ogólne**:
  - Pole wejściowe które zawiera nazwę pakietu instalacyjnego, który może zostać edytowany ręcznie
  - **Aplikacja**

    Nazwa aplikacji innej firmy, dla której tworzony jest pakiet instalacyjny.
  - **Wersja**

    Numer wersji aplikacji innej firmy, dla której tworzony jest pakiet instalacyjny.
  - **Rozmiar**

    Rozmiar pakietu instalacyjnego innej firmy (w kilobajtach).
  - **Utworzono**

    Data i godzina utworzenia pakietu instalacyjnego innej firmy.
  - **Ścieżka dostępu**

    Ścieżka do folderu sieciowego, w którym przechowywany jest pakiet instalacyjny innej firmy.
- Zakładka **Procedura instalacji**:
  - **Zainstaluj wymagane ogólne składniki systemu**

    Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

    Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

Domyślnie opcja ta jest wyłączona.

- Tabela która wyświetla właściwości aktualizacji i zawierająca następujące kolumny:
  - **Nazwa**

    Nazwa aktualizacji.

  - **Opis**

    Opis aktualizacji.

  - **Źródło**

    Źródło aktualizacji, czyli czy została ona wydana przez firmę Microsoft, czy przez inną niezależną firmę.

  - **Typ**

    Rodzaj aktualizacji, czyli czy jest przeznaczona dla sterownika czy aplikacji.

  - **Kategoria**

    Kategoria Windows Server Update Services (WSUS) wyświetlana dla aktualizacji firmy Microsoft (aktualizacje krytyczne, aktualizacje definicji, sterowniki, pakiety funkcji, aktualizacje zabezpieczeń, dodatki Service Pack, narzędzia, pakiety zbiorcze aktualizacji, aktualizacje lub uaktualnienie).

  - **Istotność zgodnie z MSRC**

    Istotność aktualizacji określona przez Microsoft Security Response Center (MSRC).

  - **Istotność**

    Istotność aktualizacji określona przez Kaspersky.

  - **Istotność poprawki**

    Istotność poprawki, jeśli jest ona przeznaczona dla aplikacji Kaspersky.

  - **Artykuł**

    Identyfikator (ID) artykułu w bazie wiedzy opisującego aktualizację.

  - **Biuletyn**

    Identyfikator biuletynu zabezpieczeń opisującego aktualizację.

  - **Nieprzypisane do instalacji (nowa wersja)**

    Wyświetla, czy aktualizacja ma stan Nieprzypisane do instalacji.

  - **Do zainstalowania**

    Wyświetla, czy aktualizacja ma stan Do zainstalowania.

  - **Instalowanie**

    Wyświetla, czy aktualizacja ma stan Instalowanie.

- **Zainstalowano**

  Wyświetla, czy aktualizacja ma stan Zainstalowana.

- **Niepowodzenie**

  Wyświetla, czy aktualizacja ma stan Niepowodzenie.

- **Wymagane jest ponowne uruchomienie**

  Wyświetla, czy aktualizacja ma stan Wymagane ponowne uruchomienie.

- **Zarejestrowano**

  Wyświetla datę i godzinę rejestracji aktualizacji.

- **Zainstalowana w trybie interaktywnym**

  Wyświetla, czy aktualizacja wymaga interakcji z użytkownikiem podczas instalacji.

- **Wycofano**

  Wyświetla datę i godzinę odwołania aktualizacji.

- **Stan zatwierdzenia aktualizacji**

  Wyświetla, czy aktualizacja została zatwierdzona do instalacji.

- **Zmiana**

  Wyświetla aktualny numer wersji aktualizacji.

- **ID aktualizacji**

  Wyświetla identyfikator aktualizacji.

- **Wersja aplikacji**

  Wyświetla numer wersji, do której ma zostać zaktualizowana aplikacja.

- **Zastąpiony**

  Wyświetla inne aktualizacje, które mogą zastąpić aktualizację.

- **Zastępowanie**

  Wyświetla inne aktualizacje, które mogą zostać zastąpione przez aktualizację.

- **Akceptacja warunków Umowy licencyjnej jest wymagana**

  Wyświetla, czy aktualizacja wymaga akceptacji warunków Umowy licencyjnej użytkownika końcowego (EULA).

- **Adres strony z opisem**

  Wyświetla nazwę producenta aktualizacji.

- **Rodzina aplikacji**

  Wyświetla nazwę rodziny aplikacji, do której należy aktualizacja.

- **Aplikacja**

  Wyświetla nazwę aplikacji, do której należy aktualizacja.

- **Wersja językowa**

  Wyświetla język aktualizacji.

- **Nieprzypisane do instalacji (nowa wersja)**

  Wyświetla, czy aktualizacja ma stan Nie przypisano do instalacji (nowa wersja).

- **Wymaga instalacji elementów należących do wymagań wstępnych**

  Wyświetla, czy aktualizacja ma stan Wymaga instalacji wymagań wstępnych.

- **Tryb pobierania**

  Wyświetla tryb pobierania aktualizacji.

- **Jest poprawką**

  Wyświetla, czy aktualizacja jest poprawką.

- **Nie zainstalowano**

  Wyświetla, czy aktualizacja ma stan Nie zainstalowano.

- Tabela **Ustawienia**, która wyświetla ustawienia pakietu instalacyjnego — z ich nazwami, opisami i wartościami — użyte jako parametry wiersza poleceń podczas instalacji. Jeśli pakiet nie zawiera takich ustawień, wyświetlana jest odpowiednia wiadomość. Możesz zmodyfikować wartości tych ustawień.

- Zakładka **Historia rewizji** wyświetlająca rewizje pakietów instalacyjnych i zawierająca następujące kolumny:

  - **Zmiana** — wyświetla liczbę rewizji pakietów instalacyjnych.

  - **Czas** — data i godzina modyfikacji ustawień pakietu instalacyjnego.

  - **Użytkownik** — nazwa użytkownika, który zmodyfikował pakiet instalacyjny.

  - **Akcja** — wyświetla działanie (działania) wykonane na pakiecie instalacyjnym w obrębie rewizji.

  - **Opis** — opis rewizji związanej ze zmianą wprowadzoną w ustawieniach pakietu instalacyjnego.

    Domyślnie, pole opisu rewizji jest puste. Aby dodać opis do rewizji, wybierz żądaną rewizję i kliknij przycisk **Edytuj opis**. W otwartym oknie wprowadź tekst opisu rewizji.

Znaczniki aplikacji

Kaspersky Security Center umożliwia oznaczanie aplikacji z rejestru aplikacji. Znacznik to etykieta aplikacji, która może zostać użyta do grupowania lub wyszukiwania aplikacji. Znacznik przypisany do aplikacji może służyć jako warunek w wyborach urządzeń.

Na przykład, możesz utworzyć znacznik `[Browsers]` i przypisać go do wszystkich przeglądarek Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Tworzenie znacznika aplikacji

W celu utworzenia znacznika aplikacji:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Znaczniki aplikacji**.
2. Kliknij **Dodaj**.

   Zostanie otwarte okno nowego znacznika.
3. Wprowadź nazwę znacznika.
4. Kliknij **OK**, aby zachować zmiany.

Nowy znacznik pojawi się na liście znaczników aplikacji.

Zmienianie nazwy znacznika aplikacji

W celu zmiany nazwy znacznika aplikacji:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Znaczniki aplikacji**.
2. Zaznacz pole obok znacznika, którego nazwę chcesz zmienić, a następnie kliknij **Edytuj**.

   Zostanie otwarte okno właściwości znacznika.
3. Zmień nazwę znacznika.
4. Kliknij **OK**, aby zachować zmiany.

Zaktualizowany znacznik pojawi się na liście znaczników aplikacji.

Przydzielanie znaczników do aplikacji

W celu przydzielenia jednego lub kilku znaczników do aplikacji:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Rejestr aplikacji**.
2. Kliknij nazwę aplikacji, do której chcesz przydzielić znaczniki.
3. Wybierz zakładkę **Znaczniki**.

   Zakładka wyświetla wszystkie znaczniki aplikacji, które istnieją na Serwerze administracyjnym. Dla znaczników przypisanych do wybranej aplikacji, w kolumnie **Przypisany znacznik** zaznaczone jest pole.
4. Dla znaczników, które chcesz przypisać, w kolumnie **Przypisany znacznik** zaznacz pola.
5. Kliknij **Zapisz**, aby zachować zmiany.

Znaczniki zostają przypisane do aplikacji.

Usuwanie przydzielonych znaczników z aplikacji

W celu usunięcia jednego lub kilku znaczników z aplikacji:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Rejestr aplikacji**.
2. Kliknij nazwę aplikacji, z której chcesz usunąć znaczniki.
3. Wybierz zakładkę **Znaczniki**.

   Zakładka wyświetla wszystkie znaczniki aplikacji, które istnieją na Serwerze administracyjnym. Dla znaczników przypisanych do wybranej aplikacji, w kolumnie **Przypisany znacznik** zaznaczone jest pole.
4. Dla znaczników, które chcesz usunąć, w kolumnie **Przypisany znacznik** odznacz pola.
5. Kliknij **Zapisz**, aby zachować zmiany.

Znaczniki zostają usunięte z aplikacji.

Usunięte znaczniki aplikacji nie zostają całkowicie usunięte. Jeśli chcesz, możesz usunąć je ręcznie.

Usuwanie znacznika aplikacji

W celu usunięcia znacznika aplikacji:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Znaczniki aplikacji**.
2. Z listy wybierz znacznik aplikacji, który chcesz usunąć.
3. Kliknij przycisk **Usuń**.
4. W otwartym oknie potwierdzenia kliknij **OK**.

Znacznik aplikacji zostanie usunięty. Usunięty znacznik jest automatycznie usuwany ze wszystkich aplikacji, do których został przydzielony.

Monitorowanie i raportowanie

Ta sekcja opisuje możliwości monitorowania i raportowania Kaspersky Security Center. Te możliwości dają ogląd infrastruktury, stanów ochrony i statystyk.

Po zainstalowaniu programu Kaspersky Security Center lub podczas jego działania, możesz skonfigurować funkcje monitorowania i raportowania, aby najlepiej odpowiadały Twoim potrzebom.

Scenariusz: Monitorowanie i raportowanie

Ta sekcja zawiera scenariusz konfigurowania funkcji monitorowania i raportowania w Kaspersky Security Center.

Wymagania wstępne

Po wdrożeniu Kaspersky Security Center w sieci organizacji, możesz uruchomić jej monitorowanie i wygenerować raporty dotyczące jej funkcjonowania.

Monitorowanie i raportowanie w sieci organizacji odbywa się w etapach:

1. **Konfigurowanie przełączania stanów urządzeń**

   Zapoznaj się z ustawieniami stanów urządzeń w zależności od określonych warunków. Zmieniając te ustawienia, możesz zmienić liczbę zdarzeń z poziomem istotności *Krytyczne* lub *Ostrzeżenie*. Podczas konfigurowania przełączania stanów urządzeń, upewnij się, że:

   - Nowe ustawienia nie są sprzeczne z polityką bezpieczeństwa informacji, obowiązującą w Twojej firmie.
   - Możesz reagować na ważne zdarzenia dotyczące bezpieczeństwa w sieci Twojej organizacji w odpowiednim momencie.

2. **Konfigurowanie powiadomień o zdarzeniach występujących na urządzeniach klienckich**

   Dostępne instrukcje:

   Skonfiguruj powiadamianie (poprzez e-mail, wiadomość SMS lub przez uruchomienie pliku wykonywalnego) o zdarzeniach na urządzeniach klienckich

3. **Zmiana reakcji ochrony sieci na zdarzenie Epidemia wirusa**

   Możesz zmienić określone wartości progowe we właściwościach Serwera administracyjnego. Możesz także utworzyć rygorystyczną zasadę, która zostanie aktywowana, lub utworzyć zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.

4. **Wykonywanie zalecanych działań dla powiadomień krytycznych i ostrzegających**

   Dostępne instrukcje:

   Wykonaj zalecane działania dla sieci w swojej organizacji

5. **Sprawdzanie stanu ochrony sieci w swojej organizacji**

   Dostępne instrukcje:

   - Sprawdź widżeta Stan ochrony
   - Wygeneruj i sprawdź Raport o stanie ochrony
   - Wygeneruj i przeczytaj Raport o błędach

6. **Lokalizowanie urządzeń klienckich, które nie są chronione**

Dostępne instrukcje:

- Przejrzyj widżet Nowe urządzenia
- Wygeneruj i przeczytaj Raport wdrażania ochrony

7. **Sprawdzanie ochrony urządzeń klienckich**

   Dostępne instrukcje:

   - Wygeneruj i sprawdź raporty z kategorii Stan ochrony i Statystyki zagrożeń
   - Uruchom i sprawdź wybór zdarzeń Krytyczny

8. **Oszacowanie i ograniczenie nagromadzenia zdarzeń w bazie danych**

   Informacje o zdarzeniach występujących podczas działania zarządzanych aplikacji są przesyłane z urządzenia klienckiego i zapisywane w bazie danych Serwera administracyjnego. Aby zmniejszyć obciążenie na Serwerze administracyjnym, oszacuj i ogranicz maksymalną liczbę zdarzeń przechowywanych w bazie danych.

   Dostępne instrukcje:

   - Obliczanie pojemności bazy danych
   - Ograniczanie maksymalnej liczby zdarzeń

9. **Przeglądanie informacji o licencji**

   Dostępne instrukcje:

   - Dodaj widżet Użycie kluczy licencyjnych do pulpitu nawigacyjnego i sprawdź go
   - Wygeneruj i przeczytaj Raport o użyciu kluczy licencyjnych

Wyniki

Po zakończeniu scenariusza zostaniesz poinformowany o ochronie sieci w swojej organizacji i tym samym będziesz mógł zaplanować działania związane z dalszą ochroną.

Informacje o typach monitorowania i raportowania

Informacje na temat zdarzeń dotyczących bezpieczeństwa w sieci organizacji są przechowywane w bazie danych Serwera administracyjnego. Na podstawie zdarzeń Kaspersky Security Center Web Console oferuje następujące typy monitorowania i raportowania w sieci Twojej organizacji:

- Pulpit nawigacyjny
- Raporty
- Wybory zdarzeń
- Powiadomienia

Pulpit nawigacyjny

Pulpit nawigacyjny umożliwia monitorowanie trendów bezpieczeństwa w sieci Twojej organizacji poprzez graficzne przedstawienie informacji.

Raporty

Raporty umożliwiają uzyskanie szczegółowych informacji liczbowych na temat ochrony sieci Twojej organizacji, zapisania tych informacji w pliku, wysłania ich w wiadomości e-mail oraz ich wydrukowania.

Wybory zdarzeń

Wybory zdarzeń oferują widok ekranowy nazwanych zestawów zdarzeń, które są wybrane z bazy danych Serwera administracyjnego. Te zestawy zdarzeń są grupowane zgodnie z następującymi kategoriami:

- Według istotności—**Zdarzenia krytyczne**, **Błędy funkcjonalne**, **Ostrzeżenia** i **Informacja o zdarzeniach**
- Według czasu—**Ostatnie zdarzenia**
- Według typu—**Żądania użytkownika** and **Zdarzenia audytu**

Możesz tworzyć i przeglądać wybory zdarzeń zdefiniowane przez użytkownika oparte na ustawieniach dostępnych do konfiguracji w interfejsie Kaspersky Security Center Web Console.

Powiadomienia

Powiadomienia informują o zdarzeniach oraz pomagają w przyspieszeniu odpowiedzi na te zdarzenia poprzez wykonanie zalecanych działań lub działań, które uznajesz za odpowiednie.

Pulpit nawigacyjny i widżety

Ta sekcja zawiera informacje o panelu kontrolnym i widżetach udostępnianych przez panel kontrolny. Sekcja zawiera instrukcje dotyczące zarządzania widżetami i konfigurowania ich ustawień.

Korzystanie z pulpitu nawigacyjnego

Pulpit nawigacyjny umożliwia monitorowanie trendów bezpieczeństwa w sieci Twojej organizacji poprzez graficzne przedstawienie informacji.

Pulpit nawigacyjny jest dostępny w Kaspersky Security Center Web Console w sekcji **Monitorowanie i raportowanie** po kliknięciu **Pulpit nawigacyjny**.

Pulpit nawigacyjny zawiera widżety, które można dostosować. Możesz wybrać dużą liczbę różnych widżetów, przedstawionych w postaci wykresu kołowego lub diagramu pierścieniowego, tabeli, wykresów, wykresów słupkowych oraz list. Informacje wyświetlane w widżetach są automatycznie aktualizowane, okres aktualizacji wynosi od jednej do dwóch minut. Przedział czasu między aktualizacjami jest inny dla każdego widżeta. Możesz ręcznie odświeżyć dane dotyczące widżeta w dowolnym momencie, korzystając z menu ustawień.

Domyślnie widżety zawierają informacje o wszystkich zdarzeniach przechowywanych w bazie danych Serwera administracyjnego.

Kaspersky Security Center Web Console zawiera domyślny zestaw widżetów należących do następujących kategorii:

- **Stan ochrony**
- **Wdrażanie**
- **Aktualizowanie**
- **Statystyki zagrożeń**
- **Inne**

Niektóre widżety posiadają informacje tekstowe z odnośnikami. Po kliknięciu odnośnika zostaną wyświetlone informacje szczegółowe.

Podczas konfigurowania pulpitu nawigacyjnego możesz dodać widżety, których potrzebujesz, ukryć widżety, których nie potrzebujesz, zmienić rozmiar lub wygląd widżetów, przenieść widżety, a także zmienić ich ustawienia.

Dodawanie widżetów do pulpitu nawigacyjnego

W celu dodania widżetów do pulpitu nawigacyjnego:

1. W menu głównym przejdź do **Monitorowanie i raportowanie → Pulpit nawigacyjny**.
2. Kliknij przycisk **Dodaj lub przywróć widżet sieciowy**.
3. Na liście dostępnych widżetów wybierz widżety, które chcesz dodać do pulpitu nawigacyjnego.

   Widżety są pogrupowane według kategorii. Aby wyświetlić listę widżetów należących do kategorii, kliknij ikonę strzałki skierowanej w prawo (>), znajdującą się obok nazwy kategorii.
4. Kliknij przycisk **Dodaj**.

Wybrane widżety zostaną dodane na końcu pulpitu nawigacyjnego.

Teraz możesz edytować reprezentację i parametry dodanych widżetów.

Ukrywanie widżetu na pulpicie nawigacyjnym

W celu ukrycia widżetu na pulpicie nawigacyjnym:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia(⚙), znajdującą się obok widżetu, który chcesz ukryć.
3. Wybierz **Ukryj widżet sieciowy**.
4. W otwartym oknie **Ostrzeżenie** kliknij **OK**.

Wybrany widżet zostanie ukryty. Następnie możesz ponownie dodać ten widżet do pulpitu nawigacyjnego.

Przenoszenie widżetu na pulpicie nawigacyjnym

W celu przeniesienia widżetu na pulpicie nawigacyjnym:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia (⚙), znajdującą się obok widżetu, który chcesz przenieść.
3. Wybierz **Przenieś**.
4. Kliknij miejsce, do którego chcesz przenieść widżet. Możesz wybrać tylko inny widżet.

Miejsca wybranych widżetów zostaną zamienione.

Zmiana wyglądu i rozmiaru widżetu

Dla widżetów, które wyświetlają wykres, możesz zmienić jego reprezentację-wykres słupkowy lub wykres liniowy. Dla niektórych widżetów możesz zmienić ich rozmiar: kompaktowy, średni lub maksymalny.

W celu zmiany reprezentacji widżetu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia (⚙), znajdującą się obok widżetu, który chcesz edytować.
3. Wykonaj jedną z poniższych czynności:
   - Aby wyświetlić widżet jako wykres słupkowy, wybierz **Typ wykresu: Słupki**.
   - Aby wyświetlić widżet jako wykres liniowy, wybierz **Typ wykresu: Linie**.

- W celu zmiany obszaru zajętego przez widżet, wybierz jedną z wartości:
  - **Kompaktowy**
  - **Kompaktowy (tylko słupek)**
  - **Średni (wykres pierścieniowy)**
  - **Średni (wykres słupkowy)**
  - **Maksymalny**

Reprezentacja wybranego widżetu zostanie zmieniona.

Zmiana ustawień widżetu

W celu zmiany ustawień widżetu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia (⚙), znajdującą się obok widżetu, który chcesz zmienić.
3. Wybierz **Pokaż ustawienia**.
4. Jeśli zostanie otwarte okno ustawień widżetu, zmień ustawienia widżetu zgodnie z wymaganiami.
5. Kliknij **Zapisz**, aby zachować zmiany.

Ustawienia wybranego widżetu zostaną zmienione.

Zestaw ustawień zależy od określonego widżetu. Poniżej znajdują się podstawowe ustawienia:

- **Obszar widżetu webowego** (zestaw obiektów, dla których widżet wyświetla informacje)—na przykład, grupa administracyjna lub wybór urządzeń.
- **Wybierz zadanie** (zadanie, dla którego widżet wyświetla informacje).
- **Przedział czasu** (przedział czasu, w trakcie którego informacje są wyświetlane w widżecie)—między dwoma określonymi datami; od określonej daty do bieżącego dnia; lub od bieżącego dnia minus określoną liczbę dni do bieżącego dnia.
- **Ustaw stan Krytyczny, jeśli** i **Ustaw stan Ostrzeżenie, jeśli** (reguły, które określają kolor wskaźnika).

Po zmianie ustawień widżetu możesz ręcznie odświeżyć dane w widżecie.

Aby odświeżyć dane w widżecie:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia (⚙), znajdującą się obok widżetu, który chcesz przenieść.
3. Wybierz opcję **Odśwież**.

Dane w widżecie zostaną odświeżone.

Informacje o trybie korzystania tylko z pulpitu

Możesz skonfigurować tryb samego pulpitu dla pracowników, którzy nie zarządzają siecią, ale chcą przeglądać statystyki ochrony sieci w Kaspersky Security Center (na przykład menedżer najwyższego poziomu). Gdy użytkownik ma włączony ten tryb, wyświetlany jest tylko pulpit nawigacyjny z predefiniowanym zestawem widżetów. Dzięki temu może monitorować statystyki określone w widżetach, na przykład stan ochrony wszystkich zarządzanych urządzeń, liczbę ostatnio wykrytych zagrożeń lub listę najczęstszych zagrożeń w sieci.

Gdy użytkownik pracuje w trybie korzystania tylko z pulpitu, stosowane są następujące ograniczenia:

- Menu główne nie jest wyświetlane użytkownikowi, więc nie może on zmienić ustawień ochrony sieci.
- Użytkownik nie może wykonywać żadnych akcji z widżetami, na przykład dodawać widżetów lub ich ukrywać. Dlatego należy umieścić w pulpicie nawigacyjnym wszystkie potrzebne użytkownikowi widżety i skonfigurować je, np. ustawić zasadę liczenia obiektów lub określić przedział czasowy.

Nie można przypisać sobie trybu korzystania tylko z pulpitu. Jeśli chcesz pracować w tym trybie, skontaktuj się z administratorem systemu, dostawcą usług zarządzanych (MSP) lub użytkownikiem z uprawnieniami **Modyfikacja listy ACL obiektów** w obszarze **Funkcje ogólne: uprawnienia użytkownika**.

Konfigurowanie trybu korzystania tylko z pulpitu

Zanim zaczniesz konfigurować Tryb korzystania tylko z pulpitu, upewnij się, że spełnione są następujące wymagania wstępne:

- Masz uprawnienia **Modyfikacja list ACL obiektów** w obszarze funkcjonalnym **Funkcje ogólne: uprawnienia użytkownika**. Jeśli nie masz tych uprawnień, nie będzie zakładki do konfiguracji trybu.
- Użytkownik ma uprawnienia **Odczyt** w obszarze funkcjonalnym **Funkcje ogólne: funkcjonalność podstawowa**.

Jeśli w Twojej sieci istnieje hierarchia Serwerów administracyjnych, aby skonfigurować tryb korzystania tylko z pulpitu, przejdź do serwera, na którym dostępne jest konto użytkownika na zakładce **Użytkownicy** sekcji **Użytkownicy i role → Użytkownicy i grupy**. Może to być serwer główny lub fizyczny serwer pomocniczy. Nie ma możliwości dostosowania trybu na serwerze wirtualnym.

W celu skonfigurowania trybu korzystania tylko z pulpitu:

1. W menu głównym przejdź do opcji **Użytkownicy i role → Użytkownicy i grupy**, a następnie wybierz zakładkę **Użytkownicy**.
2. Kliknij nazwę konta użytkownika, dla którego chcesz dostosować pulpit nawigacyjny za pomocą widżetów.
3. W otwartym oknie ustawień konta wybierz zakładkę **Pulpit nawigacyjny**.

   Na karcie, która się otworzy, zostanie wyświetlony ten sam pulpit nawigacyjny, co pulpit dla użytkownika.
4. Jeśli opcja **Wyświetlaj konsolę w trybie korzystania tylko z pulpitu** jest włączona, przełącz przełącznik, aby ją wyłączyć.

   Gdy ta opcja jest włączona, nie można również zmienić pulpitu nawigacyjnego. Po wyłączeniu opcji możesz zarządzać widżetami.

5. Skonfiguruj wygląd pulpitu nawigacyjnego. Zestaw widżetów przygotowany w zakładce **Pulpit nawigacyjny** jest dostępny dla użytkownika z konfigurowalnym kontem. Użytkownik nie może zmieniać żadnych ustawień ani rozmiaru widżetów, dodawać ani usuwać żadnych widżetów z pulpitu nawigacyjnego. Dlatego dostosuj je dla użytkownika, aby mógł przeglądać statystyki ochrony sieci. W tym celu w zakładce **Pulpit nawigacyjny** możesz wykonać te same akcje z widżetami, co w sekcji **Monitorowanie i raportowanie → Pulpit nawigacyjny**:

   - Dodaj nowe widżety do pulpitu nawigacyjnego.
   - Ukryj widżety, których użytkownik nie potrzebuje.
   - Przenieś widżety w określonej kolejności.
   - Zmień rozmiar lub wygląd widżetów.
   - Zmień ustawienia widżetu.

6. Przełącz przycisk przełącznika, aby włączyć opcję **Wyświetlaj konsolę w trybie korzystania tylko z pulpitu**.

   Następnie dla użytkownika dostępny będzie tylko pulpit nawigacyjny. Użytkownik może monitorować statystyki, ale nie może zmieniać ustawień ochrony sieci i wyglądu pulpitu nawigacyjnego. Ponieważ wyświetlany jest ten sam pulpit nawigacyjny, co dla użytkownika, nie można również zmienić pulpitu nawigacyjnego.

   Jeśli pozostawisz tę opcję wyłączoną, dla użytkownika zostanie wyświetlone menu główne, dzięki czemu będzie on mógł wykonywać różne akcje w Kaspersky Security Center, w tym zmieniać ustawienia bezpieczeństwa i widżety.

7. Po zakończeniu konfigurowania trybu korzystania tylko z pulpitu kliknij przycisk **Zapisz**. Dopiero po tym przygotowany pulpit nawigacyjny zostanie wyświetlony użytkownikowi.

8. Jeśli użytkownik chce przeglądać statystyki obsługiwanych aplikacji Kaspersky i potrzebuje do tego uprawnień dostępu, skonfiguruj uprawnienia dla użytkownika. Następnie dane aplikacji Kaspersky będą wyświetlane dla użytkownika w widżetach tych aplikacji.

Teraz użytkownik może zalogować się do Kaspersky Security Center na swoim koncie i monitorować statystyki ochrony sieci w trybie samego pulpitu.

Raporty administracyjne i ochrony

W tej sekcji opisano, jak używać raportów, zarządzać niestandardowymi szablonami raportów, używać szablonów raportów do generowania nowych raportów i tworzyć zadania dostarczania raportów.

Korzystanie z raportów

Raporty umożliwiają uzyskanie szczegółowych informacji liczbowych na temat ochrony sieci Twojej organizacji, zapisania tych informacji w pliku, wysłania ich w wiadomości e-mail oraz ich wydrukowania.

Raporty są dostępne w Kaspersky Security Center Web Console w sekcji **Monitorowanie i raportowanie** po kliknięciu **Raporty**.

Domyślnie, raporty zawierają informacje dla ostatnich 30 dni.

Kaspersky Security Center posiada domyślny zestaw raportów należących do następujących kategorii:

- **Stan ochrony**
- **Wdrażanie**
- **Aktualizowanie**
- **Statystyki zagrożeń**
- **Inne**

Możesz tworzyć niestandardowe szablony raportu, edytować szablony raportu oraz usuwać je.

Możesz tworzyć raporty, które są oparte na istniejących szablonach, eksportować raporty do plików, a także tworzyć zadania dostarczania raportów.

Tworzenie szablonu raportu

W celu utworzenia szablonu raportu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie → Raporty**
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Wprowadź nazwę raportu i wybierz typ raportu.
4. W kroku **Zakres** wybierz zestaw urządzeń klienckich (grupę administracyjną, wybór urządzeń, wybrane urządzenia lub wszystkie urządzenia w sieci), których dane zostaną wyświetlone w raportach, które są oparte na tym szablonie raportu.
5. W kroku **Okres raportowania** kreatora określ okres raportowania. Dostępne wartości wyglądają następująco:

   - Między dwoma określonymi datami
   - Od określonej daty do daty utworzenia raportu
   - Od daty utworzenia raportu minus określona liczba dni do daty utworzenia raportu

   Dla niektórych raportów ta strona może nie być wyświetlana.
6. Kliknij **OK**, aby zamknąć kreator.
7. Wykonaj jedną z poniższych czynności:

   - Kliknij przycisk **Zapisz i uruchom**, aby zapisać nowy szablon raportu i uruchomić raport w oparciu o niego.

     Szablon raportu zostanie zapisany. Raport zostanie wygenerowany.
   - Kliknij przycisk **Zapisz**, aby zapisać nowy szablon raportu.

     Szablon raportu zostanie zapisany.

Możesz użyć nowego szablonu do generowania i wyświetlania raportów.

Przeglądanie i edytowanie właściwości szablonu raportu

Możesz przeglądać i edytować podstawowe właściwości szablonu raportu, na przykład, nazwę szablonu raportu lub pola wyświetlane w raporcie.

W celu przejrzenia i edytowania właściwości szablonu raportu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Raporty**.
2. Zaznacz pole obok szablonu raportu, którego właściwości chcesz przejrzeć i edytować.

   Alternatywnie możesz w pierwszej kolejności wygenerować raport, a następnie kliknąć przycisk **Edytuj**.
3. Kliknij przycisk **Otwórz właściwości szablonu raportu**.

   Zostanie otwarte okno **Edytowanie raportu <Nazwa raportu>** na zakładce **Ogólne**.
4. Edytuj właściwości szablonu raportu:
   - Zakładka **Ogólne**:
     - Nazwa szablonu raportu
     - **Maksymalna liczba wyświetlanych wpisów**

       Jeśli ta opcja jest włączona, liczba wpisów wyświetlanych w tabeli ze szczegółowymi danymi raportu nie wynosi więcej niż określona wartość.

       Wpisy w raporcie są najpierw przechowywane zgodnie z regułami określonymi w sekcji **Pola** → **Pola szczegółów** właściwości szablonu raportu, a następnie przechowywane są tylko pierwsze wpisy wynikowe. Nagłówek tabeli ze szczegółowymi danymi raportu pokazuje wyświetloną liczbę wpisów oraz całkowitą dostępną liczbę wpisów, które odpowiadają ustawieniom innego szablonu raportu.

       Jeśli ta opcja jest wyłączona, tabela ze szczegółowymi danymi raportu wyświetla wszystkie dostępne wpisy. Nie jest zalecane wyłączenie tej opcji. Ograniczenie liczby wyświetlanych wpisów raportu zmniejsza obciążenie systemu zarządzania bazą danych (DBMS) i skraca czas wymagany do wygenerowania i eksportowania raportu. Niektóre z raportów zawierają zbyt wiele wpisów. W takiej sytuacji może być trudno przeczytać i przeanalizować je wszystkie. Dodatkowo, podczas tworzenia takiego raportu, na Twoim urządzeniu może zabraknąć pamięci, co w konsekwencji uniemożliwi przejrzenie raportu.

       Domyślnie opcja ta jest włączona. Domyślna wartość to 1000.

     - **Grupa**

       Kliknij przycisk **Ustawienia**, aby zmienić zestaw urządzeń klienckich, dla których tworzony jest raport. Dla niektórych typów raportów przycisk może być niedostępny. Rzeczywiste ustawienia zależą od ustawień określonych podczas tworzenia szablonu raportu.

     - **Przedział czasu**

Kliknij przycisk **Ustawienia**, aby zmodyfikować okres raportowania. Dla niektórych typów raportów przycisk może być niedostępny. Dostępne wartości wyglądają następująco:

- Między dwoma określonymi datami
- Od określonej daty do daty utworzenia raportu
- Od daty utworzenia raportu minus określona liczba dni do daty utworzenia raportu

- **Dołącz dane z podrzędnych i wirtualnych Serwerów administracyjnych**

  Jeśli ta opcja jest włączona, raport zawiera informacje z podrzędnych i wirtualnych Serwerów administracyjnych, które podlegają Serwerowi administracyjnemu, dla którego utworzono szablon raportu.

  Wyłącz tę opcję, jeśli chcesz przejrzeć dane tylko z bieżącego Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Do poziomu zagnieżdżenia**

  Raport zawiera dane z podrzędnych i wirtualnych Serwerów administracyjnych, które znajdują się pod bieżącym Serwerem administracyjnym na poziomie zagnieżdżenia, który jest mniejszy niż lub równy określonej wartości.

  Domyślna wartość to 1. Możesz chcieć zmienić tę wartość, jeśli musisz zbierać informacje z podrzędnych Serwerów administracyjnych znajdujących się na niższych poziomach drzewa.

- **Czas oczekiwania na dane (min)**

  Przed wygenerowaniem raportu, Serwer administracyjny, dla którego tworzony jest szablon raportu, oczekuje na dane z podrzędnych Serwerów administracyjnych przez określoną liczbę minut. Jeśli żadne dane nie są pobierane z podrzędnego Serwera administracyjnego pod koniec tego okresu, raport i tak zostanie uruchomiony. Zamiast rzeczywistych danych, raport wyświetla dane pobrane z pamięci podręcznej (jeśli opcja **Buforuj dane z podrzędnych Serwerów administracyjnych** jest włączona) lub **N/A** (nie jest dostępne) w innym przypadku.

  Domyślna wartość to 5 (minuty).

- **Buforuj dane z podrzędnych Serwerów administracyjnych**

  Podrzędne Serwery administracyjne regularnie przesyłają dane do Serwera administracyjnego, dla którego został utworzony szablon raportu. Przesłane dane są przechowywane w pamięci podręcznej.

  Jeśli podczas generowania raportu bieżący Serwer administracyjny nie może odbierać danych z podrzędnego Serwera administracyjnego, raport wyświetla dane pobrane z pamięci podręcznej. Wyświetlana jest także data przesłania danych do pamięci podręcznej.

  Włączenie tej opcji umożliwia przeglądanie informacji z podrzędnych Serwerów administracyjnych nawet wtedy, gdy aktualne dane nie mogą zostać pobrane. Jednakże wyświetlane dane mogą być przestarzałe.

  Domyślnie opcja ta jest wyłączona.

- **Częstotliwość aktualizacji pamięci podręcznej (godz.)**

  Podrzędne Serwery administracyjne regularnie przesyłają dane do Serwera administracyjnego, dla którego został utworzony szablon raportu. Możesz określić ten okres w godzinach. Jeśli określisz 0 godzin, dane są przesyłane tylko wtedy, gdy raport zostaje wygenerowany.

  Domyślna wartość to 0.

- **Prześlij szczegółowe informacje z podrzędnych Serwerów administracyjnych**

  W wygenerowanym raporcie tabela ze szczegółowymi danymi raportu zawiera dane z podrzędnych Serwerów administracyjnych Serwera administracyjnego, dla którego został utworzony szablon raportu.

  Włączenie tej opcji spowalnia tworzenie raportu i zwiększa ruch sieciowy między Serwerami administracyjnymi. Jednakże możesz przejrzeć wszystkie dane w jednym raporcie.

  Zamiast włączyć tę opcję, możesz chcieć przeanalizować szczegółowe dane raportu, aby wykryć wadliwy podrzędny Serwer administracyjny, a następnie wygenerować ten sam raport tylko dla tego wadliwego Serwera administracyjnego.

  Domyślnie opcja ta jest wyłączona.

- Zakładka **Pola**

  Wybierz pola, które będą wyświetlane w raporcie i użyj przycisku **W górę** oraz przycisku **W dół**, aby zmienić kolejność tych pól. Użyj przycisku **Dodaj** lub przycisku **Edytuj**, aby określić, czy informacje w raporcie muszą być sortowane i filtrowane według każdego z pól.

  W sekcji **Pola filtrów szczegółów** możesz również kliknąć przycisk **Konwertuj filtry**, aby rozpocząć korzystanie z rozszerzonego formatu filtrowania. Ten format umożliwia łączenie warunków filtrowania określonych w różnych polach za pomocą operacji logicznej LUB. Po kliknięciu przycisku po prawej stronie zostanie otwarty panel **Konwertuj filtry**. Kliknij przycisk **Konwertuj filtry**, aby potwierdzić konwersję. Możesz teraz zdefiniować przekonwertowany filtr z warunkami z sekcji **Pola szczegółów**, które są stosowane przy użyciu operacji logicznej LUB.

  > Konwersja raportu do formatu obsługującego złożone warunki filtrowania spowoduje, że raport będzie niezgodny z poprzednimi wersjami Kaspersky Security Center (11 i starszymi). Przekonwertowany raport nie będzie zawierał żadnych danych z podrzędnych Serwerów administracyjnych, na których działają takie niekompatybilne wersje.

5. Kliknij **Zapisz**, aby zachować zmiany.
6. Zamknij okno **Edycja raportu <Nazwa raportu>**.

Zaktualizowany szablon raportu pojawi się na liście szablonów raportu.

Eksportowanie raportu do pliku

Możesz wyeksportować raport do pliku XML, HTML lub PDF.

W celu wyeksportowania raportu do pliku:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Raporty**.
2. Zaznacz pole obok raportu, który chcesz wyeksportować do pliku.
3. Kliknij przycisk **Eksportuj raport**.
4. W otwartym oknie, w polu **Nazwa** zmień nazwę pliku raportu. Domyślnie, nazwa pliku pokrywa się z nazwą wybranego szablonu raportu.
5. Wybierz typ pliku raportu: XML, HTML lub PDF.

6. Kliknij przycisk **Eksportuj raport**.

   Raport w wybranym formacie zostanie pobrany na Twoje urządzenie—do folderu domyślnego Twojego urządzenia—lub zostanie otwarte standardowe okno **Zapisywanie jako** w Twojej przeglądarce, aby umożliwić Ci zapisanie pliku w miejscu, w którym chcesz.

Raport zostanie zapisany do pliku.

Generowanie i przeglądanie raportu

W celu utworzenia i przejrzenia raportu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Raporty**.
2. Kliknij nazwę szablonu raportu, którego chcesz użyć do utworzenia raportu.

Raport zostanie wygenerowany przy użyciu wybranego szablonu i wyświetlony.

Dane raportu są wyświetlane zgodnie z lokalizacją ustawioną dla Serwera administracyjnego.

Raport wyświetla następujące dane:

- Na zakładce **Podsumowanie**:
  - Nazwę i typ raportu, krótki opis i okres raportowania, a także informacje o grupie urządzeń, dla których generowany jest raport.
  - Wykres graficzny przedstawiający najbardziej reprezentatywne dane raportu.
  - Tabelę zbiorczą z wyliczonymi wskaźnikami raportu.
- Na zakładce **Szczegóły** wyświetlona zostanie tabela ze szczegółowymi danymi raportu.

Tworzenie zadania dostarczania raportu

Możesz utworzyć zadanie, które będzie dostarczać wybrane raporty.

W celu utworzenia zadania dostarczania raportu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Raporty**.
2. Zaznacz pole obok szablonów raportu, dla którego chcesz utworzyć zadanie dostarczania raportu.
3. Kliknij przycisk **Utwórz zadanie dostawy**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
4. W kroku kreatora **Ustawienia nowych zadań** wprowadź nazwę zadania.

   Domyślna nazwa to **Dostarcz raporty**. Jeżeli zadanie o tej nazwie już istnieje, do nazwy zadania dodawany jest numer porządkowy (<N>).

5. W kroku **Konfiguracja raportu** kreatora określ następujące ustawienia:

   a. Szablony raportu, które zostaną dostarczone przez zadanie.

   b. Format raportu: HTML, XLS lub PDF.

      Do konwersji raportu do formatu PDF wymagane jest narzędzie wkhtmltopdf. Po wybraniu opcji PDF Serwer administracyjny sprawdza, czy na urządzeniu jest zainstalowane narzędzie wkhtmltopdf. Jeżeli narzędzie nie jest zainstalowane, aplikacja wyświetla komunikat o konieczności zainstalowania narzędzia na urządzeniu Serwera administracyjnego. Zainstaluj narzędzie ręcznie, a następnie przejdź do następnego kroku.

   c. Czy raporty są wysyłane za pośrednictwem poczty elektronicznej wraz z ustawieniami powiadomień e-mail.

      Możesz określić maksymalnie 20 adresów e-mail. Aby oddzielić adresy e-mail, naciśnij klawisz **Enter**. Możesz także wkleić listę adresów e-mail rozdzielonych przecinkami, a następnie nacisnąć klawisz **Enter**.

   d. Czy raporty są zapisywane do folderu, czy wcześniej zapisane raporty w tym folderze są nadpisywane i czy określone konto będzie używane do uzyskania dostępu do tego folderu (dla folderu współdzielonego).

6. W kroku **Konfiguruj terminarz zadania** kreatora wybierz harmonogram rozpoczęcia zadania.

   Dostępne są następujące opcje harmonogramu zadań:

   - **Ręcznie**

     Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

     Domyślnie opcja ta jest zaznaczona.

   - **Co N minut**

     Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

     Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

   - **Co N godzin**

     Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

     Domyślnie, zadanie jest uruchamiane co 6 godzin, począwszy od bieżącej daty i godziny systemowej.

   - **Co N dni**

     Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

     Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

   - **Co N tygodni**

     Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

     Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

   - **Co miesiąc**

     Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **W określone dni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie godzina rozpoczęcia to 18:00, a żadne dni miesiąca nie są wybrane.

  > Należy pamiętać, że nie wybiera się konkretnej daty w miesiącu ani numeru tygodnia (pierwszy, drugi tydzień miesiąca), ale kolejny numer dnia tygodnia w miesiącu. Na przykład, jeśli ustawisz kursor w komórce **Wt** w **Pierwszy** wierszu, oznacza to, że zadanie będzie uruchamiane w każdy pierwszy wtorek każdego nowego miesiąca.

  Można wybrać kilka dni tygodnia.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować ataki wirusa. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji zabezpieczającej, która zgłosiła atak wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Opcja ta działa tylko wtedy, gdy oba zadania są przypisane do tych samych urządzeń. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami* z opcją **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie antywirusowe*, jako zadanie wyzwalające.

  Musisz wybrać z tabeli zadanie wyzwalające i status, z jakim to zadanie musi zostać ukończone (**Pomyślnie zakończone** lub **Niepowodzenie**).

  W razie potrzeby możesz wyszukiwać, sortować i filtrować zadania w tabeli w następujący sposób:

  - Wpisz nazwę zadania w polu wyszukiwania, aby wyszukać zadanie na podstawie jego nazwy.
  - Kliknij ikonę sortowania, aby posortować zadania według nazwy.

    Domyślnie zadania są sortowane alfabetycznie, w porządku rosnącym.
  - Kliknij ikonę filtra i w oknie, które zostanie otwarte, przefiltruj zadania według grupy, a następnie kliknij przycisk **Zastosuj**.

7. W tym kroku kreatora skonfiguruj pozostałe ustawienia harmonogramu zadań:

   - W sekcji **Terminarz zadania** sprawdź lub skonfiguruj wcześniej wybrany harmonogram i ustaw przedział czasowy, dni miesiąca lub tygodnia, ustaw stan ataku wirusa lub wykonanie innego zadania jako wyzwalacz uruchomienia zadania. W tej sekcji można również określić godzinę rozpoczęcia, jeśli wybrany zostanie odpowiedni harmonogram.

   - W sekcji **Ustawienia dodatkowe** określ następujące ustawienia:

     - **Uruchom pominięte zadania**

       Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

       Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

       Jeśli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania. W przypadku harmonogramu **Ręcznie**, **Raz** i **Natychmiast** zadania są uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

       Domyślnie opcja ta jest wyłączona.

     - **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

       Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

       Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

       Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

     - **Użyj automatycznego losowego opóźnienia dla zadań uruchamianych w przedziale**

       Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

       Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

       Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

     - **Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż**

       Po minięciu określonego czasu, zadanie jest zatrzymywane automatycznie, niezależnie od tego, czy zostało zakończone.

       Włącz tę opcję, jeśli chcesz przerwać (lub zatrzymać) zadania, których wykonanie zajmuje zbyt dużo czasu.

       Domyślnie opcja ta jest wyłączona. Domyślny czas wykonania zadania to 120 minut.

8. Na etapie **Wybieranie konta do uruchomienia zadania** kreatora określ poświadczenia konta użytkownika używanego do uruchomienia zadania.

9. Jeśli chcesz zmodyfikować inne ustawienia zadania po utworzeniu zadania, w kroku **Zakończ tworzenie zadania** włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** (ta opcja jest domyślnie włączona).

10. Kliknij przycisk **Zakończ**, aby utworzyć zadanie i zamknąć kreator.

    Zostanie utworzone zadanie dostarczania raportów. Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, zostanie otwarte okno ustawień zadania.

Usuwanie szablonów raportu

W celu usunięcia jednego lub kilku szablonów raportu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Raporty**.

2. Zaznacz pola obok szablonów raportu, które chcesz usunąć.

3. Kliknij przycisk **Usuń**.

4. W otwartym oknie kliknij **OK**, aby potwierdzić swój wybór.

Wybrane szablony raportu zostaną usunięte. Jeśli te szablony raportu znajdowały się w zadaniach dostarczania raportów, zostaną usunięte z zadań.

Zdarzenia i wybory zdarzeń

Ta sekcja zawiera informacje o zdarzeniach i wyborach zdarzeń, o typach zdarzeń występujących w komponentach Kaspersky Security Center oraz o zarządzaniu blokowaniem częstych zdarzeń.

Informacje o zdarzeniach Kaspersky Security Center

Kaspersky Security Center umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Informacje o zdarzeniach są zapisywane w bazie danych Serwera administracyjnego.

Typy zdarzeń

W Kaspersky Security Center dostępne są następujące typy zdarzeń:

- Zdarzenia ogólne. Te zdarzenia występują we wszystkich zarządzanych aplikacjach firmy Kaspersky. Przykładem zdarzenia ogólnego jest Epidemia wirusa. Zdarzenia ogólne mają dokładnie zdefiniowaną składnię i semantykę. Zdarzenia ogólne są używane, na przykład, w raportach i pulpitach nawigacyjnych.

- Zarządzane zdarzenia charakterystyczne dla aplikacji firmy Kaspersky. Każda zarządzana aplikacja firmy Kaspersky posiada swój zestaw zdarzeń.

Źródła zdarzeń

Zdarzenia mogą być generowane przez następujące aplikacje:

- Składniki Kaspersky Security Center:
  - Serwer administracyjny
  - Agent sieciowy
  - Serwer iOS MDM
  - Serwer urządzeń mobilnych Exchange
- Zarządzane aplikacje Kaspersky

  Szczegółowe informacje na temat zdarzeń generowanych przez aplikacje zarządzane przez Kaspersky można znaleźć w dokumentacji odpowiedniej aplikacji.

Możesz wyświetlić pełną listę zdarzeń, które mogą być generowane przez aplikację na karcie **Konfiguracja zdarzenia** w zasadzie aplikacji. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić listę zdarzeń we właściwościach Serwera administracyjnego.

Poziom ważności zdarzeń

Każde zdarzenie posiada określony poziom istotności. W zależności od warunków wystąpienia zdarzenia, może ono posiadać różne poziomy istotności. Istnieją cztery poziomy istotności zdarzeń:

- *Zdarzenie krytyczne* to zdarzenie, które wskazuje wystąpienie krytycznego problemu mogącego prowadzić do utraty danych, problemów z działaniem lub błędu krytycznego.
- *Błąd funkcjonalny* to zdarzenie, które wskazuje poważny problem, błąd lub problem z działaniem, który wystąpił podczas działania aplikacji lub podczas przeprowadzania procedury.
- *Ostrzeżenie* to zdarzenie, które niekoniecznie jest poważne, ale wskazuje możliwość wystąpienia potencjalnego problemu w przyszłości. Większość zdarzeń otrzymuje priorytet „Ostrzeżenie", jeśli aplikacja może zostać przywrócona bez utraty danych lub możliwości funkcyjnych aplikacji.
- *Informacja* to zdarzenie, którego celem jest informowanie o pomyślnym zakończeniu działania, właściwym funkcjonowaniu aplikacji lub zakończeniu procedury.

Każde zdarzenie posiada zdefiniowany okres przechowywania, w trakcie którego możesz przejrzeć lub zmodyfikować to zdarzenie w Kaspersky Security Center. Niektóre zdarzenia nie są domyślnie zapisywane w bazie danych Serwera administracyjnego, ponieważ ich zdefiniowany okres przechowywania wynosi zero. Tylko te zdarzenia, które będą przechowywane w bazie danych Serwera administracyjnego przynajmniej jeden dzień, mogą zostać wyeksportowane do systemów zewnętrznych.

Używanie wyborów zdarzeń

Wybory zdarzeń oferują widok ekranowy nazwanych zestawów zdarzeń, które są wybrane z bazy danych Serwera administracyjnego. Te zestawy zdarzeń są grupowane zgodnie z następującymi kategoriami:

- Według istotności—**Zdarzenia krytyczne**, **Błędy funkcjonalne**, **Ostrzeżenia** i **Informacja o zdarzeniach**
- Według czasu—**Ostatnie zdarzenia**
- Według typu—**Żądania użytkownika** and **Zdarzenia audytu**

Możesz tworzyć i przeglądać wybory zdarzeń zdefiniowane przez użytkownika oparte na ustawieniach dostępnych do konfiguracji w interfejsie Kaspersky Security Center Web Console.

Wybory zdarzeń są dostępne w Kaspersky Security Center Web Console w sekcji **Monitorowanie i raportowanie** po kliknięciu **Wybory zdarzeń**.

Domyślnie, wybory zdarzeń zawierają informacje dla ostatnich siedmiu dni.

Kaspersky Security Center posiada domyślny (predefiniowany) zestaw wyborów zdarzeń:

- Zdarzenia z różnymi priorytetami:
  - **Zdarzenia krytyczne**
  - **Błędy funkcjonalne**
  - **Ostrzeżenia**
  - **Zdarzenia informacyjne**
- **Żądania użytkownika** (zdarzenia zarządzanych aplikacji)
- **Ostatnie zdarzenia** (w ostatnim tygodniu)
- Zdarzenia audytu.

Możesz także utworzyć i skonfigurować dodatkowe wybory zdefiniowane przez użytkownika. W wyborach zdefiniowanych przez użytkownika możesz filtrować zdarzenia według właściwości urządzeń, z których pochodzą (nazwy urządzeń, zakresy IP i grupy administracyjne), według typów zdarzeń i priorytetów, według aplikacji i nazwy komponentu oraz według przedziału czasu. Możliwe jest także uwzględnienie wyników zadania w obszarze wyszukiwania. Możesz także użyć pola prostego wyszukiwania, gdzie można wpisać słowo lub kilka słów. Zostaną wyświetlone wszystkie zdarzenia, które zawierają dowolne z wpisanych słów w swoich atrybutach (takie jak: nazwa zdarzenia, opis, nazwa komponentu).

Dla predefiniowanych wyborów oraz wyborów zdefiniowanych przez użytkownika możesz ograniczyć liczbę wyświetlanych zdarzeń lub liczbę wyszukiwanych wpisów. Obie opcje wpływają na czas, jakie zajmuje programowi Kaspersky Security Center wyświetlanie zdarzeń. Im większa baza danych, tym więcej czasu może zająć proces.

Możesz wykonać następujące czynności:

- Edytuj właściwości wyborów zdarzeń
- Wygeneruj wybory zdarzeń

- Zobacz szczegóły wyborów zdarzeń
- Usuń wybory zdarzeń
- Usuń zdarzenia z bazy danych Serwera administracyjnego

Tworzenie kryterium wyboru zdarzenia

W celu utworzenia wyboru zdarzeń:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Wybory zdarzeń**.
2. Kliknij **Dodaj**.
3. W otwartym oknie **Nowy wybór zdarzeń** określ ustawienia nowego wyboru zdarzeń. Wykonaj te czynności w jednej lub kilku sekcjach w oknie.
4. Kliknij **Zapisz**, aby zachować zmiany.

   Zostanie otwarte okno potwierdzenia.
5. Aby sprawdzić wynik wyboru zdarzenia, pozostaw pole **Przejdź do wyniku wyboru** zaznaczone.
6. Kliknij **Zapisz**, aby potwierdzić tworzenie wyboru zdarzenia.

Jeśli pozostawiłeś pole **Przejdź do wyniku wyboru** zaznaczone, zostanie wyświetlony wynik wyboru zdarzenia. Jeśli tak się nie stanie, nowy wybór zdarzenia pojawi się na liście wyborów zdarzeń.

Edytowanie kryterium wyboru zdarzenia

W celu edytowania kryterium wyboru zdarzenia:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Wybory zdarzeń**.
2. Zaznacz pole obok wyboru zdarzeń, który chcesz edytować.
3. Kliknij przycisk **Właściwości**.

   Zostanie otwarte okno ustawień wyboru zdarzenia.
4. Edytuj właściwości wyboru zdarzenia.

   > Dla predefiniowanych wyborów zdarzeń możesz edytować tylko właściwości na następujących zakładkach: **Ogólne** (za wyjątkiem nazwy wyboru), **Czas** i **Prawa dostępu**.

   Dla wyborów zdefiniowanych przez użytkownika możesz edytować wszystkie właściwości.
5. Kliknij **Zapisz**, aby zachować zmiany.

Edytowany wybór zdarzenia zostanie wyświetlony na liście.

Przeglądanie listy wyboru zdarzeń

W celu przejrzenia wyboru zdarzeń:

1. W menu głównym przejdź do **Monitorowanie i raportowanie → Wybory zdarzeń**.
2. Zaznacz pole obok wyboru zdarzeń, który chcesz uruchomić.
3. Wykonaj jedną z poniższych czynności:
   - Jeśli chcesz skonfigurować sortowanie w wyniku wyboru zdarzeń, wykonaj następujące czynności:
     a. Kliknij przycisk **Skonfiguruj sortowanie i uruchom**.
     b. W wyświetlonym oknie **Skonfiguruj sortowanie wyboru zdarzeń** określ ustawienia sortowania.
     c. Kliknij nazwę wyboru.
   - W innej sytuacji, jeśli chcesz przejrzeć listę zdarzeń posortowanych na Serwerze administracyjnym, kliknij nazwę wyboru.

Zostanie wyświetlony wynik wyboru zdarzeń.

Eksportowanie wyboru zdarzeń

Kaspersky Security Center umożliwia zapisanie wyboru zdarzeń i jego ustawień w pliku KLO. Możesz użyć tego pliku KLO do zaimportowania zapisanego wyboru zdarzeń zarówno do Kaspersky Security Center Windows, jak i Kaspersky Security Center Linux.

> Należy pamiętać, że możesz eksportować tylko wybory zdarzeń zdefiniowane przez użytkownika. Wybory zdarzeń z domyślnego zestawu Kaspersky Security Center (wybory predefiniowane) nie mogą zostać zapisane do pliku.

W celu wyeksportowania wyboru zdarzeń:

1. W menu głównym przejdź do **Monitorowanie i raportowanie → Wybory zdarzeń**.
2. Zaznacz pole obok wyboru zdarzeń, który chcesz wyeksportować.

   Nie można jednocześnie eksportować kilku wyborów zdarzeń. Jeśli wybierzesz więcej niż jeden zestaw, przycisk **Eksportuj** będzie nieaktywny.
3. Kliknij przycisk **Eksportuj**.
4. W otwartym oknie **Zapisz jako** określ nazwę i ścieżkę pliku wyboru zdarzeń, a następnie kliknij przycisk **Zapisz**.

   Okno **Zapisz jako** jest wyświetlane tylko wtedy, gdy korzystasz z przeglądarki Google Chrome, Microsoft Edge lub Opera. Jeśli używasz innej przeglądarki, plik wyboru zdarzeń jest automatycznie zapisywany w folderze **Pobrane**.

Importowanie wyboru zdarzeń

Kaspersky Security Center umożliwia import zestawu wybranych zdarzeń z pliku KLO. Plik KLO zawiera wyeksportowany zestaw wybranych zdarzeń i jego ustawienia.

W celu importowania wyboru zdarzeń:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Wybory zdarzeń**.
2. Kliknij przycisk **Importuj**, a następnie wybierz plik wyboru zdarzeń, który chcesz zaimportować.
3. W otwartym oknie określ ścieżkę do pliku KLO, a następnie kliknij przycisk **Otwórz**. Należy pamiętać, że można wybrać tylko jeden wybór zdarzeń.

   Rozpoczyna się przetwarzanie wyboru zdarzeń.

Pojawi się powiadomienie z wynikami importu. Jeśli wybór zdarzeń zostanie pomyślnie zaimportowany, możesz kliknąć odnośnik **Wyświetl szczegóły importu**, aby wyświetlić właściwości wyboru zdarzeń.

Po pomyślnym imporcie wybór zdarzeń zostanie wyświetlony na liście wyborów. Importowane są również ustawienia wyboru zdarzeń.

Jeżeli nowo importowany zdarzeń ma nazwę identyczną z nazwą istniejącego wyboru zdarzeń, nazwa importowanego wyboru zdarzeń jest rozszerzana o indeks **(<następny numer sekwencji>)**, na przykład: **(1)**, **(2)**.

Przeglądanie szczegółów zdarzenia

W celu przejrzenia szczegółów zdarzenia:

1. Uruchom wybór zdarzeń.
2. Kliknij czas żądanego zdarzenia.

   Zostanie otwarte okno **Właściwości zdarzenia**.
3. W wyświetlonym oknie możesz wykonać następujące czynności:
   - Przejrzeć informacje o wybranym zdarzeniu
   - Przejść do kolejnych i poprzednich zdarzeń w wyniku wyboru zdarzeń
   - Przejść do urządzenia, na którym wystąpiło zdarzenie
   - Przejść do grupy administracyjnej, która zawiera urządzenie, na którym wystąpiło zdarzenie
   - W przypadku zdarzenia związanego z zadaniem przejdź do właściwości zadania

Eksportowanie zdarzeń do pliku

Kaspersky Security Center umożliwia zapisywanie zdarzeń z wybranego wyboru zdarzeń do pliku TXT.

W celu wyeksportowania zdarzeń do pliku:

1. Uruchom wybór zdarzeń.
2. Zaznacz pole obok żądanego zdarzenia.

   Można również zaznaczyć kilka wydarzeń lub cały wybór wydarzeń.
3. Kliknij przycisk **Eksportuj do pliku**.

Wybrane zdarzenie zostanie wyeksportowane do pliku TXT.

Przeglądanie historii obiektu ze zdarzenia

Ze zdarzenia utworzenia lub modyfikacji obiektu, które obsługuje zarządzanie rewizją, możesz przełączyć się na historię rewizji obiektu.

W celu przejrzenia historii obiektu ze zdarzenia:

1. Uruchom wybór zdarzeń.
2. Zaznacz pole obok żądanego zdarzenia.
3. Kliknij przycisk **Historia rewizji**.

Historia rewizji obiektu zostanie otwarta.

Usuwanie zdarzeń

W celu usunięcia jednego lub kilku zdarzeń:

1. Uruchom wybór zdarzeń.
2. Zaznacz pola obok żądanych zdarzeń.
3. Kliknij przycisk **Usuń**.

Wybrane zdarzenia zostaną usunięte i nie można ich przywrócić.

Usuwanie wyborów zdarzeń

Możesz usuwać tylko wybory zdarzeń zdefiniowane przez użytkownika. Predefiniowanych wyborów zdarzeń nie można usunąć.

W celu usunięcia jednego lub kilku wyborów zdarzeń:

1. W menu głównym przejdź do **Monitorowanie i raportowanie → Wybory zdarzeń**.
2. Zaznacz pola obok wyborów zdarzeń, które chcesz usunąć.
3. Kliknij **Usuń**.
4. W otwartym oknie potwierdzenia kliknij **OK**.

   Wybór zdarzenia zostanie usunięty.

Ustawianie czasu przechowywania dla zdarzenia

Kaspersky Security Center umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Informacje o zdarzeniach są zapisywane w bazie danych Serwera administracyjnego. Konieczne może być przechowywanie niektórych zdarzeń przez dłuższy lub krótszy okres niż określony przez wartości domyślne. Możesz zmienić domyślne ustawienia czasu przechowywania zdarzenia.

Jeśli nie masz zamiaru przechowywać niektórych zdarzeń w bazie danych Serwera administracyjnego, możesz wyłączyć odpowiednie ustawienie w zasadzie Serwera administracyjnego oraz w zasadzie aplikacji Kaspersky lub we właściwościach Serwera administracyjnego (tylko dla zdarzeń Serwera administracyjnego). Zmniejszy to liczbę typów zdarzeń w bazie danych.

Im dłuższy okres przechowywania zdarzenia, tym szybciej baza danych osiągnie maksymalną pojemność. Jednakże dłuższy okres przechowywania zdarzenia umożliwia monitorowanie i raportowanie zadań dla dłuższego przedziału czasu.

W celu skonfigurowania czasu przechowywania zdarzenia w bazie danych Serwera administracyjnego:

1. W menu głównym przejdź do **Zasoby (urządzenia) → Profile zasad**.
2. Kliknij nazwę żądanej zasady.

   Możesz wybrać zasady zarządzanej aplikacji Kaspersky, Agenta sieciowego lub Serwera administracyjnego. W przypadku Serwera administracyjnego można również skonfigurować okres przechowywania zdarzeń, klikając ikonę ustawień () obok nazwy wymaganego Serwera administracyjnego.
3. Wybierz zakładkę **Konfiguracja zdarzenia**.

   Zostanie wyświetlona lista typów zdarzeń dotyczących sekcji **Krytyczny**. W razie potrzeby możesz przejść do sekcji **Błąd funkcjonalny**, **Ostrzeżenie** lub **Informacja**.

4. Na liście typów zdarzeń w prawej części okna kliknij odnośnik dla zdarzenia, którego okres przechowywania chcesz zmienić.

   W sekcji **Rejestracja zdarzenia** otwartego okna dostępny jest przycisk **Przechowuj w bazie danych Serwera administracyjnego przez (dni)**.

5. W polu edycji znajdującym się pod tym przyciskiem przełącznika wprowadź liczbę dni, przez jaką zdarzenie ma być przechowywane.

6. Jeśli nie chcesz przechowywać zdarzenia w bazie danych Serwera administracyjnego, wyłącz opcję **Przechowuj w bazie danych Serwera administracyjnego przez (dni)**.

   Jeśli konfigurujesz zdarzenia Serwera administracyjnego w oknie właściwości Serwera administracyjnego i jeśli ustawienia zdarzeń są blokowane w zasadzie Serwera administracyjnego Kaspersky Security Center, nie możesz ponownie zdefiniować wartości okresu przechowywania dla zdarzenia.

7. Kliknij przycisk **OK**, a następnie po zamknięciu prawego panelu kliknij przycisk **Zapisz**.

   Okno właściwości zasady zostanie zamknięte.

Od tej chwili, gdy serwer administracyjny odbiera i przechowuje zdarzenia wybranego typu, będą one miały zmieniony okres przechowywania. Serwer administracyjny nie zmienia okresu przechowywania wcześniej odebranych zdarzeń.

Zdarzenia składników Kaspersky Security Center

Każdy komponent Kaspersky Security Center posiada swój zestaw typów zdarzeń. W tej sekcji wymienione są typy zdarzeń, które występują w Serwerze administracyjnym Kaspersky Security Center, Agencie sieciowym i serwerze iOS MDM. Typy zdarzeń, które występują w aplikacjach Kaspersky, nie zostały wymienione w tej sekcji.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Struktura danych opisu typu zdarzeń

Dla każdego typu zdarzenia dostarczone są następujące elementy: wyświetlana nazwa, identyfikator (ID), kod alfabetyczny, opis oraz domyślny czas przechowywania.

- **Nazwa wyświetlanego typu zdarzenia**. Ten tekst jest wyświetlany w Kaspersky Security Center, gdy konfigurujesz zdarzenia oraz podczas występowania zdarzeń.
- **ID typu zdarzenia**. Ten kod numeryczny jest używany, gdy przetwarzasz zdarzenia przy użyciu narzędzi firm trzecich do analizy zdarzeń.
- **Typ zdarzenia** (kod alfabetyczny). Ten kod jest używany, gdy przeglądasz i przetwarzasz zdarzenia, korzystając z widoków publicznych, dostępnych w bazie danych Kaspersky Security Center, a także podczas eksportowania zdarzeń do systemu SIEM.
- **Opis**. Ten tekst zawiera sytuacje, gdy zdarzenie wystąpi i co należy zrobić w takiej sytuacji.

- **Domyślny czas przechowywania**. To jest liczba dni, przez jaką zdarzenie jest przechowywane w bazie danych Serwera administracyjnego i jest wyświetlane na liście zdarzeń na Serwerze administracyjnym. Po upłynięciu tego czasu, zdarzenie jest usuwane. Jeśli wartość czasu przechowywania zdarzenia to 0, takie zdarzenia są wykrywane, ale nie są wyświetlane na liście zdarzeń na Serwerze administracyjnym. Jeśli skonfigurowałeś zapisywanie takich zdarzeń w dzienniku zdarzeń systemu operacyjnego, znajdziesz je tam.

  Możesz zmienić czas przechowywania zdarzeń:

  - Konsola administracyjna: Ustawianie czasu przechowywania dla zdarzenia
  - Kaspersky Security Center Web Console: Ustawianie czasu przechowywania dla zdarzenia

Inne dane mogą zawierać następujące pola:

- **event_id**: unikatowa liczba zdarzeń w bazie danych, wygenerowana i przypisana automatycznie; nie mylić z **ID typu zdarzenia**.
- **task_id**: identyfikator zadania, które spowodowało wystąpienie zdarzenia (jeśli są jakiekolwiek)
- **severity**: jeden z następujących priorytetów (w kolejności rosnącej):

  0) Niepoprawny priorytet

  1) Informacja

  2) Ostrzeżenie

  3) Błąd

  4) Krytyczny

Zdarzenia Serwera administracyjnego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Serwera administracyjnego.

Zdarzenia krytyczne Serwera administracyjnego

Poniższa tabela wyświetla zdarzenia Serwera administracyjnego Kaspersky Security Center, które posiadają priorytet **Krytyczny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Jeśli określono port w oknie właściwości Serwera administracyjnego w Konsoli administracyjnej, **Kaspersky Security Center opublikuje metryki** i zdarzenia krytyczne, które mają zostać pozyskane przez Prometheus, system monitorowania i ostrzegania. Prometheus pozyskuje metryki i zdarzenia krytyczne, a następnie generuje ostrzeżenia dla każdego zdarzenia.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Zdarzenia krytyczne Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Limit licencji został przekroczony	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Raz dziennie Kaspersky Security Center sprawdza, czy limity licencji nie zostały przekroczone. Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre ograniczenia licencyjne są przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją przekracza 110% całkowitej liczby jednostek objętych licencją. Nawet jeśli to zdarzenie wystąpi, urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu. • Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center określa reguły generowania zdarzeń, gdy limit licencji zostanie przekroczony.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Epidemia wirusa	26 (dla Ochrony plików)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	180 dni
Epidemia wirusa	27 (dla Ochrony poczty)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	180 dni
Epidemia wirusa	28 (dla Zapory sieciowej)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	180 dni
Zarządzanie urządzeniem nie jest możliwe	4111	KLSRV_HOST_OUT_CONTROL	Zdarzenia tego typu występują, jeśli zarządzane urządzenie jest widoczne w sieci, ale nie ma podłączonego Serwera administracyjnego przez pewien czas. Dowiedz się, co uniemożliwia poprawne działanie Agenta sieciowego na urządzeniu. Możliwe przyczyny obejmują problemy z siecią i usuwanie Agenta sieciowego z urządzenia.	180 dni
Stan urządzenia: Krytyczny	4113	KLSRV_HOST_STATUS_CRITICAL	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan *Krytyczny*. Możesz skonfigurować warunki, zgodnie z którymi stan urządzenia zostanie zmieniony na *Krytyczny*.	180 dni
Plik klucza został dodany do listy zablokowanych	4124	KLSRV_LICENSE_BLACKLISTED	Zdarzenia tego typu występują, gdy firma Kaspersky dodała kod aktywacyjny lub plik klucza, którego używasz, do listy zablokowanych. Aby uzyskać więcej informacji, skontaktuj się z działem pomocy technicznej.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Tryb ograniczonej funkcjonalności	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Zdarzenia tego typu występują, gdy Kaspersky Security Center zaczyna działać z podstawową funkcjonalnością, bez funkcji Zarządzanie lukami i poprawkami oraz bez funkcji Zarządzanie urządzeniami mobilnymi. Poniższe elementy są przyczynami i odpowiednimi odpowiedziami na zdarzenie: • Okres licencji wygasł. Zapewnij licencję do korzystania z trybu pełnej funkcjonalności Kaspersky Security Center (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). • Serwer administracyjny zarządza większą liczbą urządzeń niż określona przez ograniczenie licencji. Przenieś urządzenia z grup administracyjnych Serwera administracyjnego do tych należących do innego Serwera administracyjnego (jeśli ograniczenie licencji innego Serwera administracyjnego zezwala na to).	180 dni
Licencja wkrótce utraci ważność	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Tego typu zdarzenia mają miejsce, gdy zbliża się data wygaśnięcia licencji komercyjnej. Raz dziennie Kaspersky Security Center sprawdza, czy nie zbliża się data wygaśnięcia licencji. Wydarzenia tego typu publikowane są 30 dni, 15 dni, 5 dni i 1 dzień przed datą wygaśnięcia licencji. Nie możesz zmienić liczby dni. Jeśli Serwer administracyjny zostanie wyłączony określonego dnia przed datą wygaśnięcia licencji, zdarzenie nie zostanie opublikowane, aż do następnego dnia. Po wygaśnięciu licencji komercyjnej Kaspersky Security Center zapewnia tylko podstawową funkcjonalność. Możesz zareagować na zdarzenie w następujące sposoby: • Upewnij się, że zapasowy klucz licencyjny został dodany do Serwera administracyjnego. • Jeśli korzystasz z subskrypcji, pamiętaj o jej odnowieniu. Nieograniczona subskrypcja jest odnawiana automatycznie, jeśli została opłacona w odpowiednim terminie.	180 dni
Certyfikat wygasł	4132	KLSRV_CERTIFICATE_EXPIRED	Wydarzenia tego typu występują, gdy certyfikat mobilny klienta na urządzeniu mobilnym wygaśnie.	180 dni
Certyfikat Serwera administracyjnego wygasł.	6129	ServerCertificateExpired	Zdarzenia tego typu występują, gdy certyfikat Serwera administracyjnego dla urządzeń mobilnych i urządzeń UEFI utraci ważność. Należy zaktualizować certyfikat, który utracił ważność.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Aktualizacje dla modułów aplikacji Kaspersky zostały wycofane	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Zdarzenia tego typu występują, jeśli aktualizacje typu seamless zostały wycofane (dla tych aktualizacji wyświetlany jest stan *Wycofano*) przez specjalistów z pomocy technicznej Kaspersky; na przykład, muszą zostać zaktualizowane do nowszej wersji. Zdarzenie dotyczy poprawek Kaspersky Security Center i nie dotyczy modułów zarządzanych aplikacji firmy Kaspersky. Zdarzenie zawiera przyczynę niezainstalowania aktualizacji typu seamless.	180 dni
Audyt: Eksport do SIEM nie powiódł się	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Zdarzenia tego typu mają miejsce, gdy eksport zdarzeń do systemu SIEM nie powiódł się z powodu błędu połączenia z systemem SIEM.	180 dni

Zdarzenia błędu funkcjonalnego Serwera administracyjnego

Poniższa tabela wyświetla zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Błąd funkcjonalny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia błędu funkcjonalnego Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Błąd w czasie wykonywania	4125	KLSRV_RUNTIME_ERROR	Zdarzenia tego typu występują w wyniku nieznanych problemów. Najczęściej są to problemy z systemem DBMS, problemy z siecią oraz inne problemy z oprogramowaniem i sprzętem. Szczegóły zdarzenia można znaleźć w opisie zdarzenia.	180 dni
Przekroczono limit instalacji dla jednej z grup licencjonowanych aplikacji	4126	KLSRV_INVLICPROD_EXCEDED	Serwer administracyjny generuje zdarzenia tego typu okresowo (co godzinę). Zdarzenia tego typu występują, jeśli w Kaspersky Security Center zarządzasz kluczami licencyjnymi aplikacji innych firm i jeśli liczba instalacji przekroczyła ograniczenie ustawione przez klucz licencyjny aplikacji innej firmy. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń aplikację innej firmy z urządzeń, na których aplikacja nie jest używana. • Użyj licencji innej firmy dla większej liczby urządzeń. Możesz zarządzać kluczami licencyjnymi aplikacji firm trzecich, korzystając z funkcjonalności grup licencjonowanych aplikacji. Grupa licencjonowanych aplikacji zawiera aplikacje firm trzecich spełniające kryteria ustalone przez Ciebie.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Przeszukanie segmentu chmury nie powiodło się	4143	KLSRV_KLCLOUD_SCAN_ERROR	Zdarzenia tego typu mają miejsce, gdy serwer administracyjny nie może przeszukać segmentu sieci w środowisku chmury. Przeczytaj szczegóły w opisie zdarzenia i zareaguj odpowiednio.	Nie jest przechowywany
Kopiowanie aktualizacji do określonego folderu nie powiodło się	4123	KLSRV_UPD_REPL_FAIL	Zdarzenia tego typu występują, gdy aktualizacje oprogramowania są kopiowane do dodatkowych folderów współdzielonych. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy konto użytkownika, który ma uzyskać dostęp do folderu(ów) posiada prawo do zapisu. • Sprawdź, czy nazwa użytkownika i/lub hasło do folderu/-ów nie uległy zmianie. • Sprawdź połączenie z internetem, gdyż to może być przyczyną zdarzenia. Aby zaktualizować bazy danych i moduły oprogramowania, postępuj zgodnie z instrukcjami.	180 dni
Brak wolnego miejsca na dysku	4107	KLSRV_DISK_FULL	Tego typu zdarzenia występują, gdy dysk twardy urządzenia, na którym jest zainstalowany Serwer administracyjny, zabraknie wolnego miejsca. Zwolnij miejsce na dysku na urządzeniu.	180 dni
Folder współdzielony nie jest dostępny	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Zdarzenia tego typu występują, jeśli folder współdzielony Serwera administracyjnego jest niedostępny. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy Serwer administracyjny (na którym znajduje się folder współdzielony) jest włączony i dostępny. • Sprawdź, czy nazwa użytkownika i/lub hasło do folderu uległy zmianie. • Sprawdź połączenie sieciowe.	180 dni
Baza danych Serwera administracyjnego jest niedostępna	4109	KLSRV_DATABASE_UNAVAILABLE	Zdarzenia tego typu występują, jeśli baza danych Serwera administracyjnego stała się niedostępna. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy zdalny serwer, na którym jest zainstalowany serwer SQL, jest dostępny. • Przejrzyj raporty systemu DBMS, aby odkryć przyczynę braku dostępności bazy danych Serwera administracyjnego. Na przykład, ze względu na profilaktyczną obsługę, zdalny serwer z zainstalowanym serwerem SQL może być niedostępny.	180 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Brak wolnego miejsca w bazie danych Serwera administracyjnego	4110	KLSRV_DATABASE_FULL	Zdarzenia tego typu występują, gdy nie ma wolnego miejsca w bazie danych Serwera administracyjnego. Serwer administracyjny nie działa, gdy jego baza danych osiągnęła swoją pojemność i gdy dalsze zapisywanie w bazie danych nie jest możliwe. Poniżej wymienione są przyczyny tego zdarzenia, w zależności od systemu DBMS, którego używasz, oraz odpowiednie reakcje na to zdarzenie: • Korzystasz z SQL Server Express Edition DBMS: W dokumentacji SQL Server Express sprawdź ograniczenie rozmiaru bazy danych dla wersji, której używasz. Prawdopodobnie Twoja baza danych Serwera administracyjnego przekroczyła ograniczenie rozmiaru bazy danych. Ograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. W bazie danych Serwera administracyjnego istnieje zbyt dużo zdarzeń wysłanych przez komponent Kontrola aplikacji. Możesz zmienić ustawienia zasady Kaspersky Endpoint Security for Windows dotyczące przechowywania zdarzeń Kontroli aplikacji w bazie danych Serwera administracyjnego. • Używasz systemu DBMS innego niż SQL Server Express Edition: Nieograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Zmniejszanie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Przeglądanie informacji dotyczących wyboru systemu DBMS.	180 dni

Zdarzenia ostrzegające Serwera administracyjnego

Poniższa tabela prezentuje zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Ostrzeżenie**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Wykryto często występujące zdarzenie		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje często występujące zdarzenie na zarządzanym urządzeniu. Aby uzyskać szczegółowe informacje, zapoznaj się z następującą sekcją: Blokowanie często występujących zdarzeń.	90 dni
Limit licencji został przekroczony	4098	KLSRV_EV_LICENSE_CHECK_100_110	Raz dziennie Kaspersky Security Center sprawdza, czy limity licencji nie zostały przekroczone. Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre ograniczenia licencyjne są przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją stanowi od 100% do 110% całkowitej liczby jednostek objętych licencją. Nawet jeśli to zdarzenie wystąpi, urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu. • Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center określa reguły generowania zdarzeń, gdy limit licencji zostanie przekroczony.	90 dni
Urządzenie było nieaktywne w sieci od dłuższego czasu	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Zdarzenia tego typu występują, gdy zarządzane urządzenie nie wykazuje brak aktywności przez pewien czas. Najczęściej dzieje się tak, gdy zarządzane urządzenie zostaje wycofane z eksploatacji. Możesz zareagować na zdarzenie w następujące sposoby: • W celu usunięcia urządzenia z listy zarządzanych urządzeń. • Określ przedział czasu, po którym tworzone jest zdarzenie **Urządzenie było nieaktywne w sieci od dłuższego czasu**, przy użyciu Konsoli administracyjnej lub przy użyciu Kaspersky Security Center Web Console. • Określ przedział czasu, po którym urządzenie zostanie automatycznie usunięte z grupy, przy użyciu Konsoli administracyjnej lub Kaspersky Security Center Web Console.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Konflikt nazw urządzeń	4102	KLSRV_EVENT_HOSTS_CONFLICT	Zdarzenia tego typu występują, gdy Serwer administracyjny traktuje dwa lub więcej zarządzanych urządzeń jako jedno urządzenie. Ma to miejsce najczęściej wtedy, gdy sklonowany dysk twardy został użyty do wdrożenia oprogramowania na zarządzanych urządzeniach i bez przełączania Agenta sieciowego do trybu klonowania dedykowanego dysku na odpowiednim urządzeniu. Aby uniknąć tego problemu, przełącz Agenta sieciowego do trybu klonowania dysku na odpowiednim urządzeniu przed sklonowaniem dysku twardego tego urządzenia.	90 dni
Stan urządzenia: Ostrzeżenie	4114	KLSRV_HOST_STATUS_WARNING	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan *Ostrzeżenie*. Możesz skonfigurować warunki, zgodnie z którymi stan urządzenia zostanie zmieniony na *Ostrzeżenie*.	90 dni
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony	4127	KLSRV_INVLICPROD_FILLED	Zdarzenia tego typu występują, gdy liczba instalacji aplikacji innych firm, zawartych w grupie licencjonowanych aplikacji osiągnie 90% maksymalnej dozwolonej wartości określonej we właściwościach klucza licencyjnego. Możesz zareagować na zdarzenie w następujące sposoby: • Jeśli aplikacja innej firmy nie jest używana na niektórych zarządzanych urządzeniach, usuń aplikację z tych urządzeń. • Jeśli spodziewasz się, że w najbliższej przyszłości liczba instalacji dla aplikacji innej firmy przekroczy dozwoloną maksymalną wartość, uwzględnij uzyskanie licencji innej firmy dla większej liczby urządzeń w przyszłości. Możesz zarządzać kluczami licencyjnymi aplikacji firm trzecich, korzystając z funkcjonalności grup licencjonowanych aplikacji.	90 dni
Certyfikat został zażądany	4133	KLSRV_CERTIFICATE_REQUESTED	Zdarzenia tego typu występują, gdy certyfikat dla Zarządzania urządzeniami mobilnymi nie zostanie automatycznie wystawiony ponownie. Poniżej znajdują się możliwe przyczyny wystąpienia tego zdarzenia oraz odpowiednie reakcje na nie: • Automatyczne ponowne wydawanie zostało zainicjowane dla certyfikatu, dla którego wyłączona jest opcja **Odnów certyfikat automatycznie, jeśli jest to możliwe**. Może to być spowodowane błędem, który wystąpił podczas tworzenia certyfikatu. Konieczne może być ręczne ponowne wystawienie certyfikatu. • Jeśli korzystasz z integracji z infrastrukturą klucza publicznego, przyczyną może być brak atrybutu SAM-Account-Name konta użytego do integracji z PKI oraz do wystawienia certyfikatu. Przejrzyj właściwości konta.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Certyfikat został usunięty	4134	KLSRV_CERTIFICATE_REMOVED	Zdarzenia tego typu występują, gdy administrator usunie dowolny typ certyfikatu (Ogólny, Poczta, VPN) dla Zarządzania urządzeniami mobilnymi. Po usunięciu certyfikatu urządzenia mobilne, podłączone za pośrednictwem tego certyfikatu, nie nawiążą połączenia z Serwerem administracyjnym. To zdarzenie może być pomocne podczas sprawdzania problemów z działaniem, skojarzonych z zarządzaniem urządzeń mobilnych.	90 dni
Certyfikat wygasa	6128	ServerCertificateExpiresSoon	Zdarzenia tego typu występują, gdy certyfikat Serwera administracyjnego dla urządzeń mobilnych i urządzeń UEFI utraci ważność. Należy zaktualizować certyfikat, który utracił ważność.	90 dni
Certyfikat APNs wygasł	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Zdarzenia tego typu występują, gdy certyfikat APNs utraci ważność. Należy ręcznie odnowić certyfikat APNs i zainstalować go na serwerze iOS MDM.	Nie jest przechowywany
Certyfikat APNs wkrótce utraci ważność	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Zdarzenia tego typu występują, gdy do wygaśnięcia certyfikatu APNs pozostało mniej niż 14 dni. Jeśli certyfikat APNs utraci ważność, należy ręcznie odnowić certyfikat APNs i zainstalować go na serwerze iOS MDM. Zalecane jest wcześniejsze utworzenie terminarza odnawiania certyfikatu APNs.	Nie jest przechowywany
Błąd podczas przesyłania wiadomości FCM do urządzenia mobilnego	4138	KLSRV_GCM_DEVICE_ERROR	Zdarzenia tego typu występują, gdy Zarządzanie urządzeniami mobilnymi jest skonfigurowane do użycia Firebase Cloud Messaging (FCM) w celu połączenia z zarządzanymi urządzeniami mobilnymi z systemem operacyjnym Android, a serwer FCM nie może obsłużyć niektórych żądań otrzymanych z Serwera administracyjnego. To oznacza, że niektóre zarządzane urządzenia mobilne nie otrzymają powiadomienia push. Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio. Więcej informacji na temat kodów HTTP otrzymanych z serwera FCM i powiązanych błędów można znaleźć w dokumentacji do usługi Firebase (zajrzyj do rozdziału „Podrzędne kody odpowiedzi na komunikaty o błędzie").	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Błąd HTTP podczas wysyłania wiadomości FCM do serwera FCM	4139	KLSRV_GCM_HTTP_ERROR	Zdarzenia tego typu występują, gdy Zarządzanie urządzeniami mobilnymi jest skonfigurowane do użycia Firebase Cloud Messaging (FCM) w celu połączenia z zarządzanymi urządzeniami mobilnymi z systemem operacyjnym Android, a serwer FCM przywróci żądanie Serwera administracyjnego z kodem HTTP innym niż 200 (OK). Poniżej znajdują się możliwe przyczyny wystąpienia tego zdarzenia oraz odpowiednie reakcje na nie: • Problemy po stronie serwera FCM. Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio. Więcej informacji na temat kodów HTTP otrzymanych z serwera FCM i powiązanych błędów można znaleźć w dokumentacji do usługi Firebase (zajrzyj do rozdziału „Podrzędne kody odpowiedzi na komunikaty o błędzie"). • Problemy po stronie serwera proxy (jeśli korzystasz z serwera proxy). Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio.	90 dni
Błąd podczas przesyłania wiadomości FCM do serwera FCM	4140	KLSRV_GCM_GENERAL_ERROR	Zdarzenia tego typu występują w wyniku niespodziewanych błędów po stronie Serwera administracyjnego podczas pracy z protokołem Firebase Cloud Messaging HTTP. Przeczytaj szczegóły w opisie zdarzenia i zareaguj odpowiednio. Jeżeli nie znajdziesz rozwiązania swojego problemu, skontaktuj się z działem pomocy technicznej firmy Kaspersky.	90 dni
Pozostała niewielka ilość wolnego miejsca na dysku twardym	4105	KLSRV_NO_SPACE_ON_VOLUMES	Tego typu zdarzenia występują, gdy dysk twardy urządzenia, na którym jest zainstalowany Serwer administracyjny, prawie zabraknie wolnego miejsca. Zwolnij miejsce na dysku na urządzeniu.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Mała ilość wolnego miejsca w bazie danych Serwera administracyjnego	4106	KLSRV_NO_SPACE_IN_DATABASE	Zdarzenia tego typu występują, jeśli miejsce w bazie danych Serwera administracyjnego jest zbyt ograniczone. Jeśli nie rozwiążesz tego problemu, wkrótce baza danych Serwera administracyjnego osiągnie swoją pojemność, a Serwer administracyjny nie będzie działał. Poniżej wymienione są przyczyny tego zdarzenia, w zależności od systemu DBMS, którego używasz, oraz odpowiednie reakcje na to zdarzenie. Korzystasz z SQL Server Express Edition DBMS: • W dokumentacji SQL Server Express sprawdź ograniczenie rozmiaru bazy danych dla wersji, której używasz. Prawdopodobnie Twoja baza danych Serwera administracyjnego zaraz osiągnie ograniczenie rozmiaru bazy danych. • Ograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • W bazie danych Serwera administracyjnego istnieje zbyt dużo zdarzeń wysłanych przez komponent Kontrola aplikacji. Możesz zmienić ustawienia zasady Kaspersky Endpoint Security for Windows dotyczące przechowywania zdarzeń Kontroli aplikacji w bazie danych Serwera administracyjnego. Używasz systemu DBMS innego niż SQL Server Express Edition: • Nieograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Przeglądanie informacji dotyczących wyboru systemu DBMS.	90 dni
Połączenie z podrzędnym Serwerem administracyjnym zostało zerwane	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Zdarzenia tego typu występują, gdy połączenie z podrzędnym Serwerem administracyjnym zostanie przerwane. Przeczytaj dziennik zdarzeń aplikacji Kaspersky na urządzeniu, na którym jest zainstalowany podrzędny Serwer administracyjny i zareaguj odpowiednio.	90 dni
Połączenie z głównym Serwerem administracyjnym zostało zerwane	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Zdarzenia tego typu występują, gdy połączenie z głównym Serwerem administracyjnym zostanie przerwane. Przeczytaj dziennik zdarzeń aplikacji Kaspersky na urządzeniu, na którym jest zainstalowany główny Serwer administracyjny i zareaguj odpowiednio.	90 dni
Zarejestrowano nowe aktualizacje dla modułów aplikacji Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Zdarzenia tego typu występują, gdy Serwer administracyjny zarejestruje nowe aktualizacje dla oprogramowania firmy Kaspersky, zainstalowanego na zarządzanych urządzeniach, których instalacja wymaga zatwierdzenia. Zatwierdź lub odrzuć aktualizacje, korzystając z Konsoli administracyjnej lub Kaspersky Security Center Web Console.	90 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Przekroczono limit wydarzeń w bazie danych. Rozpoczęto usuwanie wydarzeń	4145	KLSRV_EVP_DB_TRUNCATING	Zdarzenia tego typu występują, jeśli usuwanie starszych zdarzeń z bazy danych Serwera administracyjnego rozpoczęło się, gdy pojemność bazy danych Serwera administracyjnego została osiągnięta. Możesz zareagować na zdarzenie w następujące sposoby: • Zmiana maksymalnej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	Nie jest przechowywany
Przekroczono limit wydarzeń w bazie danych. Usunięto wydarzenia	4146	KLSRV_EVP_DB_TRUNCATED	Zdarzenia tego typu występują, jeśli starsze zdarzenia zostały usunięte z bazy danych Serwera administracyjnego po osiągnięciu pojemności bazy danych Serwera administracyjnego. Możesz zareagować na zdarzenie w następujące sposoby: • Zmiana maksymalnej dozwolonej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	Nie jest przechowywany
Audyt (połączenie testowe z serwerem SIEM nie powiodło się)	5120	KLAUD_EV_SIEM_TEST_FAILED	Zdarzenia tego typu mają miejsce w przypadku niepowodzenia połączenia testowego z serwerem SIEM.	30 dni
Nie udało się automatycznie wystawić certyfikatu		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Zdarzenia tego typu mają miejsce w przypadku wystąpienia błędu podczas tworzenia certyfikatu klienta dla urządzenia mobilnego (urządzenia działającego w oparciu o protokół mobilny).	90 dni

Zdarzenia informacyjne Serwera administracyjnego

Poniższa tabela prezentuje zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Informacja**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić i skonfigurować listę zdarzeń we właściwościach Serwera administracyjnego. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia informacyjne Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania	Uwagi
Ponad 90% tego klucza licencyjnego jest wykorzystane	4097	KLSRV_EV_LICENSE_CHECK_90	30 dni	
Wykryto nowe urządzenie	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 dni	
Urządzenie zostało automatycznie dodane do grupy	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 dni	

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania	Uwagi
Urządzenie zostało automatycznie przeniesione zgodnie z regułą	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 dni	
Urządzenie zostało usunięte z grupy: nieaktywność w sieci od dłuższego czasu	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 dni	
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony (wykorzystywanych jest więcej niż 95%)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 dni	
Wykryto pliki do przesłania do firmy Kaspersky w celu analizy	4131	KLSRV_APS_FILE_APPEARED	30 dni	
ID instancji FCM na tym urządzeniu mobilnym zmieniło się	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 dni	
Aktualizacje zostały pomyślnie skopiowane do wskazanego folderu	4122	KLSRV_UPD_REPL_OK	30 dni	
Nawiązano połączenie z podrzędnym Serwerem administracyjnym	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 dni	
Nawiązano połączenie z głównym Serwerem administracyjnym	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 dni	
Bazy danych zostały zaktualizowane	4144	KLSRV_UPD_BASES_UPDATED	30 dni	
Audyt: Połączenie z Serwerem administracyjnym zostało nawiązane	4147	KLAUD_EV_SERVERCONNECT	30 dni	Zdarzenia tego typu występują, gdy użytkownik łączy się z Serwerem administracyjnym za pomocą Konsoli administracyjnej lub Kaspersky Security Center Web Console. Do zdarzeń tych należy adres IP urządzenia, na którym zainstalowano Konsolę administracyjną opartą na MMC lub Kaspersky Security Center Web Console Server.
Audyt: Obiekt został zmodyfikowany	4148	KLAUD_EV_OBJECTMODIFY	30 dni	To zdarzenie śledzi zmiany w następujących obiektach: • Grupa administracyjna • Grupa bezpieczeństwa • Użytkownik • Pakiet • Zadanie • Zasada • Serwer • Wirtualny Serwer
Audyt: Stan obiektu zmienił się	4150	KLAUD_EV_TASK_STATE_CHANGED	30 dni	Na przykład to zdarzenie występuje, gdy zadanie nie powiodło się z powodu błędu.

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania	Uwagi
Audyt: Ustawienia grupy zostały zmodyfikowane	4149	KLAUD_EV_ADMGROUP_CHANGED	30 dni	
Audyt: Połączenie z Serwerem administracyjnym zostało zakończone	4151	KLAUD_EV_SERVERDISCONNECT	30 dni	
Audyt: Właściwości obiektu zostały zmodyfikowane	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 dni	To zdarzenie śledzi zmiany w następujących właściwościach: • Użytkownik • Licencja • Serwer • Wirtualny serwer
Audyt: uprawnienia użytkownika zostały zmodyfikowane	4153	KLAUD_EV_OBJECTACLMODIFIED	30 dni	
Audyt: Klucze szyfrowania zostały zaimportowane lub wyeksportowane z Serwera administracyjnego	5100	KLAUD_EV_DPEKEYSEXPORT	30 dni	
Audyt: połączenie testowe z serwerem SIEM powiodło się	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 dni	Zdarzenia tego typu mają miejsce w przypadku udanego połączenia testowego z serwerem SIEM.
Utworzono certyfikat zapasowy		ServerReserveCertificateCreated	30 dni	To zdarzenie występuje, gdy zostanie utworzony certyfikat Serwera administracyjnego.
Odnowienie certyfikatu		ServerCertificateRenewed	30 dni	To zdarzenie występuje, gdy zostanie odnowiony certyfikat Serwera administracyjnego.

Zdarzenia **Utworzono certyfikat zapasowy** oraz **Odnowienie certyfikatu** są automatycznie publikowane przez Serwer administracyjny i wyświetlane w Konsoli administracyjnej tylko wtedy, gdy operacje odpowiadające tym zdarzeniom zostaną wykonane dla certyfikatów Serwera administracyjnego dla urządzeń mobilnych i urządzeń UEFI.

Zdarzenia Agenta sieciowego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Agenta sieciowego.

Zdarzenia błędu funkcjonalnego Agenta sieciowego

Poniższa tabela wyświetla typy zdarzeń Agenta sieciowego Kaspersky Security Center, których priorytet to **Błąd funkcjonalny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny czas przechowywania
Błąd podczas instalacji aktualizacji	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli automatyczne aktualizowanie i instalowanie poprawek dla składników Kaspersky Security Center nie zakończyło się pomyślnie. Zdarzenie nie dotyczy aktualizacji zarządzanych aplikacji firmy Kaspersky. Przeczytaj opis zdarzenia. Przyczyną tego zdarzenia może być problem z systemem Windows na Serwerze administracyjnym. Jeśli w opisie wspomniany jest jakikolwiek problem z konfiguracją systemu Windows, rozwiąż ten problem.	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej nie powiodła się	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli używane są funkcje Zarządzanie lukami i poprawkami i Zarządzanie urządzeniami mobilnymi oraz jeśli aktualizacja oprogramowania innych firm nie zakończyła się pomyślnie. Sprawdź, czy odnośnik do oprogramowania innej firmy jest ważny. Przeczytaj opis zdarzenia.	30 dni
Zainstalowanie aktualizacji Windows Update nie powiodło się	7717	KLNAG_EV_WUA_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli aktualizacje systemu Windows nie zakończyły się pomyślnie. Konfiguruj aktualizacji systemu Windows w zasadzie Agenta sieciowego. Przeczytaj opis zdarzenia. Poszukaj błędu w Bazie wiedzy Microsoft. Skontaktuj się z pomocą techniczną Microsoft, jeśli sam nie możesz rozwiązać problemu.	30 dni
Zarządzanie użytkownikami: błędy	7723	KLNAG_EV_USR_MNG_ERR	Ogólne zdarzenie ostrzegające.	30 dni
Nie udało się przywrócić pliku sudoers do wartości referencyjnej	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Zdarzenie zawiera opis błędu zamiany pliku sudoers.	30 dni
Instalacja certyfikatów głównych nie powiodła się	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Zdarzenie zawiera opis błędu instalacji certyfikatów.	30 dni
Usunięcie certyfikatów głównych nie powiodło się	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Zdarzenie zawiera opis błędu usunięcia certyfikatów.	30 dni

Zdarzenia ostrzegające Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego Kaspersky Security Center, które posiadają priorytet **Ostrzeżenie**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia ostrzegające Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Proces instalacji aktualizacji modułów oprogramowania zwrócił ostrzeżenie	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została zakończona ostrzeżeniem	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została odroczona	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 dni
Wystąpił incydent związany z bezpieczeństwem	549	GNRL_EV_APP_INCIDENT_OCCURED	30 dni
Serwer KSN proxy został uruchomiony. Sprawdzenie dostępności KSN nie powiodło się	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 dni
Zarządzanie użytkownikami: ostrzeżenia	7722	KLNAG_EV_USR_MNG_WRN	30 dni
Plik Sudoers nie pasuje do wartości referencyjnej	7724	KLNAG_EV_SUDOER_DIFFERENT	30 dni

Zdarzenia informacyjne Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego Kaspersky Security Center, które posiadają priorytet **Informacja**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia informacyjne Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Aktualizacja modułów aplikacji została pomyślnie zainstalowana	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 dni
Instalacja aktualizacji modułów oprogramowania została uruchomiona	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 dni
Aplikacja została zainstalowana	7703	KLNAG_EV_INV_APP_INSTALLED	30 dni
Aplikacja została odinstalowana	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 dni
Monitorowana aplikacja została zainstalowana	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 dni
Monitorowana aplikacja została odinstalowana	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 dni
Aplikacja innego producenta została zainstalowana	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 dni
Dodano nowe urządzenie	7708	KLNAG_EV_DEVICE_ARRIVAL	30 dni
Urządzenie zostało usunięte	7709	KLNAG_EV_DEVICE_REMOVE	30 dni
Wykryto nowe urządzenie	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 dni
Urządzenie zostało zautoryzowane	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 dni
Udostępnianie pulpitu Windows: Plik został odczytany	7712	KLUSRLOG_EV_FILE_READ	30 dni
Udostępnianie pulpitu Windows: Plik został zmodyfikowany	7713	KLUSRLOG_EV_FILE_MODIFIED	30 dni
Udostępnianie pulpitu Windows: Aplikacja została uruchomiona	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 dni
Udostępnianie pulpitu Windows: Uruchomiono	7715	KLUSRLOG_EV_WDS_BEGIN	30 dni
Udostępnianie pulpitu Windows: Zatrzymano	7716	KLUSRLOG_EV_WDS_END	30 dni

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Aktualizacja oprogramowania firmy trzeciej została pomyślnie zainstalowana	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została uruchomiona	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 dni
Serwer KSN proxy został uruchomiony. Sprawdzenie dostępności KSN zostało pomyślnie zakończone	7719	KSNPROXY_STARTED_CON_CHK_OK	30 dni
KSN Proxy został zatrzymany	7720	KSNPROXY_STOPPED	30 dni

Zdarzenia serwera iOS MDM

Ta sekcja zawiera informacje o zdarzeniach dotyczących serwera iOS MDM.

Zdarzenia błędu funkcjonalnego serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Błąd funkcjonalny**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia błędu funkcjonalnego serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Pobranie listy profili nie powiodło się	PROFILELIST_COMMAND_FAILED	30 dni
Instalacja profilu nie powiodła się	INSTALLPROFILE_COMMAND_FAILED	30 dni
Usunięcie profilu nie powiodło się	REMOVEPROFILE_COMMAND_FAILED	30 dni
Pobranie listy profili informacyjnych nie powiodło się	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 dni
Instalacja profilu informacyjnego nie powiodła się	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 dni
Usunięcie profilu informacyjnego nie powiodło się	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 dni
Usunięcie profilu informacyjnego nie powiodło się	CERTIFICATELIST_COMMAND_FAILED	30 dni
Pobranie listy zainstalowanych aplikacji nie powiodło się	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 dni
Pobranie ogólnych informacji o urządzeniu mobilnym nie powiodło się	DEVICEINFORMATION_COMMAND_FAILED	30 dni
Pobranie informacji o zabezpieczeniach nie powiodło się	SECURITYINFO_COMMAND_FAILED	30 dni
Zablokowanie urządzenia mobilnego nie powiodło się	DEVICELOCK_COMMAND_FAILED	30 dni
Zresetowanie hasła nie powiodło się	CLEARPASSCODE_COMMAND_FAILED	30 dni
Usunięcie danych z urządzenia mobilnego nie powiodło się	ERASEDEVICE_COMMAND_FAILED	30 dni
Instalacja aplikacji nie powiodła się	INSTALLAPPLICATION_COMMAND_FAILED	30 dni
Ustawienie kodu wykupu dla aplikacji nie powiodło się	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 dni
Pobranie listy zarządzanych aplikacji nie powiodło się	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 dni
Usunięcie zarządzanej aplikacji nie powiodło się	REMOVEAPPLICATION_COMMAND_FAILED	30 dni
Ustawienia roamingu zostały odrzucone	SETROAMINGSETTINGS_COMMAND_FAILED	30 dni

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Wystąpił błąd działania aplikacji	PRODUCT_FAILURE	30 dni
Wynik polecenia zawiera niepoprawne dane	MALFORMED_COMMAND	30 dni
Przesłanie powiadomienia push nie powiodło się	SEND_PUSH_NOTIFICATION_FAILED	30 dni
Wysłanie polecenia nie powiodło się	SEND_COMMAND_FAILED	30 dni
Nie odnaleziono urządzenia	DEVICE_NOT_FOUND	30 dni

Zdarzenia ostrzegające serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Ostrzeżenie**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia ostrzegające serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Wykryto próbę podłączenia zablokowanego urządzenia mobilnego	INACTICE_DEVICE_TRY_CONNECTED	30 dni
Profil został usunięty	MDM_PROFILE_WAS_REMOVED	30 dni
Wykryto próbę ponownego użycia certyfikatu klienta	CLIENT_CERT_ALREADY_IN_USE	30 dni
Wykryto nieaktywne urządzenie	FOUND_INACTIVE_DEVICE	30 dni
Wymagany jest kod wykupu	NEED_REDEMPTION_CODE	30 dni
Profil zawarty w zasadach został usunięty z urządzenia	UMDM_PROFILE_WAS_REMOVED	30 dni

Zdarzenia informacyjne serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Informacja**.

Dla każdego zdarzenia, które może być generowane przez aplikację, określić można ustawienia powiadomień i ustawienia dot. przechowywania w zasadzie aplikacji, w karcie **Konfiguracja zdarzenia**. Jeśli chcesz skonfigurować ustawienia powiadomień dla wszystkich zdarzeń jednocześnie, skonfiguruj ogólne ustawienia powiadomień we właściwościach Serwera administracyjnego.

Zdarzenia informacyjne serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Podłączono nowe urządzenie mobilne	NEW_DEVICE_CONNECTED	30 dni
Lista profili została pomyślnie pobrana	PROFILELIST_COMMAND_SUCCESSFULL	30 dni
Profil został pomyślnie zainstalowany	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 dni
Profil został pomyślnie usunięty	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 dni
Lista profili informacyjnych została pomyślnie pobrana	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 dni
Profil informacyjny został pomyślnie zainstalowany	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dni
Profil informacyjny został pomyślnie usunięty	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dni
Lista certyfikatów cyfrowych została pomyślnie pobrana	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 dni

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Lista zainstalowanych aplikacji została pomyślnie zażądana	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dni
Ogólne informacje o urządzeniu mobilnym zostały pomyślnie pobrane	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 dni
Informacje o zabezpieczeniach zostały pomyślnie pobrane	SECURITYINFO_COMMAND_SUCCESSFULL	30 dni
Urządzenie mobilne zostało pomyślnie zablokowane	DEVICELOCK_COMMAND_SUCCESSFULL	30 dni
Hasło zostało pomyślnie zresetowane	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 dni
Dane zostały pomyślnie usunięte z urządzenia mobilnego	ERASEDEVICE_COMMAND_SUCCESSFULL	30 dni
Aplikacja została pomyślnie zainstalowana	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 dni
Kod wykupu aplikacji został pomyślnie ustawiony dla aplikacji	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 dni
Lista zarządzanych aplikacji została pomyślnie pobrana	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dni
Zarządzana aplikacja została pomyślnie usunięta	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 dni
Ustawienia roamingu zostały pomyślnie zastosowane	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 dni

Blokowanie często występujących zdarzeń

Ta sekcja zawiera informacje dotyczące zarządzania blokowaniem często występujących zdarzeń oraz usuwania blokowania często występujących zdarzeń.

Informacje o blokowaniu często występujących zdarzeń

Zarządzana aplikacja, na przykład Kaspersky Endpoint Security for Windows, zainstalowana na jednym lub kilku zarządzanych urządzeniach, może wysyłać wiele zdarzeń tego samego typu do Serwera administracyjnego. Otrzymywanie częstych zdarzeń może przeciążyć bazę danych Serwera administracyjnego i nadpisać inne zdarzenia. Serwer administracyjny zaczyna blokować najczęstsze zdarzenia, gdy liczba wszystkich odebranych zdarzeń przekracza określony limit dla bazy danych.

Serwer administracyjny blokuje automatyczne odbieranie często występujących zdarzeń. Nie możesz samodzielnie blokować często występujących zdarzeń ani wybierać, które zdarzenia mają być blokowane.

Jeśli chcesz dowiedzieć się, czy zdarzenie jest zablokowane, możesz sprawdzić listę powiadomień lub możesz sprawdzić, czy to zdarzenie jest obecne w sekcji **Blokowanie często występujących zdarzeń** właściwości Serwera administracyjnego. Jeśli zdarzenie jest zablokowane, możesz wykonać następujące czynności:

- Jeśli chcesz zapobiec nadpisywaniu bazy danych, możesz kontynuować blokowanie odbieranie tego typu zdarzeń.
- Jeśli chcesz, na przykład, znaleźć przyczynę wysyłania często występujących zdarzeń na Serwer administracyjny, możesz odblokować często występujące zdarzenia i mimo wszystko nadal otrzymywać tego typu zdarzenia.
- Jeśli chcesz nadal otrzymywać często występujące zdarzenia, dopóki nie zostaną ponownie zablokowane, możesz usunąć z blokowania często występujące zdarzenia.

Zarządzanie blokowaniem często występujących zdarzeń

Serwer administracyjny blokuje automatyczne odbieranie często występujących zdarzeń, ale możesz odblokować tę opcję i nadal odbierać często występujące zdarzenia. Możesz także zablokować odbieranie często występujących zdarzeń, które wcześniej odblokowałeś.

W celu zarządzania blokowaniem często występujących zdarzeń:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Blokowanie często występujących zdarzeń**
3. W sekcji **Blokowanie często występujących zdarzeń**:
   - Jeśli chcesz odblokować odbieranie często występujących zdarzeń:
     a. Wybierz często występujące zdarzenia, które chcesz odblokować, a następnie kliknij przycisk **Wyklucz**.
     b. Kliknij przycisk **Zapisz**.
   - Jeśli chcesz zablokować często występujące zdarzenia:
     a. Wybierz często występujące zdarzenia, które chcesz zablokować, a następnie kliknij przycisk **Zablokuj**.
     b. Kliknij przycisk **Zapisz**.

Serwer administracyjny odbiera odblokowane często występujące zdarzenia i nie odbiera zablokowanych często występujących zdarzeń.

Usuwanie blokowania często występujących zdarzeń

Możesz usunąć blokowanie często występujących zdarzeń i rozpocząć ich odbieranie, dopóki Serwer administracyjny nie zablokuje ponownie tych często występujących zdarzeń.

W celu usunięcia blokowania często występujących zdarzeń:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Blokowanie często występujących zdarzeń**

3. W sekcji **Blokowanie często występujących zdarzeń** wybierz typy często występujących zdarzeń, dla których chcesz usunąć blokowanie.

4. Kliknij przycisk **Usuń z blokowania**.

Często występujące zdarzenie zostanie usunięte z listy często występujących zdarzeń. Serwer administracyjny będzie odbierał zdarzenia tego typu.

Powiadomienia i stany urządzeń

Ta sekcja zawiera informacje o tym, jak przeglądać powiadomienia, konfigurować dostarczanie powiadomień, używać stanów urządzeń i włączać zmianę stanów urządzeń.

Korzystanie z powiadomień

Powiadomienia informują o zdarzeniach oraz pomagają w przyspieszeniu odpowiedzi na te zdarzenia poprzez wykonanie zalecanych działań lub działań, które uznajesz za odpowiednie.

W zależności od wybranej metody powiadamiania, dostępne są następujące typy powiadomień:

- Powiadomienia na ekranie
- Powiadomienia przez SMS
- Powiadomienia przez e-mail
- Powiadomienia przez uruchomienie pliku wykonywalnego lub skryptu

Powiadomienia na ekranie

Powiadomienia ekranowe informują o zdarzenia pogrupowanych według istotności (*Krytyczne*, *Ostrzeżenie* i *Komunikaty informacyjne*).

Powiadomienie ekranowe może przyjąć jeden z dwóch stanów:

- *Przejrzane*. Oznacza to, że wykonałeś zalecane działanie dla powiadomienia lub ręcznie przypisałeś ten stan do powiadomienia.
- *Nieprzejrzane*. Oznacza to, że nie wykonałeś zalecanego działania dla powiadomienia lub nie przypisałeś tego stanu do powiadomienia ręcznie.

Domyślnie, lista powiadomień zawiera powiadomienia ze stanem *Nieprzejrzane*.

Możesz monitorować sieć organizacji, przeglądając powiadomienia ekranowe i odpowiadając na nie w czasie rzeczywistym.

Powiadomienia przez e-mail, przez SMS i przez plik wykonywalny lub skrypt

Kaspersky Security Center oferuje możliwość monitorowania sieci organizacji, wysyłając powiadomienia o zdarzeniu, które uważasz za ważne. Dla każdego zdarzenia możesz skonfigurować powiadomienia przez e-mail, przez SMS lub przez uruchomienie pliku wykonywalnego lub skryptu.

Po otrzymaniu powiadomień przez e-mail lub przez SMS, możesz zdecydować, jaka będzie odpowiedź na zdarzenie. Ta odpowiedź powinna być najbardziej odpowiednia dla sieci Twojej organizacji. Uruchamiając plik wykonywalny lub skrypt, wcześniej definiujesz odpowiedź na zdarzenie. Możesz także rozważyć uruchomienie pliku wykonywalnego lub skryptu jako głównej odpowiedzi na zdarzenie. Po uruchomieniu pliku wykonywalnego, możesz podjąć inne kroki w celu odpowiedzi na zdarzenie.

Przeglądanie powiadomień na ekranie

Powiadomienia na ekranie można wyświetlać na trzy sposoby:

- W sekcji **Monitorowanie i raportowanie** → **Powiadomienia**. W tym miejscu możesz przejrzeć powiadomienia dotyczące predefiniowanych kategorii.
- W oddzielnym oknie, które może zostać otwarte niezależnie od sekcji, której używasz w danym momencie. W tym przypadku możesz oznaczyć powiadomienia jako przejrzane.
- W widżecie **Powiadomienia według wybranego priorytetu**, w sekcji **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**. W widżecie możesz przeglądać tylko powiadomienia o zdarzeniach na poziomach istotności *Krytyczny* i *Ostrzeżenie*.

Możesz wykonywać akcje, na przykład, odpowiadać na zdarzenie.

W celu przejrzenia powiadomień z predefiniowanych kategorii:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Powiadomienia**.

   Kategoria **Wszystkie powiadomienia** została wybrana w lewej części okna, a w prawej części okna są wyświetlane wszystkie powiadomienia.

2. W lewej części okna wybierz jedną z kategorii:

   - **Wdrażanie**
   - **Urządzenia**
   - **Ochrona**
   - **Aktualizacje** (ta kategoria zawiera powiadomienia dotyczące aplikacji Kaspersky, dostępnych do pobrania, i powiadomienia na temat pobranych aktualizacji antywirusowych baz danych)
   - **Ochrona przed exploitami**

- **Serwer administracyjny** (ta kategoria obejmuje zdarzenia dotyczące tylko Serwera administracyjnego)
- **Przydatne odnośniki** (ta kategoria obejmuje odnośniki do zasobów Kaspersky, na przykład pomocy technicznej Kaspersky, forum Kaspersky, strony odnowienia licencji lub Encyklopedii IT Kaspersky)

Zostanie wyświetlona lista powiadomień wybranej kategorii. Lista zawiera następujące elementy:

- Ikona związana z tematem powiadomienia: wdrożenie (), ochrona (), aktualizacje (), zarządzanie urządzeniami (), Ochrona przed exploitami (), Serwer administracyjny ().
- Poziom istotności powiadomienia. Wyświetlane są powiadomienia następujących poziomów istotności: **Powiadomienia krytyczne** (), **Powiadomienia ostrzegawcze** (), **Powiadomienia informacyjne**. Powiadomienia na liście są pogrupowane według poziomów istotności.
- **Powiadomienie**. Ta kategoria zawiera opis powiadomienia.
- **Akcja**. Ta kategoria zawiera odnośnik do akcji, której wykonanie zalecamy. Na przykład, klikając ten odnośnik, możesz przejść do repozytorium i zainstalować aplikacje zabezpieczające na urządzeniach lub przejrzeć listę urządzeń lub listę zdarzeń. Po wykonaniu zalecanego działania dla powiadomienia, do tego powiadomienia przypisano stan *Przejrzane*.
- **Zarejestrowany stan**. Ta kategoria zawiera liczbę dni lub godzin, które minęły od momentu, gdy powiadomienie zostało zarejestrowane na Serwerze administracyjnym.

W celu przejrzenia powiadomień ekranowych w oddzielnym oknie według poziomu istotności:

1. W prawym górnym rogu Kaspersky Security Center Web Console kliknij ikonę flagi ().

   Jeśli ikona flagi posiada czerwoną kropkę, oznacza to, że istnieją powiadomienia, które nie zostały przejrzane.

   Zostanie otwarte okno wyświetlające powiadomienia. Domyślnie wybrana jest zakładka **Wszystkie powiadomienia**, a powiadomienia są pogrupowane według poziomów istotności: *Krytyczne*, *Ostrzeżenie* i *Informacja*.

2. Wybierz zakładkę **System**.

   Zostanie wyświetlona lista z powiadomieniami posiadającymi poziom istotności powiadomienia *Krytyczne* () i *Ostrzeżenie* (). Lista powiadomień obejmuje następujące obiekty:

   - Znacznik koloru. Powiadomienia krytyczne są oznaczone na czerwono. Powiadomienia ostrzegające są oznaczone na żółto.
   - Ikona wskazująca temat powiadomienia: wdrożenie (), ochrona (), aktualizacje (), zarządzanie urządzeniami (), Ochrona przed exploitami (), Serwer administracyjny ().
   - Opis powiadomienia.
   - Ikona flagi. Ikona flagi jest szara, jeśli do powiadomień jest przypisany stan *Nieprzejrzane*. Jeśli wybierzesz szarą ikonę flagi i przypiszesz stan *Przejrzane* do powiadomienia, ikona zmieni kolor na biały.
   - Odnośnik do zalecanej akcji. Jeśli po kliknięciu odnośnika wykonasz zalecaną akcję, do powiadomienia zostanie przypisany stan *Przejrzane*.
   - Liczba dni, jaka minęła od daty zarejestrowania powiadomienia na Serwerze administracyjnym.

3. Wybierz zakładkę **Więcej**.

   Zostanie wyświetlona lista powiadomień posiadających poziom istotności *Informacja*.

   Organizacja listy jest taka sama, jak listy na zakładce **System** (zapoznaj się z powyższym opisem). Jedyna różnica to brak znacznika koloru.

Możesz filtrować powiadomienia według dat, gdy zostały zarejestrowane na Serwerze administracyjnym. Użyj pola **Pokaż filtr**, aby zarządzać filtrem.

W celu wyświetlenia powiadomień ekranowych na widżecie:

1. W sekcji **Pulpit nawigacyjny** wybierz **Dodaj lub przywróć widżet sieciowy**.

2. W otwartym oknie kliknij kategorię **Inne**, wybierz widżet **Powiadomienia według wybranego priorytetu** i kliknij Dodaj.

   Teraz widżet pojawi się na zakładce **Pulpit nawigacyjny**. Domyślnie, powiadomienia z poziomem istotności *Krytyczne* są wyświetlane na widżecie.

   Możesz kliknąć przycisk **Ustawienia** na widżecie i zmienić ustawienia widżetu, aby przejrzeć powiadomienia z poziomem istotności *Ostrzeżenie*. Lub możesz dodać inny widżet: **Powiadomienia według wybranego poziomu istotności** z priorytetem *Ostrzeżenie*.

   Lista powiadomień na widżecie jest ograniczona według rozmiaru i zawiera dwa powiadomienia. Te dwa powiadomienia odnoszą się do najnowszych zdarzeń.

Lista powiadomień na widżecie obejmuje następujące obiekty:

- Ikona związana z tematem powiadomienia: wdrożenie (), ochrona (), aktualizacje (), zarządzanie urządzeniami (), Ochrona przed exploitami (), Serwer administracyjny ().
- Opis powiadomienia z odnośnikiem do zalecanej akcji. Jeśli po kliknięciu odnośnika wykonasz zalecaną akcję, do powiadomienia zostanie przypisany stan *Przejrzane*.
- Liczbę dni lub liczbę godzin, które minęły od daty zarejestrowania powiadomienia na Serwerze administracyjnym.
- Odnośnik do innych powiadomień. Po kliknięciu tego odnośnika, zostajesz przeniesiony do widoku powiadomień w sekcji **Powiadomienia** sekcji **Monitorowanie i raportowanie**.

Informacje o stanach urządzeń

Kaspersky Security Center przypisze stan do każdego zarządzanego urządzenia. Określony stan zależy od tego, czy spełnione są warunki zdefiniowane przez użytkownika. W niektórych przypadkach, podczas przypisywania stanu do urządzenia, Kaspersky Security Center bierze pod uwagę flagę widoczności urządzenia w sieci (patrz tabela poniżej). Na przykład, jeśli do zarządzanego urządzenia został przypisany stan *Krytyczny*, ponieważ spełniony był warunek *Bazy danych są nieaktualne*, a później flaga widoczności została ustawiona dla urządzenia, wówczas do urządzenia zostanie przypisany stan *OK*. Jeśli Kaspersky Security Center nie znajdzie urządzenia w sieci w ciągu dwóch godzin, flaga widoczności urządzenia zostanie ustawiona na *Nie jest widoczne*.

Stany są następujące:

- *Krytyczny* lub *Krytyczny / Widoczne*
- *Ostrzeżenie* lub *Ostrzeżenie / Widoczne*
- *OK* lub *OK / Widoczne*

Poniższa tabela wyświetla domyślne warunki, które muszą być spełnione, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia, wraz ze wszystkimi możliwymi wartościami.

Warunki przypisania stanu do urządzenia

Warunek	Opis warunku	Dostępne wartości
Aplikacja zabezpieczająca nie jest zainstalowana	Agent sieciowy jest zainstalowany na urządzeniu, ale aplikacja zabezpieczająca nie jest zainstalowana.	• Przycisk przełącznika jest ustawiony w pozycji włączenia. • Przycisk przełącznika jest ustawiony w pozycji wyłączenia.
Wykryto zbyt wiele wirusów	Niektóre wirusy zostały wykryte na urządzeniu przez zadanie wykrywania wirusów, na przykład, zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* oraz liczba wykrytych wirusów przekraczają określoną wartość.	Większe niż 0.
Poziom ochrony w czasie rzeczywistym jest inny niż poziom zdefiniowany przez administratora	Urządzenie jest widoczne w sieci, ale poziom ochrony w czasie rzeczywistym różni się od poziomu ustawionego (w warunku) przez administratora dla stanu urządzenia.	• Zatrzymane. • Wstrzymane. • Uruchomione.
Skanowanie w poszukiwaniu złośliwego oprogramowania nie było wykonywane od dłuższego czasu	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale zadanie *Skanowanie w poszukiwaniu szkodliwego oprogramowania* ani zadanie lokalnego skanowania nie było uruchamiane w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego 7 dni temu lub wcześniej.	Więcej niż 1 dzień.
Bazy danych są nieaktualne	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale antywirusowe bazy danych nie były aktualizowane na tym urządzeniu w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego dzień wcześniej lub jeszcze wcześniej.	Więcej niż 1 dzień.
Niepołączony od dłuższego czasu	Agent sieciowy jest zainstalowany na urządzeniu, ale urządzenie nie było połączone z Serwerem administracyjnym w określonym przedziale czasu, ponieważ urządzenie było wyłączone.	Więcej niż 1 dzień.
Wykryto aktywne zagrożenia	Liczba nieprzetworzonych obiektów w folderze **Aktywne zagrożenia** przekracza określoną wartość.	Więcej niż 0 elementów.
Wymagane jest ponowne uruchomienie	Urządzenie jest widoczne w sieci, ale aplikacja wymaga ponownego uruchomienia urządzenia dłużej niż określony przedział czasu i z jednego z wybranych powodów.	Więcej niż 0 minut.
Zainstalowane są niekompatybilne aplikacje	Urządzenie jest widoczne w sieci, ale inwentaryzacja oprogramowania wykonywana poprzez Agenta sieciowego wykryła niekompatybilne aplikacje zainstalowane na urządzeniu.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto luki w oprogramowaniu	Urządzenie jest widoczne w sieci, a Agent sieciowy jest zainstalowany na urządzeniu, ale zadanie *Wyszukiwania luk i wymaganych aktualizacji* wykryło luki z określonym priorytetem w aplikacjach zainstalowanych na urządzeniu.	• Krytyczny. • Wysoki. • Średni. • Ignoruj, jeśli luka nie może być naprawiona. • Ignoruj, jeśli aktualizacja jest przypisana do instalacji.
Licencja utraciła ważność	Urządzenie jest widoczne w sieci, ale licencja utraciła ważność.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Licencja wkrótce utraci ważność	Urządzenie jest widoczne w sieci, ale licencja utraci ważność na urządzeniu za mniej niż określona liczba dni.	Mniej niż 0 dni.

Warunek	Opis warunku	Dostępne wartości
Wyszukiwanie aktualizacji Windows Update nie było przeprowadzane od dłuższego czasu	Urządzenie jest widoczne w sieci, ale zadanie *Wyszukiwania luk i wymaganych aktualizacji* nie było uruchamiane w zdefiniowanym przedziale czasu.	Więcej niż 1 dzień.
Nieprawidłowy stan szyfrowania	Agent sieciowy jest zainstalowany na urządzeniu, ale wynik szyfrowania urządzenia jest równy określonej wartości.	• Nie zgadza się z zasadą w wyniku odmowy użytkownika (tylko dla urządzeń zewnętrznych). • Nie zgadza się z zasadą w wyniku błędu. • Po zastosowaniu zasady wymagane jest ponowne uruchomienie. • Nie określono zasady szyfrowania. • Nieobsługiwany. • Po zastosowaniu zasady.
Ustawienia urządzenia mobilnego nie są zgodne z zasadą	Ustawienia urządzenia mobilnego są inne niż ustawienia, które zostały określone w zasadzie Kaspersky Endpoint Security for Android podczas sprawdzania reguł zgodności.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto nieprzetworzone incydenty związane z bezpieczeństwem	Na urządzeniu zostały wykryte pewne nieprzetworzone problemy bezpieczeństwa. Problemy bezpieczeństwa mogą być tworzone automatycznie poprzez zarządzane aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim, a także ręcznie przez administratora.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Stan urządzenia zdefiniowany przez aplikację	Stan urządzenia jest definiowany przez zarządzaną aplikację. Zarządzane urządzenia mogą mieć stan zdefiniowany przez zarządzane aplikacje, niezależnie od ustawień Kaspersky Security Center. Po zwróceniu przez ten stan jednego ze stanów zdefiniowanych przez Kaspersky Security Center, Serwer administracyjny przypisuje zarządzanemu urządzeniu najbardziej krytyczny stan spośród stanów zwróconych przez zarządzaną aplikację i przypisanych przez Serwer administracyjny. Stany zdefiniowane przez zarządzane aplikacje mają opisy przekazane przez zarządzane aplikacje. Możesz wyświetlić opisy na liście zarządzanych urządzeń, w kolumnie **Opis stanu**.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Brakuje miejsca na dysku urządzenia	Wolnego miejsca na dysku jest mniej niż określona wartość lub urządzenie nie mogło zostać zsynchronizowane z Serwerem administracyjnym. Stan *Krytyczny* lub *Ostrzeżenie* zmieniło się na stan *OK*, gdy urządzenie zostało pomyślnie zsynchronizowane z Serwerem administracyjnym, a wolna przestrzeń na urządzeniu jest większa niż lub równa określonej wartości.	Więcej niż 0 MB.
Zarządzanie urządzeniem nie jest możliwe	Podczas wykrywania urządzeń, urządzenie zostało rozpoznane jako widoczne w sieci, ale więcej niż trzy próby synchronizacji z Serwerem administracyjnym nie powiodły się.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Ochrona jest wyłączona	Urządzenie jest widoczne w sieci, ale aplikacja zabezpieczająca na urządzeniu została wyłączona na dłużej niż określony przedział czasu. W tym przypadku stan aplikacji zabezpieczającej to *zatrzymany* lub *błąd* i różni się od następujących: *uruchamianie*, *uruchomiony* lub *zawieszony*.	Więcej niż 0 minut.
Aplikacja zabezpieczająca nie jest uruchomiona	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale nie jest uruchomiona.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.

Kaspersky Security Center umożliwia skonfigurowanie automatycznego przełączania stanu urządzenia w grupie administracyjnej, gdy spełnione są określone warunki. Jeśli określone warunki są spełnione, do urządzenia klienckiego zostanie przypisany jeden z następujących stanów: *Krytyczny* lub *Ostrzeżenie*. Jeśli określone warunki zostaną spełnione, urządzeniu klienckiemu zostanie przypisany stan *OK*.

Różne stany mogą odpowiadać różnym wartościom jednego warunku. Na przykład, domyślnie, jeśli warunek **Bazy danych są nieaktualne** posiada wartość **Ponad 3 dni**, do urządzenia klienckiego zostaje przypisany stan *Ostrzeżenie*; jeśli wartość to **Ponad 7 dni**, wówczas zostanie przypisany stan *Krytyczny*.

Jeśli aktualizujesz Kaspersky Security Center z poprzedniej wersji, wartości warunku **Bazy danych są nieaktualne** dla przypisania stanu do *Krytyczne* lub *Ostrzeżenie* nie zmienią się.

Konfigurowanie przełączania stanów urządzeń

Możesz zmienić warunki, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia.

W celu włączenia zmiany stanu urządzenia na Krytyczny:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Hierarchia grup**.
2. Na otwartej liście grup kliknij odnośnik z nazwą grupy, dla której chcesz zmienić przełączanie stanów urządzeń.
3. W otwartym oknie właściwości wybierz zakładkę **Stan urządzenia**.
4. W lewej części okna wybierz **Krytyczny**.
5. W prawej części okna, w sekcji **Ustaw stan Krytyczny, jeśli** włącz warunek, aby przełączyć urządzenie do stanu *Krytyczny*.

   Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

6. Wybierz przycisk radiowy obok warunku na liście.
7. W lewym górnym rogu listy kliknij przycisk **Edytuj**.
8. Dla wybranego warunku ustaw żądaną wartość.

   Nie dla każdego warunku można ustawić wartości.

9. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Krytyczne*.

W celu włączenia zmiany stanu urządzenia na Ostrzeżenie:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Hierarchia grup**.
2. Na otwartej liście grup kliknij odnośnik z nazwą grupy, dla której chcesz zmienić przełączanie stanów urządzeń.
3. W otwartym oknie właściwości wybierz zakładkę **Stan urządzenia**.
4. W lewej części okna wybierz **Ostrzeżenie**.

5. W prawej części okna, w sekcji **Ustaw stan Ostrzeżenie, jeśli** włącz warunek, aby przełączyć urządzenie do stanu *Ostrzeżenie*.

   Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

6. Wybierz przycisk radiowy obok warunku na liście.
7. W lewym górnym rogu listy kliknij przycisk **Edytuj**.
8. Dla wybranego warunku ustaw żądaną wartość.

   Nie dla każdego warunku można ustawić wartości.

9. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Ostrzeżenie*.

Konfigurowanie dostarczania powiadomień

Możesz skonfigurować powiadomienie o zdarzeniach występujących w Kaspersky Security Center. W zależności od wybranej metody powiadamiania, dostępne są następujące typy powiadomień:

- E-mail—Po wystąpieniu zdarzenia, Kaspersky Security Center wyśle powiadomienie na określone adresy e-mail.
- SMS—Po wystąpieniu zdarzenia, Kaspersky Security Center wyśle powiadomienie na określone numery telefonu.
- Plik wykonywalny—Po wystąpieniu zdarzenia, plik wykonywalny jest uruchamiany na Serwerze administracyjnym.

W celu skonfigurowania dostarczania powiadomień o zdarzeniach występujących w Kaspersky Security Center:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.

2. Kliknij sekcję **Powiadomienie** i w prawej części okna wybierz zakładkę dla metody powiadamiania, którą chcesz:

   - **E-mail**

     Na zakładce **E-mail** można skonfigurować wysyłanie powiadomień o zdarzeniach za pośrednictwem poczty elektronicznej.

     W polu **Adresaci (adresy e-mail)** określ adresy e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami.

     W polu **Serwer SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

     - Adres IPv4 lub IPv6
     - Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
     - Nazwa DNS serwera SMTP

     W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

Jeśli włączysz opcję **Użyj przeszukiwania DNS MX**, możesz użyć kilku wpisów MX adresów IP dla tej samej nazwy DNS serwera SMTP. Ta sama nazwa DNS może posiadać kilka wpisów MX z różnymi wartościami priorytetu odbierania wiadomości e-mail. Serwer administracyjny spróbuje wysłać powiadomienia e-mail do serwera SMTP w kolejności rosnącej priorytetów wpisów MX.

Jeśli włączysz opcję **Użyj przeszukiwania DNS MX** i nie włączysz korzystania z ustawień TLS, zalecane jest użycie ustawień DNSSEC na urządzeniu serwerowym jako dodatkowego środka ochrony wysyłania powiadomień e-mail.

Jeśli włączysz opcję **Użyj uwierzytelniania ESMTP**, możesz określić ustawienia uwierzytelniania ESMTP w polach **Nazwa użytkownika** i **Hasło**. Domyślnie, opcja ta jest wyłączona, a ustawienia uwierzytelniania ESMTP są niedostępne.

Możesz określić ustawienia TLS połączenia z serwerem SMTP:

- **Nie używaj TLS**

Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.

- **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.

- **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**

Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

Możesz określić certyfikat dla połączenia TLS, klikając odnośnik **Określ certyfikaty**:

- Odszukaj plik certyfikatu serwera SMTP:

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

- Odszukaj plik certyfikatu klienta:

Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

- Certyfikat X-509:

Musisz określić plik z certyfikatem oraz plik z kluczem prywatnym. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po załadowaniu obu plików należy określić hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

- Kontener pkcs12:

Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

W polu **Temat** wprowadź temat wiadomości e-mail. Możesz zostawić to pole puste.

Z listy rozwijalnej **Wybierz szablon** wybierz szablon tematu. Zmienna określona przez wybrany szablon zostanie automatycznie umieszczona w polu **Temat**. Możesz utworzyć temat wiadomości, wybierając kilka szablonów tematu.

W oknie **Adres e-mail nadawcy** określ adres e-mail nadawcy. Jeśli pozostawisz to pole puste, domyślnie użyty zostanie adres odbiorcy. Nie jest zalecane użycie adresu e-mail, który nie istnieje.

Pole **Treść powiadomienia** zawiera standardowy tekst z informacjami dotyczącymi zdarzenia, który aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera dodatkowe parametry, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny. Istnieje możliwość zmodyfikowania treści wiadomości poprzez dodanie innych parametrów zastępczych z bardziej szczegółowymi danymi dotyczącymi zdarzenia.

> Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%".

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Przycisk **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie na wskazany adres e-mail.

- **SMS**

Na zakładce **SMS** możesz skonfigurować wysyłanie powiadomień SMS o różnych zdarzeniach na telefon komórkowy. Wiadomości SMS są wysyłane poprzez bramkę pocztową.

W polu **Serwer SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
- Nazwa DNS serwera SMTP

W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

Jeśli opcja **Użyj uwierzytelniania ESMTP** jest włączona, możesz określić ustawienia uwierzytelniania ESMTP w polach **Nazwa użytkownika** i **Hasło**. Domyślnie, opcja ta jest wyłączona, a ustawienia uwierzytelniania ESMTP są niedostępne.

Możesz określić ustawienia TLS połączenia z serwerem SMTP:

- **Nie używaj TLS**

Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.

- **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.

- **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**

Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

Możesz określić plik certyfikatu serwera SMTP, klikając odnośnik **Określ certyfikaty**:

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

W polu **Adresaci (adresy e-mail)** określ adresy e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami. Powiadomienia będą dostarczane na numery telefonów skojarzone z określonymi adresami e-mail.

W polu **Temat** wprowadź temat wiadomości e-mail.

Z listy rozwijalnej **Wybierz szablon** wybierz szablon tematu. Zgodnie z wybranym szablonem zmienna zostanie umieszczona w polu **Temat**. Możesz utworzyć temat wiadomości, wybierając kilka szablonów tematu.

W oknie **Adres e-mail nadawcy: Jeśli to ustawienie nie jest określone, użyty zostanie adres odbiorcy. Uwaga: Nie zalecamy używania adresu e-mail, który nie istnieje** określ adres e-mail nadawcy. Jeśli pozostawisz to pole puste, domyślnie użyty zostanie adres odbiorcy. Nie jest zalecane użycie adresu e-mail, który nie istnieje.

W polu **Numery telefonów odbiorców wiadomości SMS** określ numery telefonów komórkowych odbiorców powiadomień SMS.

W polu **Treść powiadomienia** określ tekst z informacjami dotyczącymi zdarzenia, który aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera parametry zastępcze, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny.

Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%".

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Kliknięcie **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie do określonego odbiorcy.

- **Plik wykonywalny do uruchomienia**

  Jeśli wybrana jest ta metoda powiadamiania, w polu wejściowym określ aplikację, która zostanie uruchomiona, gdy wystąpi zdarzenie.

  W polu **Plik wykonywalny, który będzie uruchamiany na Serwerze administracyjnym w momencie wystąpienia zdarzenia** określ folder i nazwę pliku, który ma zostać uruchomiony. Przed określeniem pliku przygotuj plik i określ symbole zastępcze, które definiują szczegóły zdarzeń, które mają zostać wysłane w treści powiadomienia. Folder i plik, który określasz, muszą znajdować się na Serwerze administracyjnym.

  Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

3. Na zakładce zdefiniuj ustawienia powiadamiania.

4. Kliknij przycisk **OK**, aby zamknąć okno właściwości Serwera administracyjnego.

Zapisane ustawienia dostarczania powiadomień zostaną zastosowane do wszystkich zdarzeń, które występują w Kaspersky Security Center.

Możesz zastąpić ustawienia dostarczania powiadomień dla pewnych zdarzeń w sekcji **Konfiguracja zdarzenia** ustawień Serwera administracyjnego, ustawień zasady lub ustawień aplikacji.

Wyświetlanie powiadomień o zdarzeniach po uruchomieniu pliku wykonywalnego

Kaspersky Security Center może powiadamiać administratora o zdarzeniach na urządzeniach klienckich poprzez uruchomienie pliku wykonywalnego. Plik wykonywalny musi zawierać inny plik wykonywalny z symbolami zastępczymi zdarzenia przekazywanymi administratorowi (patrz poniższa tabela).

Symbole zastępcze opisujące zdarzenie

Symbol zastępczy	Opis symbolu zastępczego
%SEVERITY%	Priorytet zdarzenia. Możliwe wartości: • **Informacja** • **Ostrzeżenie** • **Błąd** • **Krytyczny**
%COMPUTER%	Nazwa urządzenia, na którym wystąpiło zdarzenie. Maksymalna długość nazwy urządzenia wynosi 256 znaków.
%DOMAIN%	Nazwa domeny urządzenia, na którym wystąpiło zdarzenie.
%EVENT%	Nazwa typu zdarzenia. Maksymalna długość nazwy typu zdarzenia wynosi 50 znaków.
%DESCR%	Opis zdarzenia. Maksymalna długość opisu wynosi 1000 znaków.
%RISE_TIME%	Czas utworzenia zdarzenia.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nazwa zadania. Maksymalna długość nazwy zadania wynosi 100 znaków.
%KL_PRODUCT%	Nazwa aplikacji.
%KL_VERSION%	Numer wersji aplikacji.
%KLCSAK_EVENT_SEVERITY_NUM%	Numer priorytetu zdarzenia. Możliwe wartości: • 1—**Informacja** • 2—**Ostrzeżenie** • 3—**Błąd** • 4—**Krytyczny**
%HOST_IP%	Adres IP urządzenia, na którym wystąpiło zdarzenie.
%HOST_CONN_IP%	Adres IP połączenia urządzenia, na którym wystąpiło zdarzenie.

Na przykład:
Powiadomienia o zdarzeniach są wysyłane przez plik wykonywalny (na przykład script1.bat), w którym uruchomiony jest inny plik wykonywalny (na przykład script2.bat) z symbolem zastępczym %COMPUTER%. Po wystąpieniu zdarzenia, plik script1.bat jest uruchamiany na urządzeniu administratora, który uruchamia plik script2.bat z symbolem zastępczym %COMPUTER%. Administrator uzyska nazwę urządzenia, na którym wystąpiło zdarzenie.

Ogłoszenia firmy Kaspersky

W tej sekcji opisano, jak używać, konfigurować i wyłączać ogłoszenia Kaspersky.

Informacje o ogłoszeniach firmy Kaspersky

Sekcja Zapowiedzi firmy Kaspersky (**Monitorowanie i raportowanie → Zapowiedzi firmy Kaspersky**) zawiera informacje dotyczące Twojej wersji Kaspersky Security Center i zarządzanych aplikacji, zainstalowanych na zarządzanych urządzeniach. Kaspersky Security Center okresowo aktualizuje informacje w sekcji, usuwając nieaktualne ogłoszenia i dodając nowe informacje.

Kaspersky Security Center wyświetla tylko te ogłoszenia Kaspersky, które odnoszą się do aktualnie podłączonego Serwera administracyjnego i aplikacji Kaspersky zainstalowanych na zarządzanych urządzeniach tego Serwera administracyjnego. Ogłoszenia są wyświetlane indywidualnie dla dowolnego typu Serwera administracyjnego — głównego, podrzędnego lub wirtualnego.

Serwer administracyjny musi mieć połączenie z internetem, aby otrzymywać ogłoszenia Kaspersky.

Ogłoszenia zawierają informacje następujących typów:

- Ogłoszenia związane z bezpieczeństwem

  Ogłoszenia związane z bezpieczeństwem mają na celu zapewnienie aktualności i pełnej funkcjonalności aplikacji Kaspersky zainstalowanych w Twojej sieci. Ogłoszenia mogą zawierać informacje o krytycznych aktualizacjach aplikacji Kaspersky, poprawkach znalezionych luk w zabezpieczeniach i sposobach rozwiązania innych problemów w aplikacjach Kaspersky. Ogłoszenia związane z bezpieczeństwem są domyślnie włączone. Jeśli nie chcesz otrzymywać ogłoszeń, możesz wyłącz tę funkcję.

  Aby wyświetlić informacje odpowiadające konfiguracji ochrony sieci, Kaspersky Security Center wysyła dane do serwerów Kaspersky w chmurze i odbiera tylko te powiadomienia, które odnoszą się do aplikacji Kaspersky zainstalowanych w Twojej sieci. Zestaw danych, które można wysłać do serwerów, opisano w Umowie licencyjnej użytkownika końcowego, którą akceptujesz podczas instalacji Serwera administracyjnego Kaspersky Security Center.

- Ogłoszenia marketingowe

  Ogłoszenia marketingowe obejmują informacje o specjalnych ofertach dla aplikacji Kaspersky, reklamach i nowościach od Kaspersky. Ogłoszenia marketingowe są domyślnie wyłączone. Otrzymujesz tego typu powiadomienia tylko wtedy, gdy włączyłeś Kaspersky Security Network (KSN). Możesz wyłączyć ogłoszenia marketingowe, wyłączając KSN.

  Aby wyświetlać tylko istotne informacje, które mogą być pomocne w ochronie urządzeń sieciowych i wykonywaniu codziennych zadań, Kaspersky Security Center wysyła dane do serwerów Kaspersky w chmurze i odbiera odpowiednie ogłoszenia. Zestaw danych, które można wysłać do serwerów, opisano w sekcji Przetwarzane dane w Oświadczeniu KSN.

Nowe informacje są podzielone na następujące kategorie według ważności:

1. Krytyczne informacje
2. Ważne wiadomości

3. Ostrzeżenie

4. Informacja

Jeśli w sekcji Ogłoszenia firmy Kaspersky pojawią się nowe informacje, konsola Kaspersky Security Center Web Console wyświetli etykietę powiadomienia odpowiadającą istotności ogłoszeń. Możesz kliknąć etykietę, aby wyświetlić to ogłoszenie w sekcji Ogłoszenia firmy Kaspersky.

Możesz określić Ustawienia ogłoszeń firmy Kaspersky, w tym kategorie ogłoszeń, które chcesz przeglądać, i gdzie wyświetlać etykietę powiadomienia.

Określanie ustawień ogłoszeń Kaspersky

W sekcji Ogłoszenia firmy Kaspersky możesz określić ustawienia ogłoszeń firmy Kaspersky, w tym kategorie ogłoszeń, które chcesz przeglądać, i gdzie wyświetlać etykietę powiadomienia.

W celu skonfigurowania ogłoszeń Kaspersky:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Ogłoszenia Kaspersky**.

2. Kliknij odnośnik **Ustawienia**.

   Zostanie otwarte okno ustawień ogłoszeń Kaspersky.

3. Określ następujące ustawienia:

   - Wybierz poziom istotności ogłoszeń, które chcesz przejrzeć. Ogłoszenia z innych kategorii nie będą wyświetlane.

   - Wybierz, gdzie chcesz widzieć etykietę powiadomienia. Etykieta może być wyświetlana we wszystkich sekcjach konsoli lub w sekcji **Monitorowanie i raportowanie** i jego podsekcjach.

4. Kliknij przycisk **OK**.

   Zostaną określone ustawienia ogłoszeń firmy Kaspersky.

Wyłączanie ogłoszeń Kaspersky

Sekcja Ogłoszenia firmy Kaspersky (**Monitorowanie i raportowanie** → **Ogłoszenia firmy Kaspersky**) zawiera informacje dotyczące Twojej wersji Kaspersky Security Center i zarządzanych aplikacji, zainstalowanych na zarządzanych urządzeniach. Jeśli nie chcesz otrzymywać ogłoszeń firmy Kaspersky, możesz wyłączyć tę funkcję.

Ogłoszenia firmy Kaspersky obejmują dwa rodzaje informacji: ogłoszenia związane z bezpieczeństwem oraz ogłoszenia marketingowe. Możesz wyłączyć ogłoszenia każdego typu osobno.

W celu wyłączenia ogłoszeń związanych z bezpieczeństwem:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ogłoszenia Kaspersky**.

3. Przełącz przycisk przełączania na pozycję **Ogłoszenia związane z bezpieczeństwem Wyłączono**.

4. Kliknij przycisk **Zapisz**.

   Ogłoszenia firmy Kaspersky są wyłączone.

Ogłoszenia marketingowe są domyślnie wyłączone. Otrzymujesz ogłoszenia marketingowe tylko wtedy, gdy włączyłeś Kaspersky Security Network (KSN). Możesz wyłączyć tego typu ogłoszenia, wyłączając KSN.

W celu wyłączenia ogłoszeń marketingowych:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.

3. Wyłącz opcję **Użyj Kaspersky Security Network Włączono**.

4. Kliknij przycisk **Zapisz**.

   Ogłoszenia marketingowe są wyłączone.

Przeglądanie informacji dotyczących wykrycia zagrożeń

Możesz włączyć lub wyłączyć wyświetlanie informacji o alertach.

*W celu włączenia lub wyłączenia sekcji **Alerty** w menu głównym:*

1. W menu głównym przejdź do ustawień konta i wybierz **Opcje interfejsu**.

2. W otwartym oknie **Opcje interfejsu** włącz lub wyłącz opcję **Pokaż alerty EDR**.

3. Kliknij **Zapisz**.

Konsola wyświetla podsekcję **Alerty** w sekcji **Monitorowanie i raportowanie** menu głównego. W podsekcji **Alerty** możesz przejrzeć informacje dotyczące wykrycia zagrożeń na urządzeniach końcowych. Jeśli dodasz klucz licencyjny dla EDR Optimum, wówczas Kaspersky Security Center Web Console automatycznie wyświetli podsekcję **Alerty** w sekcji **Monitorowanie i raportowanie** menu głównego. Dodatkowo, możesz dodać widżet, który wyświetla informacje o alertach.

> Podsekcja **Alerty** wyświetla się automatycznie tylko wtedy, gdy przed włączeniem opcji **Pokaż alerty EDR** dodano klucz licencyjny dla EDR Optimum. Jeśli klucz licencyjny dodano po włączeniu opcji **Pokaż alerty EDR**, podsekcja **Alerty** zostanie wyświetlona dopiero po ponownym włączeniu tej opcji.

Aby poprawnie wyświetlać szczegółowe informacje o wykrytych zagrożeniach na karcie alertu, należy zainstalować wtyczkę Kaspersky Endpoint Agent oraz zgodną wersja wtyczki Kaspersky Endpoint Security (Kaspersky Endpoint Security for Linux w wersji 12.1 lub nowszej, Kaspersky Endpoint Security for Mac w wersji 12.1 lub nowszej albo Kaspersky Endpoint Security for Windows w wersji 12.6 lub nowszej).

Użyj menu **Filtr**, aby filtrować alerty według daty i wartości pól.

Pole **Typ obiektu** zawiera następujące wartości:

- Nieznany
- Odnośnik phishingowy
- Wirus
- Trojan
- Szkodliwe narzędzie
- Backdoor
- Robak
- Inna aplikacja
- Adware
- Pornware
- Niebezpieczny spakowany program
- Niebezpieczne zachowanie

Pole **Odpowiedź automatyczna** zawiera następujące wartości:

- Wykryto szkodliwy obiekt
- Obiekt usunięty
- Obiekt wyleczony
- Wyleczenie obiektu nie powiodło się
- Obiekt przeniesiono do Kwarantanny
- Wykryto archiwum zabezpieczone hasłem
- Wykryto wirusa

Cloud Discovery

Kaspersky Security Center umożliwia monitorowanie korzystania z usług w chmurze na zarządzanych urządzeniach z systemem Windows i blokowanie dostępu do usług w chmurze, które użytkownik uważa za niepożądane. Program Cloud Discovery śledzi próby uzyskania dostępu do tych usług przez użytkowników zarówno za pośrednictwem przeglądarek, jak i aplikacji komputerowych. Śledzi także próby uzyskania przez użytkownika dostępu do usług w chmurze za pośrednictwem połączeń nieszyfrowanych (na przykład przy użyciu protokołu HTTP). Ta funkcja pomaga wykryć i zatrzymać korzystanie z usług w chmurze przez Shadow IT.

Możliwość blokowania jest dostępna tylko wtedy, gdy aktywowano Kaspersky Security Center w ramach licencji Kaspersky Next EDR Optimum lub Kaspersky Next XDR Expert.

Możliwość blokowania jest dostępna tylko w przypadku korzystania z Kaspersky Endpoint Security 11.2 for Windows lub nowszego. Wcześniejsze wersje aplikacji zabezpieczającej umożliwiają tylko monitorowanie korzystania z usług w chmurze.

Możesz włączyć funkcję Cloud Discovery i wybrać zasady lub profile bezpieczeństwa, dla których chcesz włączyć tę funkcję. Możesz także włączyć lub wyłączyć tę funkcję oddzielnie w każdej zasadzie lub profilu bezpieczeństwa. Możesz zablokować dostęp do usług w chmurze, do których nie chcesz, aby użytkownicy mieli dostęp.

Aby móc zablokować dostęp do niechcianych usług w chmurze, upewnij się, że zostały spełnione następujące warunki:

- Używasz Kaspersky Endpoint Security 11.2 for Windows lub nowszego. Wcześniejsze wersje aplikacji zabezpieczającej umożliwiają tylko monitorowanie korzystania z usług w chmurze.
- Posiadasz warstwę licencji Kaspersky Next, która zapewnia możliwość blokowania dostępu do niechcianych usług w chmurze. Aby uzyskać szczegółowe informacje, zobacz Pomoc Kaspersky Next.

Widżet Cloud Discovery i raporty Cloud Discovery wyświetlają informacje o udanych i zablokowanych próbach uzyskania dostępu do usług w chmurze. Widżet wyświetla także poziom ryzyka każdej usługi w chmurze. Kaspersky Security Center pobiera informacje o korzystaniu z usług w chmurze ze wszystkich zarządzanych urządzeń, które są chronione wyłącznie przez zasady i profile bezpieczeństwa, które mają włączoną tę funkcję.

Włączanie funkcji Cloud Discovery za pomocą widżetu

Funkcja Cloud Discovery pozwala uzyskać informacje o korzystaniu z usług w chmurze ze wszystkich zarządzanych urządzeń chronionych wyłącznie przez zasady bezpieczeństwa, które mają włączoną tę funkcję. Możesz włączyć lub wyłączyć Cloud Discovery tylko dla zasady Kaspersky Endpoint Security for Windows.

Istnieją dwa sposoby włączenia funkcji Cloud Discovery:

- Za pomocą widżetu Cloud Discovery.
- We właściwościach zasady Kaspersky Endpoint Security for Windows.

  Szczegółowe informacje na temat włączania funkcji Cloud Discovery we właściwościach zasady Kaspersky Endpoint Security for Windows można znaleźć w sekcji Cloud Discovery pomocy Kaspersky Endpoint Security for Windows.

Pamiętaj, że funkcję Cloud Discovery możesz wyłączyć wyłącznie w parametrach zasady Kaspersky Endpoint Security for Windows.

Aby włączyć Cloud Discovery, musisz mieć uprawnienia do **Zapis** w obszarze funkcjonalnym **Funkcje ogólne: funkcjonalność podstawowa**.

Aby włączyć funkcję Cloud Discovery za pomocą widżetu Cloud Discovery:

1. Przejdź do Kaspersky Security Center.
2. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.
3. W widżecie **Cloud Discovery** kliknij przycisk **Włącz**.

   Jeśli masz zainstalowany program Kaspersky Endpoint Security for Windows w wersji 12.4, włącz funkcję Cloud Discovery we właściwościach zasady Kaspersky Endpoint Security for Windows. Aby uzyskać szczegółowe informacje, zobacz Cloud Discovery w sekcji pomocy Kaspersky Endpoint Security for Windows.

   Jeżeli posiadasz Kaspersky Endpoint Security for Windows w wersji starszej niż 12.4, zaktualizuj wtyczkę Kaspersky Endpoint Security for Windows do wersji 12.5.

4. W otwartym oknie **Włącz Cloud Discovery** wybierz zasady zabezpieczeń, dla których chcesz włączyć tę funkcję, a następnie kliknij przycisk **Włącz**.

   Następujące ustawienia zasad zostaną włączone automatycznie: **Wprowadź skrypt do ruchu internetowego w celu interakcji ze stronami internetowymi**, **Monitor sesji internetowej** i **Skanowanie połączeń szyfrowanych**.

Funkcja Cloud Discovery jest włączona, a widżet zostaje dodany do pulpitu nawigacyjnego.

Dodanie widżetu Cloud Discovery do pulpitu nawigacyjnego

Do panelu kontrolnego możesz dodać widżet **Cloud Discovery**, aby monitorować wykorzystanie usług w chmurze na zarządzanych urządzeniach.

Aby dodać widżet Cloud Discovery do pulpitu nawigacyjnego, musisz mieć uprawnienie do **Zapis** w obszarze funkcjonalnym **Funkcje ogólne: funkcjonalność podstawowa**.

Aby dodać widżet Cloud Discovery do pulpitu nawigacyjnego:

1. Przejdź do Kaspersky Security Center.
2. W menu głównym przejdź do **Monitorowanie i raportowanie → Pulpit nawigacyjny**.
3. Kliknij przycisk **Dodaj lub przywróć widżet sieciowy**.
4. Na liście dostępnych widżetów kliknij ikonę jodełki (›) obok kategorii **Inny**.
5. Wybierz widżet **Cloud Discovery**, a następnie kliknij przycisk **Dodaj**.

   Jeśli funkcja Cloud Discovery jest wyłączona, postępuj zgodnie z instrukcjami w sekcji Włączanie Cloud Discovery przy użyciu widżetu.

Wybrany widżet zostanie dodany na końcu pulpitu nawigacyjnego.

Przeglądanie informacji o korzystaniu z usług w chmurze

Możesz wyświetlić widżet **Cloud Discovery**, który wyświetla informacje o próbach uzyskania dostępu do usług w chmurze. Widżet wyświetla także poziom ryzyka każdej usługi w chmurze. Kaspersky Security Center pobiera informacje o korzystaniu z usług w chmurze ze wszystkich zarządzanych urządzeń, które są chronione wyłącznie przez profile bezpieczeństwa, które mają włączoną tę funkcję.

Przed obejrzeniem upewnij się, że:

- Do pulpitu nawigacyjnego dodano widżet Cloud Discovery.
- Funkcja Cloud Discovery jest włączona.
- Masz uprawnienia do **Odczyt** w obszarze funkcjonalnym **Funkcje ogólne: podstawowa funkcjonalność**.

Aby wyświetlić widżet Cloud Discovery:

1. Przejdź do Kaspersky Security Center.
2. W menu głównym przejdź do **Monitorowanie i raportowanie → Pulpit nawigacyjny**.

   Widżet **Cloud Discovery** zostanie wyświetlony na pulpicie nawigacyjnym.
3. Po lewej stronie widżetu **Cloud Discovery** wybierz kategorię usług w chmurze.

   W tabeli po prawej stronie widżetu wyświetlanych jest maksymalnie pięć usług z wybranej kategorii, do których użytkownicy najczęściej starają się uzyskać dostęp. Liczone są zarówno próby udane, jak i zablokowane.
4. Po prawej stronie widżetu wybierz konkretną usługę.

   Poniższa tabela przedstawia aż dziesięć urządzeń, które najczęściej podejmują próbę uzyskania dostępu do usługi. W tej tabeli można wygenerować dwa rodzaje raportów: raport dotyczący udanych prób dostępu i raport dotyczący zablokowanych prób dostępu.

   Dodatkowo w tej tabeli możesz zablokować dostęp do usługi w chmurze dla określonego urządzenia.

Widżet wyświetla żądane informacje.

W wyświetlonym widżecie możesz wykonać następujące czynności:

- Przejdź do sekcji **Monitorowanie i raportowanie** → **Raporty**, aby wyświetlić raporty Cloud Discovery.
- Zablokuj lub zezwól na dostęp do wybranej usługi w chmurze.

Możliwość blokowania jest dostępna tylko wtedy, gdy aktywowano Kaspersky Security Center w ramach licencji Kaspersky Next EDR Optimum lub Kaspersky Next XDR Expert.

Możliwość blokowania jest dostępna tylko w przypadku korzystania z Kaspersky Endpoint Security 11.2 for Windows lub nowszego. Wcześniejsze wersje aplikacji zabezpieczającej umożliwiają tylko monitorowanie korzystania z usług w chmurze.

Poziom ryzyka usługi w chmurze

Dla każdej usługi w chmurze Cloud Discovery zapewnia informację o poziomie ryzyka. Poziom ryzyka pomaga określić, które usługi nie spełniają wymagań bezpieczeństwa Twojej organizacji. Na przykład możesz chcieć wziąć pod uwagę poziom ryzyka przy podejmowaniu decyzji o zablokowaniu dostępu do określonej usługi.

Poziom ryzyka jest wskaźnikiem szacunkowym i nie mówi nic o jakości usługi w chmurze ani o jej producencie. Poziom ryzyka to po prostu zalecenie ekspertów z Kaspersky.

Poziomy ryzyka usług w chmurze wyświetlane są w widżecie Cloud Discovery oraz na liście wszystkich monitorowanych usług w chmurze.

Blokowanie dostępu do niechcianych usług w chmurze

Możesz zablokować dostęp do usług w chmurze, do których nie chcesz, aby użytkownicy mieli dostęp. Możesz także zezwolić na dostęp do usług w chmurze, które zostały wcześniej zablokowane.

Decydując o zablokowaniu dostępu do określonej usługi, możesz między innymi wziąć pod uwagę poziom ryzyka.

Możesz zablokować lub zezwolić na dostęp do usług w chmurze w ramach zasady lub profilu bezpieczeństwa.

Istnieją dwa sposoby blokowania dostępu do niechcianych usług w chmurze:

- Za pomocą widżetu Cloud Discovery.

  W takim wypadku możesz po kolei blokować dostęp do poszczególnych usług.

- We właściwościach zasady Kaspersky Endpoint Security for Windows.

  W takim przypadku możesz blokować dostęp do usług pojedynczo lub od razu blokować całą kategorię.

  Szczegółowe informacje na temat włączania funkcji Cloud Discovery we właściwościach zasady Kaspersky Endpoint Security for Windows można znaleźć w sekcji Cloud Discovery pomocy Kaspersky Endpoint Security for Windows.

Aby zablokować lub zezwolić na dostęp do usługi w chmurze za pomocą widżetu:

1. Otwórz widżet Cloud Discovery, a następnie wybierz wymaganą usługę w chmurze.
2. Na **10 najpopularniejszych urządzeń korzystających z usługi** znajdź zasadę lub profil bezpieczeństwa, dla którego chcesz zablokować usługę lub zezwolić na nią.
3. W wymaganym wierszu, w kolumnie **Status dostępu w zasadach lub profilu** wykonaj dowolną z następujących czynności:
   - Aby zablokować usługę, wybierz **Zablokowano** z listy rozwijanej.
   - Aby zezwolić na usługę, wybierz z listy rozwijanej opcję **Dozwolony**.
4. Kliknij przycisk **Zapisz**.

Dostęp do wybranej usługi jest zablokowany lub dozwolony przez zasadę lub profil bezpieczeństwa.

Rejestrowanie aktywności Kaspersky Security Center Web Console

Rejestrowanie aktywności Kaspersky Security Center Web Console może pomóc w zbadaniu przyczyny problemów z działaniem oprogramowania. Jeśli kontaktujesz się z działem pomocy technicznej Kaspersky w sprawie problemów z działaniem Kaspersky Security Center Web Console, specjaliści z działu pomocy technicznej Kaspersky mogą poprosić o pliki dziennika Kaspersky Security Center Web Console. Pliki dziennika Kaspersky Security Center Web Console są przechowywane w folderze <Folder instalacyjny Kaspersky Security Center Web Console>/logs przez cały czas korzystania z aplikacji. Pliki raportów nie są automatycznie wysyłane do specjalistów z pomocy technicznej Kaspersky.

W celu włączenia rejestrowania aktywności Kaspersky Security Center Web Console:

Zaznacz pole **Włącz rejestrowanie działań Kaspersky Security Center Web Console** w oknie **Ustawienia połączenia Kaspersky Security Center Web Console** kreatora instalacji Kaspersky Security Center Web Console.

Pliki raportów są w formacie tekstowym.

Nazwy plików raportów są w formacie logs-<nazwa komponentu>.<nazwa urządzenia>-<numer rewizji pliku>.RRRR-MM-DD, gdzie:

- <nazwa składnika> to nazwa składnika Kaspersky Security Center lub nazwa wtyczki administracyjnej Kaspersky Security Center Web Console.
- <nazwa urządzenia> to nazwa urządzenia, na którym jest uruchomiony <nazwa komponentu>.

- <numer rewizji pliku> to numer pliku raportu, utworzonego dla komponentu <nazwa_komponentu>, który działa na hoście <nazwa urządzenia>. W ciągu dnia może zostać utworzonych kilka plików raportów dla tego samego komponentu <nazwa komponentu> i urządzenia <nazwa urządzenia>. Maksymalny rozmiar pliku raportu wynosi 50 megabajtów (MB). Jeśli zostanie osiągnięty maksymalny rozmiar pliku, zostanie utworzony nowy plik raportu. Nowy plik raportu <numer rewizji pliku> zostanie zwiększony o 1.

- RRRR, MM i DD to rok, miesiąc i dzień pierwszego utworzenia raportu. Gdy zacznie się nowy dzień, zostanie utworzony nowy plik raportu.

Integracja Kaspersky Security Center z innymi rozwiązaniami

W tej sekcji opisano, jak skonfigurować dostęp z Kaspersky Security Center Web Console do innej aplikacji Kaspersky, takiej jak Kaspersky Managed Detection and Response. W tej sekcji opisano również, jak skonfigurować eksport do systemów SIEM.

Nawiązywanie połączenia w tle

Aby umożliwić Kaspersky Security Center Web Console wykonywanie zadań w tle, musisz ustanowić połączenie w tle pomiędzy Kaspersky Security Center Web Console i Serwerem administracyjnym. Możesz nawiązać to połączenie tylko wtedy, jeśli Twoje konto ma uprawnienie **Modyfikuj listy ACL** obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika.**

Jeśli zainstalujesz wtyczkę Kaspersky Endpoint Security for Windows 12.6 lub zaktualizujesz wtyczkę Kaspersky Endpoint Security for Windows z wersji wcześniejszej niż 11.7, a połączenie w tle nie zostanie jeszcze nawiązane, zostanie wyświetlone powiadomienie, że musisz nawiązać połączenie w tle. Ponadto będziesz musiał nadać kontu usługi uprawnienia obszaru funkcjonalnego **Funkcje ogólne: Operacje na Serwerze administracyjnym**.

Aby nawiązać połączenie w tle:

1. W menu głównym przejdź do sekcji **Ustawienia** → **Integracja**.

2. W sekcji **Integracja** ustaw przycisk przełączania do nawiązywania połączenia w tle w pozycji: **Połączenie w tle w celu integracji Włączone**.

3. W otwartej sekcji **Włącz połączenie w tle** kliknij przycisk **OK**.

Połączenie w tle pomiędzy konsolą Kaspersky Security Center Web Console i Serwerem administracyjnym jest nawiązywane. Serwer administracyjny tworzy konto dla połączenia w tle, które jest używane jako konto usługi do utrzymywania interakcji między Kaspersky Security Center a inną aplikacją lub rozwiązaniem Kaspersky. Nazwa tego konta usługi zawiera przedrostek NWCSvcUser.

Serwer administracyjny automatycznie zmienia hasło do konta usługi co 30 dni ze względów bezpieczeństwa. Nie możesz usunąć konta usługi ręcznie. Serwer administracyjny automatycznie usuwa to konto po wyłączeniu połączenia między usługami. Serwer administracyjny tworzy jedno konto usługi dla każdej Konsoli administracyjnej i przypisuje wszystkie konta usług do grupy bezpieczeństwa o nazwie ServiceNwcGroup. Serwer administracyjny tworzy grupę zabezpieczeń automatycznie podczas procesu instalacji Kaspersky Security Center. Nie możesz usunąć tej grupy zabezpieczeń ręcznie.

Eksportowanie zdarzeń do systemów SIEM

Ta sekcja opisuje sposób skonfigurowania eksportowania zdarzeń do systemów SIEM.

Konfigurowanie eksportowania zdarzeń do systemów SIEM

Kaspersky Security Center umożliwia konfigurowanie przy użyciu jednej z następujących metod: eksportowanie do dowolnego systemu SIEM korzystającego z formatu Syslog, eksportowanie do systemów QRadar, Splunk, ArcSight SIEM korzystających z formatów LEEF i CEF lub eksportowanie zdarzeń do systemów SIEM bezpośrednio z bazy danych Kaspersky Security Center. Po zakończeniu tego scenariusza Serwer administracyjny automatycznie wysyła zdarzenia do systemu SIEM.

Wymagania wstępne

Zanim rozpoczniesz konfigurowanie eksportowania zdarzeń w Kaspersky Security Center:

- Dowiedz się więcej o metodach eksportowania zdarzeń.
- Upewnij się, że posiadasz wartości ustawień systemowych.

> Możesz wykonać kroki tego scenariusza w dowolnej kolejności.

Proces eksportowania zdarzeń do systemu SIEM obejmuje następujące kroki:

- **Konfigurowanie systemu SIEM do odbierania zdarzeń z Kaspersky Security Center**

  Instrukcja: Konfigurowanie eksportowania zdarzeń w systemie SIEM

- **Wybieranie zdarzeń, które chcesz wyeksportować do systemu SIEM:**

  Dostępne instrukcje:

  - Konsola administracyjna: Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog, Oznaczanie ogólnych zdarzeń do eksportowania w formacie Syslog
  - Kaspersky Security Center Web Console: Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog, Oznaczanie ogólnych zdarzeń do eksportowania w formacie Syslog

- **Konfigurowanie eksportowania zdarzeń do systemu SIEM za pomocą jednej z poniższych metod:**

  - Korzystanie z protokołów TCP, UDP lub TLS przez protokoły TCP.

Dostępne instrukcje:

- Konsola administracyjna: Konfigurowanie eksportowania zdarzeń do systemów SIEM
- Kaspersky Security Center Web Console: Konfigurowanie eksportowania zdarzeń do systemów SIEM

- Używanie eksportowania zdarzeń bezpośrednio z bazy danych Kaspersky Security Center (zestaw widoków publicznych jest dostępny w bazie danych Kaspersky Security Center; opis tych widoków publicznych można znaleźć w dokumencie klakdb.chm).

Wyniki

Po skonfigurowaniu eksportowania zdarzeń do systemu SIEM możesz przeglądać eksportowanie wyników, jeśli wybrałeś zdarzenia, które chcesz wyeksportować.

Czynności niezbędne do wykonania przed rozpoczęciem pracy

Podczas konfigurowania automatycznego eksportowania zdarzeń w Kaspersky Security Center musisz określić niektóre ustawienia systemu SIEM. Zalecane jest wcześniejsze sprawdzenie tych ustawień w celu przygotowania do konfiguracji Kaspersky Security Center.

W celu pomyślnego skonfigurowania automatycznego wysyłania zdarzeń do systemu SIEM należy znać następujące ustawienia:

- **Adres serwera systemu SIEM**

  Adres IP serwera, na którym zainstalowany jest aktualnie używany system SIEM. Sprawdź wartość tego ustawienia w ustawieniach systemu SIEM.

- **Port serwera systemu SIEM**

  Numer portu używanego do nawiązania połączenia pomiędzy Kaspersky Security Center a serwerem Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center i w ustawieniach odbiornika Twojego systemu SIEM.

- **Protokół**

  Protokół używany do przesyłania wiadomości z Kaspersky Security Center do Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center i w ustawieniach odbiornika Twojego systemu SIEM.

Informacje o zdarzeniach w Kaspersky Security Center

Kaspersky Security Center umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Informacje o zdarzeniach są zapisywane w bazie danych Serwera administracyjnego. Możesz wyeksportować te informacje do zewnętrznych systemów SIEM. Eksportowanie informacji o zdarzeniach do zewnętrznych systemów SIEM umożliwia administratorom systemów SIEM natychmiastowe reagowanie na zdarzenia dotyczące systemu bezpieczeństwa, które pojawiają się na zarządzanych urządzeniach lub w grupach administracyjnych.

Typy zdarzeń

W Kaspersky Security Center dostępne są następujące typy zdarzeń:

- Zdarzenia ogólne. Te zdarzenia występują we wszystkich zarządzanych aplikacjach firmy Kaspersky. Przykładem zdarzenia ogólnego jest Epidemia wirusa. Zdarzenia ogólne mają dokładnie zdefiniowaną składnię i semantykę. Zdarzenia ogólne są używane, na przykład, w raportach i pulpitach nawigacyjnych.
- Zarządzane zdarzenia charakterystyczne dla aplikacji firmy Kaspersky. Każda zarządzana aplikacja firmy Kaspersky posiada swój zestaw zdarzeń.

Źródła zdarzeń

Zdarzenia mogą być generowane przez następujące aplikacje:

- Składniki Kaspersky Security Center:
  - Serwer administracyjny
  - Agent sieciowy
  - Serwer iOS MDM
- Zarządzane aplikacje Kaspersky

  Szczegółowe informacje na temat zdarzeń generowanych przez aplikacje zarządzane przez Kaspersky można znaleźć w dokumentacji odpowiedniej aplikacji.

Możesz wyświetlić pełną listę zdarzeń, które mogą być generowane przez aplikację na karcie **Konfiguracja zdarzenia** w zasadzie aplikacji. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić listę zdarzeń we właściwościach Serwera administracyjnego.

Poziom ważności zdarzeń

Każde zdarzenie posiada określony poziom istotności. W zależności od warunków wystąpienia zdarzenia, może ono posiadać różne poziomy istotności. Istnieją cztery poziomy istotności zdarzeń:

- *Zdarzenie krytyczne* to zdarzenie, które wskazuje wystąpienie krytycznego problemu mogącego prowadzić do utraty danych, problemów z działaniem lub błędu krytycznego.
- *Błąd funkcjonalny* to zdarzenie, które wskazuje poważny problem, błąd lub problem z działaniem, który wystąpił podczas działania aplikacji lub podczas przeprowadzania procedury.
- *Ostrzeżenie* to zdarzenie, które niekoniecznie jest poważne, ale wskazuje możliwość wystąpienia potencjalnego problemu w przyszłości. Większość zdarzeń otrzymuje priorytet „Ostrzeżenie", jeśli aplikacja może zostać przywrócona bez utraty danych lub możliwości funkcyjnych aplikacji.
- *Informacja* to zdarzenie, którego celem jest informowanie o pomyślnym zakończeniu działania, właściwym funkcjonowaniu aplikacji lub zakończeniu procedury.

Każde zdarzenie posiada zdefiniowany okres przechowywania, w trakcie którego możesz przejrzeć lub zmodyfikować to zdarzenie w Kaspersky Security Center. Niektóre zdarzenia nie są domyślnie zapisywane w bazie danych Serwera administracyjnego, ponieważ ich zdefiniowany okres przechowywania wynosi zero. Tylko te zdarzenia, które będą przechowywane w bazie danych Serwera administracyjnego przynajmniej jeden dzień, mogą zostać wyeksportowane do systemów zewnętrznych.

Informacje o eksportowaniu zdarzeń

Eksportowanie zdarzeń może być używane w obrębie scentralizowanych systemów, które zajmują się problemami z bezpieczeństwem na poziomie organizacyjnym i technicznym, zapewniają usługi monitorowania ochrony oraz skonsolidowane informacje z różnych rozwiązań. To są systemy SIEM, które oferują przeprowadzania w czasie rzeczywistym analizy alertów o zagrożeniach i zdarzeń zabezpieczeń, wygenerowanych przez aplikacje i sprzęt w sieci, lub Security Operation Centers (SOCs).

Te systemy otrzymują dane z wielu źródeł, w tym sieci, ochrony, serwerów, baz danych i aplikacji. Systemy SIEM oferują także funkcjonalność konsolidowania monitorowanych danych, aby pomóc w uniknięciu przeoczenia zdarzeń krytycznych. Dodatkowo, systemy przeprowadzają zautomatyzowaną analizę powiązanych zdarzeń i alertów w celu powiadomienia administratorów o nagłych problemach z bezpieczeństwem. Wysyłanie alertów może zostać zaimplementowane poprzez pulpit nawigacyjny lub wysyłanie ostrzeżeń może się odbywać poprzez kanały firm trzecich, na przykład pocztę elektroniczną.

Proces eksportowania zdarzeń z Kaspersky Security Center do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia—Kaspersky Security Center oraz odbiorca zdarzenia—system SIEM. Aby pomyślnie eksportować zdarzenia, należy skonfigurować tę funkcję w posiadanym systemie SIEM i w Konsoli administracyjnej Kaspersky Security Center. Nie ma znaczenia, która strona zostanie skonfigurowana jako pierwsza. Możesz skonfigurować przesyłanie zdarzeń w Kaspersky Security Center, a następnie skonfigurować odbieranie zdarzeń przez system SIEM lub na odwrót.

Metody wysyłania zdarzeń z Kaspersky Security Center

Dostępne są trzy metody wysyłania zdarzeń z Kaspersky Security Center do systemów zewnętrznych:

- Wysyłanie zdarzeń po protokole Syslog do dowolnego systemu SIEM

  Korzystając z protokołu Syslog, możesz przekazywać dowolne zdarzenia, które wystąpiły na Serwerze administracyjnym Kaspersky Security Center i w aplikacjach firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Możesz go użyć do eksportowania zdarzeń do systemu SIEM.

  W tym celu należy zaznaczyć zdarzenia, które chcemy przekazać do systemu SIEM. Możesz zaznaczyć zdarzenia w Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console. Tylko zaznaczone zdarzenia będą przekazywane do systemu SIEM. Jeśli nic nie zaznaczysz, żadne zdarzenia nie zostaną przekazane.

- Wysyłanie zdarzeń po protokołach CEF i LEEF do systemów QRadar, Splunk i ArcSight

  Możesz używać protokołów CEF i LEEF do eksportowania zdarzeń ogólnych. Podczas eksportowania zdarzeń po protokołach CEF i LEEF nie masz możliwości wyboru określonych zdarzeń do wyeksportowania. Eksportowane są wszystkie zdarzenia ogólne. Aby skonwertować zdarzenia Kaspersky Security Center na zdarzenia w formacie CEF i LEEF, możesz użyć pliku siem_conversion_rules.xml. Ten plik zawiera listę atrybutów zdarzeń Kaspersky Security Center i odpowiadających im atrybutów zdarzeń w formacie CEF i LEEF. Ponadto plik siem_conversion_rules.xml zawiera reguły generowania komunikatów odpowiadających zdarzeniom. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center.

W przeciwieństwie do protokołu Syslog, protokoły CEF i LEEF nie są uniwersalne. Protokoły CEF i LEEF są przeznaczone dla odpowiednich systemów SIEM (QRadar, Splunk i ArcSight). Dlatego też, jeśli wybierzesz eksportowanie zdarzeń poprzez jeden z tych protokołów, użyjesz parsera w systemie SIEM.

- Bezpośrednio z bazy danych Kaspersky Security Center do dowolnego systemu SIEM

  Ta metoda eksportowania zdarzeń może zostać użyta do odbierania zdarzeń bezpośrednio z widoków publicznych bazy danych przy użyciu zapytań SQL. Wyniki zapytań są zapisywane do pliku XML, który może zostać użyty jako dane wejściowe systemu zewnętrznego. Tylko zdarzenia dostępne w widokach publicznych mogą być eksportowane bezpośrednio z bazy danych.

Odbieranie zdarzeń przez system SIEM

System SIEM musi odbierać i poprawnie analizować zdarzenia otrzymywane z Kaspersky Security Center. W tym celu należy odpowiednio skonfigurować system SIEM. Konfiguracja zależy od specyfiki używanego systemu SIEM. Jednakże istnieje kilka ogólnych kroków w konfiguracji wszystkich systemów SIEM, takie jak konfigurowanie odbiorcy i analizatora.

Informacje o konfigurowaniu eksportowania zdarzeń w systemie SIEM

Proces eksportowania zdarzeń z Kaspersky Security Center do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia—Kaspersky Security Center oraz odbiorca zdarzenia—system SIEM. Należy skonfigurować eksportowanie zdarzeń w posiadanym systemie SIEM i w Kaspersky Security Center.

Ustawienia określane w systemie SIEM zależą od określonego systemu, którego używasz. Zazwyczaj dla wszystkich systemów SIEM należy skonfigurować odbiorcę i, opcjonalnie, analizatora wiadomości do analizowania otrzymanych zdarzeń.

Konfigurowanie odbiorcy

Aby otrzymywać zdarzenia wysyłane przez Kaspersky Security Center, należy skonfigurować odbiorcę w swoim systemie SIEM. W systemie SIEM powinny zostać określone następujące ustawienia:

- **Protokół eksportu lub typ wejścia**

  Jest to protokół przesyłania wiadomości, na przykład UDP. Ten protokół musi być taki sam, jak protokół, który określiłeś w Kaspersky Security Center.

- **Port**

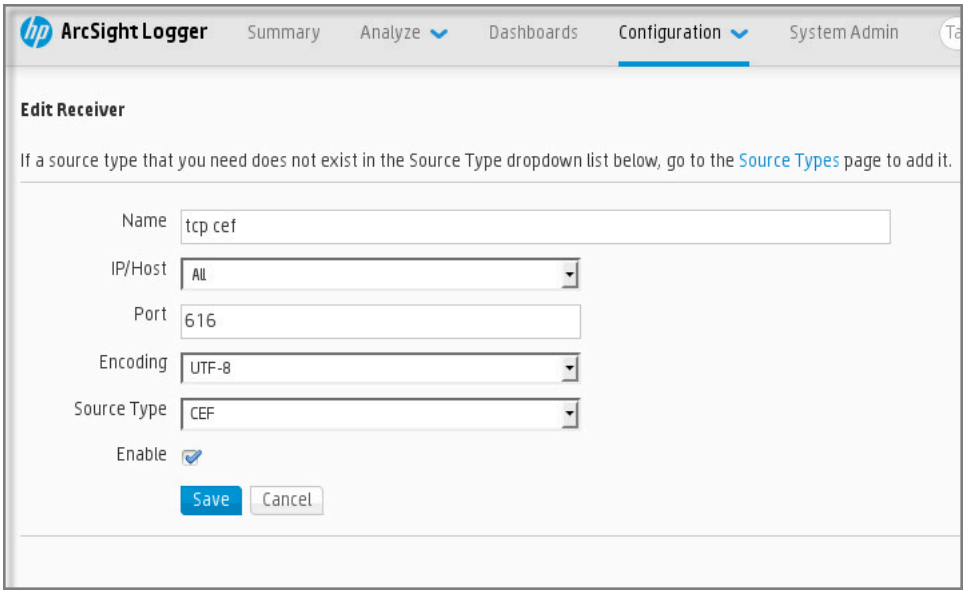
  Numer portu do nawiązana połączenia z Kaspersky Security Center. Ten port musi być taki sam, jak port, który określiłeś w Kaspersky Security Center.

- **Protokół wiadomości lub typ źródła**

  Protokół używany do eksportowania zdarzeń do systemu SIEM. Może to być jeden ze standardowych protokołów: Syslog, CEF lub LEEF. System SIEM wybiera analizatora wiadomości zgodnie z protokołem, który określiłeś.

W zależności od używanego systemu SIEM, konieczne może być określenie niektórych dodatkowych ustawień odbiorcy.

Poniższy rysunek przedstawia okno konfiguracji odbiorcy w ArcSight.



Konfiguracja odbiorcy w ArcSight

Analizator wiadomości

Wyeksportowane zdarzenia są przekazywane do systemu SIEM jako wiadomości. Te wiadomości muszą być odpowiednio przeanalizowane, aby informacje na temat zdarzeń mogły być użyte przez system SIEM. Analizatory wiadomości są częścią systemu SIEM; są używane do podzielenia zawartości wiadomości na odpowiednie pola, takie jak: identyfikator zdarzenia, priorytet, opis, parametry itd. Umożliwia to systemowi SIEM przetworzenie zdarzeń otrzymanych z Kaspersky Security Center tak, aby mogły być przechowywane w bazie danych systemu SIEM.

Oznaczenie zdarzeń do wyeksportowania do systemów SIEM w formacie Syslog

Po włączeniu automatycznego eksportowania zdarzeń, należy wskazać zdarzenia, które zostaną wyeksportowane do zewnętrznego systemu SIEM.

Możesz skonfigurować eksportowanie zdarzeń w formacie Syslog do zewnętrznego systemu w oparciu o jeden z następujących warunków:

- Oznaczanie zdarzeń ogólnych. Jeśli zdarzenia do wyeksportowania oznaczysz w zasadzie, w ustawieniach zdarzenia lub w ustawieniach Serwera administracyjnego system SIEM otrzyma oznaczone zdarzenia, które wystąpiły we wszystkich aplikacjach zarządzanych przez określoną zasadę. Jeśli wyeksportowane zdarzenia były wybrane w zasadzie, nie będziesz mógł ich ponownie zdefiniować dla aplikacji zarządzanej przez tą zasadę.

- Oznaczanie zdarzeń dla zarządzanej aplikacji. Jeśli oznaczysz zdarzenia do wyeksportowania dla zarządzanej aplikacji, zainstalowanej na zarządzanym urządzeniu, system SIEM otrzyma tylko zdarzenia, które wystąpiły w tej aplikacji.

Informacje dotyczące oznaczania zdarzeń do wyeksportowania do systemu SIEM w formacie Syslog

Po włączeniu automatycznego eksportowania zdarzeń, należy wskazać zdarzenia, które zostaną wyeksportowane do zewnętrznego systemu SIEM.

Możesz skonfigurować eksportowanie zdarzeń w formacie Syslog do zewnętrznego systemu w oparciu o jeden z następujących warunków:

- Oznaczanie zdarzeń ogólnych. Jeśli zdarzenia do wyeksportowania oznaczysz w zasadzie, w ustawieniach zdarzenia lub w ustawieniach Serwera administracyjnego system SIEM otrzyma oznaczone zdarzenia, które wystąpiły we wszystkich aplikacjach zarządzanych przez określoną zasadę. Jeśli wyeksportowane zdarzenia były wybrane w zasadzie, nie będziesz mógł ich ponownie zdefiniować dla aplikacji zarządzanej przez tą zasadę.
- Oznaczanie zdarzeń dla zarządzanej aplikacji. Jeśli oznaczysz zdarzenia do wyeksportowania dla zarządzanej aplikacji, zainstalowanej na zarządzanym urządzeniu, system SIEM otrzyma tylko zdarzenia, które wystąpiły w tej aplikacji.

Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog

Jeśli chcesz wyeksportować zdarzenia, które wystąpiły w określonej zarządzanej aplikacji, zainstalowanej na zarządzanych urządzeniach, w zasadzie aplikacji oznacz zdarzenia do wyeksportowania. W takim przypadku zaznaczone zdarzenia są eksportowane ze wszystkich urządzeń objętych zakresem zasady.

W celu oznaczenia zdarzeń do wyeksportowania dla określonej zarządzanej aplikacji:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Profile zasad**.
2. Kliknij zasadę aplikacji, dla której chcesz oznaczyć zdarzenia.

   Zostanie otwarte okno ustawień zasady.
3. Przejdź do sekcji **Konfiguracja zdarzenia**.
4. Zaznacz pola obok zdarzeń, które chcesz wyeksportować do systemu SIEM.
5. Kliknij przycisk **Zaznacz do eksportu do systemu SIEM poprzez Syslog**.

   Możesz także oznaczyć zdarzenie do wyeksportowania do systemu SIEM w sekcji **Rejestracja zdarzenia**, która zostanie otwarta po kliknięciu odnośnika zdarzenia.
6. Znacznik (✓) pojawi się w kolumnie **Syslog** zdarzenia lub zdarzeń, które oznaczyłeś do wyeksportowania do systemu SIEM.
7. Kliknij przycisk **Zapisz**.

Oznaczone zdarzenia z zarządzanej aplikacji są gotowe do wyeksportowania do systemu SIEM.

Możesz zaznaczyć, które zdarzenia wyeksportować do systemu SIEM dla określonego zarządzanego urządzenia. Jeśli poprzednio wyeksportowane zdarzenia były oznaczone w zasadzie aplikacji, nie będziesz mógł ponownie zdefiniować oznaczonych zdarzeń dla zarządzanego urządzenia.

W celu oznaczenia zdarzeń do wyeksportowania dla zarządzanego urządzenia:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Kliknij odnośnik z nazwą żądanego urządzenia na liście zarządzanych urządzeń.

   Zostanie wyświetlone okno właściwości wybranego urządzenia.

3. Przejdź do sekcji **Aplikacje**.

4. Kliknij odnośnik z nazwą żądanej aplikacji na liście aplikacji.

5. Przejdź do sekcji **Konfiguracja zdarzenia**.

6. Zaznacz pola obok zdarzeń, które chcesz wyeksportować do SIEM.

7. Kliknij przycisk **Zaznacz do eksportu do systemu SIEM poprzez Syslog**.

   Dodatkowo, możesz oznaczyć zdarzenie do wyeksportowania do systemu SIEM w sekcji **Rejestracja zdarzenia**, która zostanie otwarta po kliknięciu odnośnika zdarzenia.

8. Znacznik (✓) pojawi się w kolumnie **Syslog** zdarzenia lub zdarzeń, które oznaczyłeś do wyeksportowania do systemu SIEM.

Od tego momentu Serwer administracyjny wysyła do systemu SIEM oznaczone zdarzenia, jeśli eksportowanie do systemu SIEM zostało skonfigurowane.

Oznaczanie ogólnych zdarzeń do eksportu w formacie Syslog

Możesz oznaczyć zdarzenia ogólne, które Serwer administracyjny wyeksportuje do systemów SIEM przy użyciu formatu Syslog.

W celu oznaczenia zdarzeń ogólnych do wyeksportowania do systemu SIEM:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.
   - W menu głónym przejdź do **Zasoby (urządzenia)** → **Profile zasad**, a następnie kliknij odnośnik do zasady.

2. W otwartym oknie przejdź na zakładkę **Konfiguracja zdarzenia**.

3. Kliknij **Zaznacz do eksportu do systemu SIEM poprzez Syslog**.

   Dodatkowo, możesz oznaczyć zdarzenie do wyeksportowania do systemu SIEM w sekcji **Rejestracja zdarzenia**, która zostanie otwarta po kliknięciu odnośnika zdarzenia.

4. Znacznik (✓) pojawi się w kolumnie **Syslog** zdarzenia lub zdarzeń, które oznaczyłeś do wyeksportowania do systemu SIEM.

Od tego momentu Serwer administracyjny wysyła do systemu SIEM oznaczone zdarzenia, jeśli eksportowanie do systemu SIEM zostało skonfigurowane.

Informacje dotyczące eksportowania zdarzeń przy użyciu formatów CEF i LEEF

Możesz użyć formatów CEF i LEEF, aby wyeksportować ogólne zdarzenia do systemów SIEM, a także zdarzenia przesyłane przez aplikacje Kaspersky do Serwera administracyjnego. Zestaw eksportowanych zdarzeń jest predefiniowany i nie możesz wybrać zdarzeń do wyeksportowania. Przed wysłaniem zdarzeń do systemu SIEM (QRadar, ArcSight lub Splunk) konieczna jest interpretacja zdarzeń Kaspersky Security Center jako zdarzeń w formacie CEF i LEEF przy użyciu reguł określonych w pliku siem_conversion_rules.xml.

Wybierz format eksportowania w oparciu o używany system SIEM. Poniższa tabela wyświetla systemy SIEM i odpowiadające im formaty eksportu.

Formaty eksportowania zdarzenia do systemu SIEM

System SIEM	Format eksportu
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) - dostosowany format zdarzeń dla IBM Security QRadar SIEM. QRadar może integrować, identyfikować i przetwarzać zdarzenia LEEF. Zdarzenia LEEF muszą używać kodowania UTF-8. Szczegółowe informacje na temat protokołu LEEF można znaleźć w Centrum wiedzy IBM.

- CEF (Common Event Format)—standard zarządzania dziennikami, który ulepsza współdziałanie zdarzeń dotyczących bezpieczeństwa między różnymi urządzeniami i aplikacjami sieciowymi i zabezpieczającymi. CEF umożliwia korzystanie z podstawowego formatu dziennika zdarzeń, co ułatwia integrowanie i gromadzenie danych do analizy przez system zarządzania korporacji. Zdarzenia CEF muszą używać kodowania UTF-8.

Automatyczne eksportowanie oznacza, że Kaspersky Security Center wysyła ogólne zdarzenia do systemu SIEM. Automatyczne eksportowanie zdarzeń rozpoczyna się od razu po włączeniu tej opcji. Ta sekcja szczegółowo wyjaśnia, jak włączyć automatyczne eksportowanie zdarzeń.

Konwersja zdarzeń do formatu CEF lub LEEF

Przed wysłaniem zdarzeń do systemu SIEM (QRadar, ArcSight lub Splunk) konieczna jest interpretacja zdarzeń Kaspersky Security Center jako zdarzeń w formacie CEF i LEEF przy użyciu reguł określonych w pliku siem_conversion_rules.xml. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center.

Plik siem_conversion_rules.xml zawiera predefiniowane reguły interpretacji umożliwiające konwersję zdarzeń do formatu CEF i LEEF. Jeśli chcesz użyć dodatkowych reguł interpretacji zdarzeń, możesz dodać je do pliku ręcznie.

Plik siem_conversion_rules.xml zawiera następujące sekcje:

- `<product name="SP_QRADAR" vendor="IBM">`

  Ta sekcja zawiera reguły generowania zdarzeń w formacie LEEF, które można wyeksportować do systemu QRadar SIEM.

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  Ta sekcja zawiera reguły generowania zdarzeń w formacie CEF, które można wyeksportować do systemu ArcSight lub Splunk SIEM.

Każda sekcja ma podsekcję `<common>`, w której znajdują się atrybuty zdarzeń Kaspersky Security Center i odpowiadające im atrybuty zdarzeń w formacie LEEF. Te wspólne atrybuty są używane dla wszystkich typów zdarzeń, które można eksportować.

Ponadto każda sekcja ma podsekcje `<event>`. Każda podsekcja `<event>` zawiera dodatkowe atrybuty, które są dodawane do tych wymienionych w sekcji `<common>`.

Możesz ręcznie dodać nową regułę generowania zdarzeń do pliku siem_conversion_rules.xml.

Aby dodać nową regułę generowania zdarzeń:

1. Dodaj nową podsekcję `<event>` do sekcji `<product name="SP_QRADAR" vendor="IBM">` lub `<product name="SP_ARCSIGHT" vendor="HP">`, a następnie określ dodatkowe atrybuty zdarzenia, jeśli to konieczne.

2. Jeżeli zdarzenie składa się wyłącznie ze wspólnych atrybutów, podsekcja `<event>` będzie pusta.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

Informacje dotyczące eksportowania zdarzeń przy użyciu formatu Syslog

Możesz użyć formatu Syslog do wyeksportowania do systemów SIEM zdarzeń, które występują na Serwerze administracyjnym i w innych aplikacjach firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach.

Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Pozwala on na rozdzielenie oprogramowania, które generuje wiadomości, systemu, które je przechowuje, oraz oprogramowania, które raportuje i analizuje te wiadomości. Do każdej wiadomości przypisywany jest kod funkcji, wskazujący typ oprogramowania, które generuje wiadomość, oraz priorytet.

Format Syslog jest definiowany przez dokumenty RFC (Request for Comments — prośba o komentarze), publikowane przez Internet Engineering Task Force (standardy internetowe). Standard RFC 5424 jest używany do eksportowania zdarzeń z Kaspersky Security Center do systemów zewnętrznych.

W Kaspersky Security Center możesz skonfigurować eksportowanie zdarzeń do systemów zewnętrznych przy użyciu formatu Syslog.

Proces eksportowania składa się z dwóch etapów:

1. Włączanie automatycznego eksportowania zdarzeń. W tym kroku program Kaspersky Security Center jest konfigurowany tak, aby wysyłał zdarzenia do systemu SIEM. Kaspersky Security Center rozpoczyna wysyłanie zdarzeń natychmiast po włączeniu automatycznego eksportowania.

2. Wybieranie zdarzeń eksportowanych do systemu zewnętrznego. W tym kroku wybierasz zdarzenia, które będą eksportowane do systemu SIEM.

Konfigurowanie Kaspersky Security Center do wyeksportowania zdarzeń do systemu SIEM

Aby wyeksportować zdarzenia do systemu SIEM, musisz skonfigurować proces eksportu w Kaspersky Security Center Web Console.

Przed wysłaniem zdarzeń do systemu SIEM (QRadar, ArcSight lub Splunk) konieczna jest interpretacja zdarzeń Kaspersky Security Center jako zdarzeń w formacie CEF i LEEF przy użyciu reguł określonych w pliku siem_conversion_rules.xml.

W celu skonfigurowania eksportowania do systemów SIEM w Kaspersky Security Center Web Console:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Ogólne** wybierz sekcję **Eksportuj do SIEM**.

3. Kliknij odnośnik **Ustawienia**.

   Zostanie otwarta sekcja **Eksportuj ustawienia**.

4. W sekcji **Eksportuj ustawienia** określ ustawienia:

   - **Adres serwera systemu SIEM**

     Adres IP serwera, na którym zainstalowany jest aktualnie używany system SIEM. Sprawdź wartość tego ustawienia w ustawieniach systemu SIEM.

- **Port systemu SIEM**

  Numer portu używanego do nawiązania połączenia pomiędzy Kaspersky Security Center a serwerem Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center i w ustawieniach odbiornika Twojego systemu SIEM.

- **Protokół**

  Wybierz protokół, który będzie używany do przesyłania wiadomości do systemu SIEM. Możesz wybrać protokół TCP, UDP lub TLS poprzez protokół TCP.

  Określ następujące ustawienia TLS, jeśli wybierzesz TLS poprzez protokół TCP:

  - **Uwierzytelnianie serwera**

    W polu **Uwierzytelnianie serwera** możesz wybrać wartości **Zaufane certyfikaty** lub **Odciski palców SHA**:

    - **Zaufane certyfikaty**. Możesz otrzymać kompletny łańcuch certyfikatów (włącznie z certyfikatem głównym) od zaufanych urzędów certyfikacji (CA) i przesłać plik do Kaspersky Security Center. Kaspersky Security Center sprawdza, czy łańcuch certyfikatów serwera systemu SIEM jest również podpisany przez zaufany urząd certyfikacji, czy nie.

      Aby dodać zaufany certyfikat, kliknij przycisk **Przeglądaj w poszukiwaniu pliku certyfikatów urzędu certyfikacji**, a następnie prześlij certyfikat.

    - **Odciski palców SHA**. Możesz określić odciski palców SHA1 kompletnego łańcucha certyfikatów systemu SIEM (w tym certyfikatu głównego) w Kaspersky Security Center. Aby dodać odcisk palca SHA1, wprowadź go w polu **Odciski kciuka** palców, a następnie kliknij przycisk **Dodaj**.

    Korzystając z ustawienia **Dodaj uwierzytelnianie klienta**, możesz wygenerować certyfikat do uwierzytelnienia Kaspersky Security Center. W ten sposób będziesz używać certyfikatu z podpisem własnym wystawionego przez Kaspersky Security Center. W takim przypadku do uwierzytelnienia serwera systemu SIEM można użyć zarówno zaufanego certyfikatu, jak i odcisku palca SHA.

  - **Dodaj nazwę podmiotu / nazwę alternatywną podmiotu**

    Nazwa podmiotu to nazwa domeny, dla której otrzymano certyfikat. Kaspersky Security Center nie może połączyć się z serwerem systemu SIEM, jeśli nazwa domeny serwera systemu SIEM nie jest zgodna z nazwą podmiotu certyfikatu serwera systemu SIEM. Jednak serwer systemu SIEM może zmienić swoją nazwę domeny, jeśli zmieniła się nazwa w certyfikacie. W takim przypadku można określić nazwy podmiotów w polu **Dodaj nazwę podmiotu / nazwę alternatywną podmiotu**. Jeśli dowolna z podanych nazw podmiotów odpowiada nazwie podmiotu certyfikatu systemu SIEM, Kaspersky Security Center zweryfikuje certyfikat serwera systemu SIEM.

  - **Dodaj uwierzytelnianie klienta**

W celu uwierzytelnienia klienta możesz wstawić swój certyfikat lub wygenerować go w Kaspersky Security Center.

- **Wstaw certyfikat**. Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

  - **Certyfikat X.509 PEM**. Prześlij plik z certyfikatem w polu **Plik z certyfikatem** oraz plik z kluczem prywatnym w polu **Plik z kluczem**. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po przesłaniu obu plików określ hasło do dekodowania klucza prywatnego w polu **Weryfikacja hasła lub certyfikatu**. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

  - **Certyfikat X.509 PKCS12**. Prześlij pojedynczy plik zawierający certyfikat i jego klucz prywatny w polu **Plik z certyfikatem**. Po przesłaniu pliku określ hasło do dekodowania klucza prywatnego w polu **Weryfikacja hasła lub certyfikatu**. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

- **Generuj klucz**. Możesz wygenerować certyfikat z podpisem własnym w Kaspersky Security Center. W rezultacie Kaspersky Security Center przechowuje wygenerowany certyfikat z podpisem własnym i możesz przekazać publiczną część certyfikatu lub odcisk palca SHA1 do systemu SIEM.

- **Format danych**

  Możesz wybrać formaty Kaspersky SIEM, IBM QRadar SIEM, ArcSight, Splunk lub dziennik systemowy, w zależności od wymagań systemu SIEM.

Jeżeli wybierzesz format danych System log, musisz określić:

- **Maksymalny rozmiar wiadomości, w bajtach**

  Określ maksymalny rozmiar (w bajtach) jednej wiadomości przekazywanej do systemu SIEM. Każde zdarzenie jest przesyłane w jednej wiadomości. Jeśli rzeczywisty rozmiar wiadomości przekracza określoną wartość, wiadomość jest skracana i dane mogą zostać utracone. Domyślny rozmiar to 2048 bajtów. To pole jest dostępne tylko wtedy, gdy w polu **Protokół** wybrałeś format System log.

5. Jeśli chcesz, możesz wyeksportować zarchiwizowane zdarzenia z bazy danych Serwera administracyjnego i ustawić datę początkową, od której chcesz rozpocząć eksport zarchiwizowanych zdarzeń:

   a. Kliknij łącze **Wybierz datę rozpoczęcia eksportu**.

   b. W sekcji, która zostanie otwarta, w polu **Data rozpoczęcia eksportu zdarzeń systemowych** podaj datę rozpoczęcia.

   c. Kliknij przycisk **OK**.

6. Przełącz opcję na pozycję **Automatycznie eksportuj zdarzenia do bazy danych systemu SIEM Włączone**.

7. Aby sprawdzić, czy połączenie z systemem SIEM zostało skonfigurowane, kliknij przycisk **Sprawdź połączenie**.

   Nawiązywane jest połączenie z serwerem systemu SIEM i wysyłane jest zdarzenie testowe. Zostanie wyświetlony stan połączenia.

   Sprawdzanie jest wykonywane wyłącznie w przypadku protokołów TCP i TLS przez protokół TCP.

8. Kliknij przycisk **Zapisz**.

Eksportowanie do systemu SIEM zostało skonfigurowane.

Eksportowanie zdarzeń bezpośrednio z bazy danych

Zdarzenia można otrzymywać bezpośrednio z bazy danych Kaspersky Security Center bez konieczności korzystania z interfejsu Kaspersky Security Center. Możesz wykonać zapytanie bezpośrednio do widoków publicznych i pobrać dane zdarzenia lub utworzyć swoje własne widoki w oparciu o istniejące widoki publiczne i adresować je w celu otrzymania żądanych danych.

Widoki publiczne

Dla Twojej wygody, w bazie danych Kaspersky Security Center dostępny jest zestaw widoków publicznych. Opis tych widoków publicznych można znaleźć w dokumentacji klakdb.chm.

Widok publiczny v_akpub_ev_event zawiera zestaw pól, które reprezentują parametry zdarzenia w bazie danych. W dokumencie klakdb.chm możesz także znaleźć informacje dotyczące widoków publicznych odpowiadających innym obiektom Kaspersky Security Center, na przykład: urządzeniom, aplikacjom lub użytkownikom. Możesz użyć tych informacji w swoich zapytaniach.

Ta sekcja zawiera instrukcje dotyczące tworzenia zapytania SQL przy użyciu narzędzia klsql2 oraz przykłady zapytań.

Aby utworzyć zapytania SQL lub widoki bazy danych, możesz także użyć innego dowolnego programu do pracy z bazami danych. Informacje dotyczące przeglądania parametrów połączenia z bazą danych Kaspersky Security Center, takich jak nazwa instancji i nazwa bazy danych, znajdują się w odpowiedniej sekcji.

Tworzenie zapytania SQL przy użyciu narzędzia klsql2

Ten artykuł opisuje sposób pobierania i korzystania z narzędzia klsql2, a także sposób tworzenia zapytań SQL przy użyciu tego narzędzia.

W celu użycia narzędzia klsql2:

1. Zlokalizuj narzędzie klsql2 w folderze instalacyjnym Kaspersky Security Center. Domyślna ścieżka instalacji to <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Nie używaj wersji narzędzia klsql2 przeznaczonych dla starszych wersji Kaspersky Security Center.

2. Utwórz plik .sql w dowolnym edytorze tekstu i umieść plik w tym samym folderze co narzędzie.

3. W pliku .sql wpisz typ żądanego zapytania SQL, a następnie zapisz plik.

4. Na urządzeniu z zainstalowanym Serwerem administracyjnym Kaspersky Security Center, w wierszu polecenia wpisz następujące polecenie do uruchomienia zapytania SQL z pliku .sql i zapisz wyniki do pliku result.xml:
   ```
   klsql2 -i src.sql -u <nazwa użytkownika> -p <hasło> -o result.xml
   ```
   gdzie `<nazwa użytkownika>` i `<hasło>` to poświadczenia konta użytkownika, który ma dostęp do bazy danych.

5. W razie potrzeby wprowadź login i hasło konta użytkownika, który ma dostęp do bazy danych.

6. Otwórz nowo utworzony plik result.xml, aby wyświetlić wyniki zapytania SQL.

Możesz zmodyfikować plik .sql i utworzyć dowolne zapytanie SQL do widoków publicznych. Następnie, z poziomu wiersza poleceń, wykonaj zapytanie SQL i zapisz wyniki do pliku.

Przykład zapytania SQL w narzędziu klsql2

W tej sekcji przedstawiono przykład zapytania SQL tworzonego przy użyciu narzędzia klsql2.

Poniższe przykłady ilustrują otrzymanie zdarzeń, które wystąpiły na urządzeniach w ciągu ostatnich siedmiu dni, oraz wyświetlenie zdarzeń według czasu ich wystąpienia. Najnowsze zdarzenia są wyświetlane jako pierwsze.

Przykład dla Microsoft SQL Server:

```
SELECT
  /* identyfikator zdarzenia */
  e.nId,

  /* godzina wystąpienia zdarzenia */
  e.tmRiseTime,

  /* wewnętrzna nazwa typu zdarzenia */
  e.strEventType,

  /* wyświetlona nazwa zdarzenia */
  e.wstrEventTypeDisplayName,

  /* wyświetlony opis zdarzenia */
  e.wstrDescription,

  /* nazwa grupy, w której znajduje się zdarzenie */
  e.wstrGroupName,

  /* wyświetlona nazwa urządzenia, na którym wystąpiło zdarzenie */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* adres IP urządzenia, na którym wystąpiło zdarzenie */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Przykład dla PostgreSQL:

```
SELECT
  /* identyfikator zdarzenia */
  "e"."nId",

  /* godzina wystąpienia zdarzenia */
  "e"."tmRiseTime",

  /* wewnętrzna nazwa typu zdarzenia */
  "e"."strEventType",

  /* wyświetlona nazwa zdarzenia */
  "e"."wstrEventTypeDisplayName",

  /* wyświetlony opis zdarzenia */
  "e"."wstrDescription",

  /* wyświetlony opis zdarzenia */
  "e"."wstrGroupName",

  /* wyświetlona nazwa urządzenia, na którym wystąpiło zdarzenie */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* adres IP urządzenia, na którym wystąpiło zdarzenie */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Przykład dla MySQL lub MariaDB:

```
SELECT

  /* identyfikator zdarzenia */
  `e`.`nId`,

  /* godzina wystąpienia zdarzenia */
  `e`.`tmRiseTime`,

  /* wewnętrzna nazwa typu zdarzenia */
  `e`.`strEventType`,

  /* wyświetlona nazwa zdarzenia */
  `e`.`wstrEventTypeDisplayName`,

  /* wyświetlony opis zdarzenia */
  `e`.`wstrDescription`,

  /* nazwa grupy urządzeń */
  `e`.`wstrGroupName`,

  /* wyświetlona nazwa urządzenia, na którym wystąpiło zdarzenie */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* adres IP urządzenia, na którym wystąpiło zdarzenie */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Sprawdzanie nazwy bazy danych Kaspersky Security Center

Jeśli chcesz uzyskać dostęp do bazy danych Kaspersky Security Center przy użyciu narzędzi do zarządzania serwerem SQL lub bazą danych MySQL lub MariaDB, musisz znać nazwę bazy danych, aby nawiązać z nią połączenie z poziomu swojego edytora skryptów SQL.

W celu wyświetlenia nazwy bazy danych Kaspersky Security Center:

1. W menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Ogólne** wybierz sekcję **Szczegóły bieżącej bazy danych**.

   Nazwa bazy danych jest określona w polu **Nazwa bazy danych**. Użyj nazwy bazy danych, aby adresować bazę danych w swoich zapytaniach SQL.

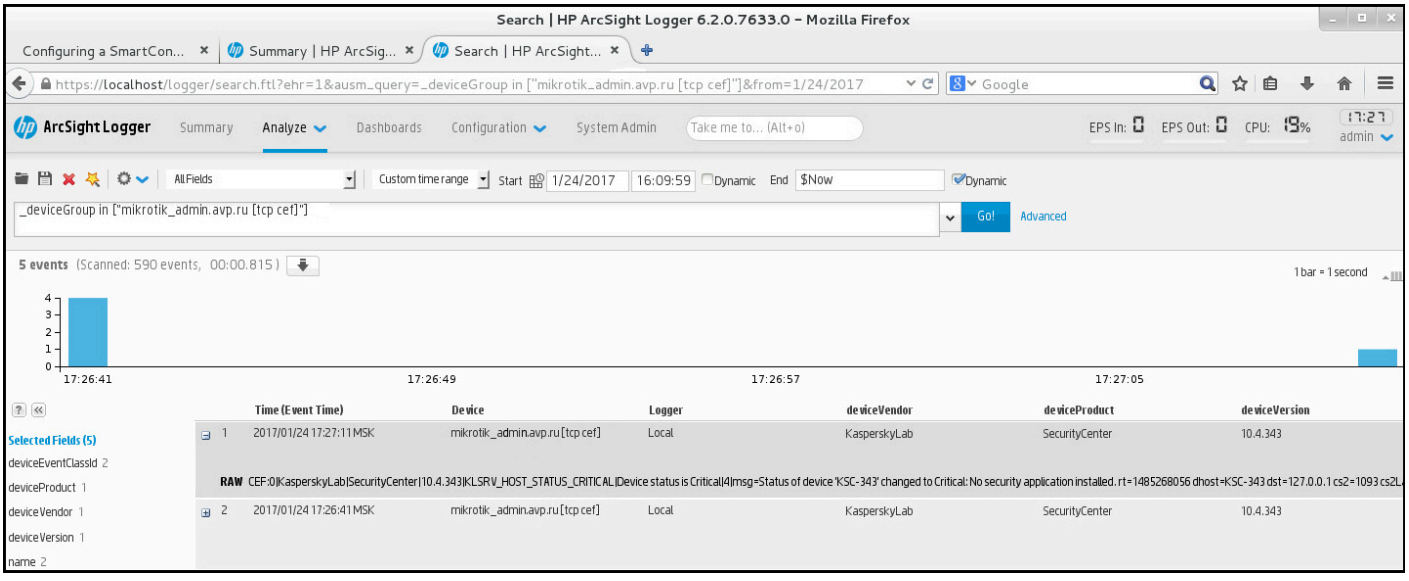
Przeglądanie wyników eksportowania

Możesz kontrolować pomyślne zakończenie procedury eksportowania zdarzeń. W tym celu sprawdź, czy wiadomości z eksportowanymi zdarzeniami są otrzymywane przez Twój system SIEM.

Jeśli zdarzenia wysłane z Kaspersky Security Center są odbierane i poprawnie analizowane przez Twój system SIEM, konfiguracja po obu stronach została przeprowadzona właściwie. Jeśli jest inaczej, sprawdź ustawienia, które określiłeś w Kaspersky Security Center, porównując je z konfiguracją w Twoim systemie SIEM.

Poniższy rysunek przedstawia zdarzenia wyeksportowane do ArcSight. Na przykład, pierwsze zdarzenie jest krytycznym zdarzeniem Serwera administracyjnego: „*Urządzenie posiada stan Krytyczny*”.

Reprezentacja eksportowania zdarzeń w systemie SIEM różni się w zależności od tego, którego systemu SIEM używasz.



Przykład zdarzeń

Praca z Kaspersky Security Center Web Console i środowiskiem w chmurze

Ta sekcja zawiera informacje o funkcjach Kaspersky Security Center Web Console dotyczących zdalnej instalacji i konserwacji Kaspersky Security Center w środowiskach chmury, takich jak Amazon Web Services, Microsoft Azure lub Google Cloud.

Aby móc pracować w obrębie środowiska chmury, potrzebna jest specjalna licencja. Jeśli nie posiadasz takiej licencji, elementy interfejsu dotyczące urządzeń w chmurze nie są wyświetlane.

Konfiguracja środowiska chmury w Kaspersky Security Center Web Console

Aby skonfigurować Kaspersky Security Center przy użyciu Kreatora konfiguracji środowiska chmury, musisz mieć:

- Następujące dane uwierzytelniające środowiska w chmurze:
  - Rolę IAM, której udzielono uprawnienie do przeszukiwania segmentu chmury lub konto użytkownika IAM, któremu udzielono uprawnienia do przeszukiwania segmentu chmury (do pracy z Amazon Web Services)
  - ID aplikacji Azure, hasło i subskrypcję (do pracy z Microsoft Azure)
  - Poczta klienta Google, ID projektu i klucz prywatny (do pracy z Google Cloud)
- Pakiety instalacyjne:
  - Agent sieciowy dla systemu Windows
  - Agent sieciowy dla systemu Linux
  - Kaspersky Endpoint Security for Linux
- Wtyczka sieciowa dla Kaspersky Endpoint Security for Linux
- Wybierz jeden z następujących:
  - Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Endpoint Security for Windows (zalecane)
  - Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Security for Windows Server

Kreator konfiguracji środowiska chmury uruchamia się automatycznie przy pierwszym połączeniu z Serwerem administracyjnym za pośrednictwem Konsoli administracyjnej, jeśli program Kaspersky Security Center jest instalowany za pomocą gotowego do użycia obrazu. Kreator można również uruchomić ręcznie w dowolnym momencie.

Aby ręcznie uruchomić Kreatora konfiguracji środowiska chmury:

W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Konfiguruj środowisko chmury**.

Zostanie uruchomiony kreator.

Przeciętna sesja pracy nad konfiguracją środowiska chmury trwa około 15 minut.

Krok 1. Sprawdzanie wymaganych wtyczek i pakietów instalacyjnych

Ten krok nie jest wyświetlany, jeśli masz wszystkie wymagane wtyczki internetowe i pakiety instalacyjne wymienione poniżej.

Aby skonfigurować środowisko w chmurze, musisz mieć następujące komponenty:

- Pakiety instalacyjne:
  - Agent sieciowy dla systemu Windows
  - Agent sieciowy dla systemu Linux
  - Kaspersky Endpoint Security for Linux
- Wtyczka sieciowa dla Kaspersky Endpoint Security for Linux
- Wybierz jeden z następujących:
  - Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Endpoint Security for Windows (zalecane)
  - Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Security for Windows Server

    Zalecamy używanie Kaspersky Endpoint Security for Windows zamiast Kaspersky Security for Windows Server.

Kaspersky Security Center automatycznie wykrywa komponenty, które już posiadasz i wyświetla listę tylko tych, których brakuje. Pobierz wymienione komponenty, klikając przycisk **Wybierz aplikacje do pobrania**, a następnie wybierając wymagane wtyczki i pakiety instalacyjne. Po pobraniu składnika można użyć przycisku **Odśwież**, aby zaktualizować listę brakujących składników.

Krok 2. Licencjonowanie aplikacji

Ten krok jest wyświetlany tylko wtedy, gdy używasz BYOL AMI i nie aktywowałeś aplikacji przy użyciu licencji dla Kaspersky Security for Virtualization lub licencji dla Kaspersky Hybrid Cloud Security.

Określ klucz licencyjny i kliknij **Dalej**, aby przejść dalej.

Klucz licencyjny, który określiłeś, zostanie dodany do repozytorium Serwera administracyjnego.

Jeśli uruchomisz kreator ponownie, ten krok nie będzie wyświetlany.

Krok 3. Wybieranie środowiska chmury i autoryzacji

Ta sekcja opisuje funkcje stosowane tylko do Kaspersky Security Center 12.1 lub nowszej wersji.

Określ następujące ustawienia:

- **Środowisko chmury**

  Wybierz środowisko chmury, w którym instalujesz Kaspersky Security Center: AWS, Azure lub Google Cloud.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem w chmurze, wybierz jedno środowisko, a następnie uruchom kreator ponownie.

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment", „AWS Segment" lub „Google Segment".

Wprowadź swoje dane uwierzytelniające do autoryzacji w środowisku chmury.

AWS

Jeśli jako typ segmentu chmury wybrałeś AWS, potrzebujesz roli IAM lub klucza dostępu AWS IAM do dalszego przeszukiwania segmentu chmury.

- **Rola AWS IAM przypisana do instancji EC2**

  Wybierz tę opcję, jeśli posiadasz rolę IAM z wymaganymi uprawnieniami dla Serwera administracyjnego.

- **Użytkownik AWS IAM**

  Wybierz tę opcję, jeśli posiadasz klucz dostępu AWS IAM. Wprowadź swoje dane klucza:

  - **Identyfikator klucza dostępu**

    Identyfikator klucza dostępu IAM to sekwencja znaków alfanumerycznych. Identyfikator klucza otrzymałeś podczas tworzenia konta użytkownika IAM.

    Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

  - **Klucz tajny**

    Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

    Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

    Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

    Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

Azure

Jeśli jako typ segmentu chmury wybrałeś Azure, określ następujące ustawienia dla połączenia, które będą używane do dalszego przeszukiwania segmentu chmury:

- **ID aplikacji Azure**

  Ten ID aplikacji utworzyłeś na portalu Azure.

  Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **ID subskrypcji platformy Azure**

  Subskrypcję utworzyłeś na portalu Azure.

- **Hasło do aplikacji Azure**

  Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

  Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

  Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

- **Nazwa konta magazynu Azure**

  Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

- **Klucz dostępu do magazynu Azure**

  Hasło (klucz) uzyskałeś po utworzeniu konta magazynu Azure do pracy z Kaspersky Security Center.

  Klucz jest dostępny w sekcji „Overview of the Azure storage account", w podsekcji „Keys".

  Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

Google Cloud

Jeśli jako typ segmentu chmury wybrałeś Google Cloud, określ następujące ustawienia dla połączenia, które będą używane do dalszego przeszukiwania segmentu chmury:

- **Adres e-mail klienta**

  Wprowadź adres e-mail klienta, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Identyfikator projektu**

  Identyfikator projektu to identyfikator, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Klucz prywatny**

  Klucz prywatny to sekwencja znaków, które otrzymałeś jako klucz prywatny po zarejestrowaniu projektu w Google Cloud. Możesz skopiować i wkleić tę sekwencję, aby uniknąć błędów.

Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

To połączenie, które określiłeś, zostanie zapisane w ustawieniach aplikacji.

Kreator konfiguracji środowiska chmury umożliwia określenie tylko jednego segmentu. Później możesz określić więcej połączeń do zarządzania innymi segmentami chmury.

Kliknij **Dalej**, aby przejść dalej.

Krok 4. Przeszukiwanie segmentu, konfigurowanie synchronizacji z chmurą i wybieranie dalszych działań

W tym kroku rozpoczyna się przeszukiwanie segmentu chmury i automatycznie tworzona jest specjalna grupa administracyjna dla urządzeń w chmurze. Urządzenia, wykryte podczas przeszukiwania, zostają umieszczone w tej grupie. Konfigurowany jest terminarz przeszukiwania segmentu chmury (domyślnie, co 5 minut; możesz zmienić to ustawienie później).

Tworzona jest także reguła automatycznego przydzielania **Synchronizuj z chmurą**. Dla każdego kolejnego skanowania sieci chmury, wykryte urządzenia wirtualne zostaną przeniesione do odpowiedniej podgrupy w obrębie grupy **Zarządzane urządzenia****Chmura**.

Określ następujące ustawienia:

- **Synchronizuj grupy administracyjne ze strukturą chmury**

  Jeśli ta opcja jest włączona, grupa **Chmura** jest automatycznie tworzona w obrębie grupy **Zarządzane urządzenia** oraz zostaje uruchomione wyszukiwanie urządzeń w chmurze. Instancje i maszyny wirtualne, które zostały wykryte w trakcie każdego skanowania sieci chmury, zostają umieszczone w grupie Chmura. Struktura podgrup administracyjnych w obrębie tej grupy odpowiada strukturze Twojego segmentu chmury (w AWS, strefy dostępności i grupy położenia nie są przedstawione w strukturze; w Azure, podsieci nie są przedstawione w strukturze). Urządzenia, które nie zostały zidentyfikowane jako instancje w środowisku chmury, znajdują się w grupie **Urządzenia nieprzypisane**. Struktura grupa umożliwia korzystanie z grupowych zadań instalacji do zainstalowania aplikacji antywirusowych na instancjach, a także skonfigurowanie różnych zasad dla różnych grup.

  Jeśli ta opcja jest wyłączona, tworzona jest także grupa **Chmura** oraz uruchamiane jest wyszukiwanie urządzeń; jednakże podgrupy odpowiadające strukturze segmentu chmury nie są tworzone w obrębie tej grupy. Wszystkie wykryte instancje znajdują się w grupie administracyjnej **Chmura**, więc są wyświetlane na jednej liście. Jeśli Twoja praca z Kaspersky Security Center wymaga synchronizacji, możesz zmodyfikować właściwości reguły **Synchronizuj z chmurą** i wymusić ją. Wymuszenie tej reguły zmieni strukturę podgrup w grupie Chmura tak, że będzie ona odpowiadała strukturze segmentu chmury.

  Domyślnie opcja ta jest wyłączona.

- **Roześlij ochronę**

  Jeśli ta opcja jest zaznaczona, kreator tworzy zadanie instalacji aplikacji zabezpieczających na instancjach. Po zakończeniu pracy kreatora, na urządzeniach w Twoich segmentach chmury automatycznie uruchamiany jest Kreator wdrażania ochrony, dzięki czemu możliwe będzie zainstalowanie Agenta sieciowego i aplikacji zabezpieczających na tych urządzeniach.

  Kaspersky Security Center może przeprowadzić zdalną instalację przy użyciu swoich narzędzi. Jeśli nie masz uprawnień do instalowania aplikacji na instancjach EC2 lub maszynach wirtualnych Azure, możesz ręcznie skonfigurować zadanie **Zdalna instalacja** oraz określić konto z wymaganymi uprawnieniami. W tym przypadku, zadanie Zdalna instalacja nie będzie działało dl urządzeń wykrytych przy użyciu AWS API lub Azure. To zadanie będzie działało tylko dla urządzeń wykrytych przy użyciu przeszukiwania Active Directory, przeszukiwania domeny Windows lub przeszukiwania zakresu IP.

Jeśli ta opcja nie jest zaznaczona, Kreator wdrażania ochrony nie zostanie uruchomiony, a zadania instalacji aplikacji zabezpieczających na instancjach nie zostaną utworzone. Te działania można wykonać ręcznie w późniejszym czasie.

Jeśli wybierzesz opcję Roześlij ochronę, sekcja **Ponowne uruchamianie urządzeń** stanie się dostępna. W tej sekcji musisz wybrać, co zrobić, gdy system operacyjny urządzenia docelowego musi zostać uruchomiony ponownie. Wybierz, czy instancje powinny być uruchamiane ponownie, jeśli system operacyjny urządzenia musi być uruchomiony ponownie podczas instalacji aplikacji:

- **Nie uruchamiaj ponownie**

  Jeśli ta opcja jest zaznaczona, urządzenie nie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

- **Uruchom ponownie**

  Jeśli ta opcja jest zaznaczona, urządzenie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

Kliknij **Dalej**, aby przejść dalej.

W przypadku Google Cloud możesz przeprowadzić tylko zdalną instalację natywnych narzędzi Kaspersky Security Center. Jeśli wybrałeś Google Cloud, opcja **Roześlij ochronę** nie jest dostępna.

Krok 5. Wybieranie aplikacji, w odniesieniu do której mają zostać utworzone zasada i zadania

Ten krok jest wyświetlany tylko wtedy, gdy posiadasz pakiety instalacyjne i wtyczki zarówno dla Kaspersky Endpoint Security for Windows, jak i Kaspersky Security for Windows Server. Jeśli masz wtyczkę i pakiet instalacyjny tylko dla jednej z tych aplikacji, ten krok zostanie pominięty, a Kaspersky Security Center utworzy zasadę i zadania dla istniejącej aplikacji.

Wybierz aplikację, dla której chcesz utworzyć zasadę i zadania:

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

Krok 6. Konfigurowanie Kaspersky Security Network dla Kaspersky Security Center

Określ ustawienia przekazywania informacji o działaniach Kaspersky Security Center do bazy wiedzy Kaspersky Security Network (KSN). Wybierz jedną z następujących opcji:

- **Zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje zainstalowane na urządzeniach klienckich automatycznie prześlą szczegóły swoich działań do Kaspersky Security Network. Uczestnictwo w Kaspersky Security Network umożliwia szybsze aktualizowanie baz danych zawierających informacje o wirusach i innych zagrożeniach, co zapewnia szybszą reakcję na pojawiające się zagrożenia bezpieczeństwa.

- **Nie zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje nie dostarczą informacji do Kaspersky Security Network.

  Jeśli wybierzesz tę opcję, korzystanie z Kaspersky Security Network zostanie wyłączone.

Kaspersky zaleca uczestniczenie w Kaspersky Security Network.

Mogą zostać wyświetlone także oświadczenia KSN. Jeśli zgodzisz się na korzystanie z Kaspersky Security Network, zarządzana aplikacja będzie wysyłała dane do Kaspersky. Jeśli nie wyrażasz zgody na uczestnictwo w Kaspersky Security Network, zarządzana aplikacja nie wyśle danych do Kaspersky (możesz zmienić to ustawienie w późniejszym czasie w zasadzie aplikacji).

Kliknij **Dalej**, aby przejść dalej.

Krok 7. Tworzenie wstępnej konfiguracji ochrony

Możesz sprawdzić listę utworzonych zasad i zadań.

Zaczekaj, aż tworzenie zasad i zadań zostanie zakończone, a następnie kliknij **Dalej**, aby przejść dalej. Na ostatniej stronie kreatora kliknij przycisk **Zakończ**, aby wyjść.

Przeszukiwanie segmentu sieci za pośrednictwem Kaspersky Security Center Web Console

Informacje o strukturze sieci (i urządzeniach w tej sieci) są otrzymywane przez Serwer administracyjny poprzez regularne przeszukiwanie segmentów chmury przy pomocy narzędzi AWS API, Azure API lub Google API. Kaspersky Security Center używa tych informacji do aktualizacji zawartości folderów: Urządzenia nieprzypisane i Zarządzane urządzenia. Jeżeli skonfigurowałeś automatyczne przenoszenie urządzeń do grup administracyjnych, wykryte urządzenia zostaną włączone do grup administracyjnych.

Aby zezwolić Serwerowi administracyjnemu na przeszukiwanie segmentów chmury, musisz posiadać odpowiednie uprawnienia dla roli IAM lub dla konta użytkownika IAM (w AWS) lub przy pomocy hasła i ID aplikacji (w Azure) lub przy pomocy poczty klienta Google, identyfikatora projektu Google i klucza prywatnego (w Google Cloud).

Możesz dodawać i usuwać połączenia, a także ustawić terminarz przeszukiwania dla każdego segmentu chmury.

Dodawanie połączeń dla przeszukiwania segmentu chmury

W celu dodania połączenia dla przeszukiwania segmentu chmury do listy dostępnych połączeń:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Chmura**.
2. W otwartym oknie kliknij **Właściwości**.
3. W otwartym oknie **Ustawienia** kliknij **Dodaj**.

   Zostanie otwarte okno **Ustawienia segmentu chmury**.

4. Określ nazwę środowiska chmury dla połączenia, która będzie używana do dalszego przeszukiwania segmentu chmury:

   - **Środowisko chmury**

     Wybierz środowisko chmury, w którym instalujesz Kaspersky Security Center: AWS, Azure lub Google Cloud.

     Jeśli planujesz pracować z więcej niż jednym środowiskiem w chmurze, wybierz jedno środowisko, a następnie uruchom kreator ponownie.

   - **Nazwa połączenia**

     Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

     Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

     Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment", „AWS Segment" lub „Google Segment".

5. Wprowadź swoje dane uwierzytelniające do autoryzacji w środowisku chmury.

   - Jeśli wybrałeś AWS, określ następujące ustawienia:

     - **Użyj roli AWS IAM**

       Wybierz tę opcję, jeśli już utworzyłeś rolę IAM dla Serwera administracyjnego do korzystania z usług AWS.

     - **Poświadczenia konta użytkownika AWS IAM**

       Wybierz tę opcję, jeśli posiadasz konto użytkownika IAM z wymaganymi uprawnieniami oraz możesz wprowadzić ID klucza oraz tajny klucz.

       Jeśli określiłeś, że posiadasz Poświadczenia konta użytkownika AWS IAM, określ następujące elementy:

       - **Identyfikator klucza dostępu**

         Identyfikator klucza dostępu IAM to sekwencja znaków alfanumerycznych. Identyfikator klucza otrzymałeś podczas tworzenia konta użytkownika IAM.

         Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

       - **Klucz tajny**

         Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

         Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

         Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

       Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

   - Jeśli wybrałeś Azure, określ następujące ustawienia:

     - **ID aplikacji Azure**

       Ten ID aplikacji utworzyłeś na portalu Azure.

       Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **ID subskrypcji platformy Azure**

  Subskrypcję utworzyłeś na portalu Azure.

- **Hasło do aplikacji Azure**

  Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

  Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

  Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

- **Nazwa konta magazynu Azure**

  Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

- **Klucz dostępu do magazynu Azure**

  Hasło (klucz) uzyskałeś po utworzeniu konta magazynu Azure do pracy z Kaspersky Security Center.

  Klucz jest dostępny w sekcji „Overview of the Azure storage account", w podsekcji „Keys".

  Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

Jeśli wybrałeś Google Cloud, określ następujące ustawienia:

- **Adres e-mail klienta**

  Wprowadź adres e-mail klienta, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Identyfikator projektu**

  Identyfikator projektu to identyfikator, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Klucz prywatny**

  Klucz prywatny to sekwencja znaków, które otrzymałeś jako klucz prywatny po zarejestrowaniu projektu w Google Cloud. Możesz skopiować i wkleić tę sekwencję, aby uniknąć błędów.

  Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

6. Jeśli chcesz, kliknij **Ustaw terminarz przeszukiwania** i zmień ustawienia domyślne.

To połączenie zostanie zapisane w ustawieniach aplikacji.

Po pierwszym przeszukaniu nowego segmentu chmury, w grupie administracyjnej **Zarządzane urządzenia\Chmura** pojawi się podgrupa odpowiadająca temu segmentowi.

Jeśli określisz niepoprawne dane uwierzytelniające, podczas przeszukiwania segmentu chmury nie zostaną wykryte żadne instancje, a nowa podgrupa nie pojawi się w grupie administracyjnej **Zarządzane urządzenia\Chmura**.

Usuwanie połączenia dla przeszukiwania segmentu chmury

Jeśli już nie chcesz przeszukiwać określonego segmentu chmury, możesz usunąć połączenie odpowiadające temu segmentowi z listy dostępnych połączeń. Połączenie można usunąć także wtedy, gdy, na przykład, uprawnienia do przeszukiwania segmentu chmury zostały przeniesione na innego użytkownika, który posiada inne dane uwierzytelniające.

W celu usunięcia połączenia:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Chmura**.
2. W otwartym oknie kliknij **Właściwości**.
3. W oknie **Ustawienia**, które zostanie otwarte, kliknij nazwę segmentu, który chcesz usunąć.
4. Kliknij **Usuń**.
5. W otwartym oknie kliknij przycisk **OK**, aby potwierdzić swój wybór.

Połączenie zostanie usunięte. Urządzenia w segmencie chmury odpowiadające temu połączeniu są automatycznie usuwane z grup administracyjnych.

Konfigurowanie terminarza przeszukiwania za pośrednictwem Kaspersky Security Center Web Console

Przeszukiwanie segmentu chmury odbywa się zgodnie z terminarzem. Możesz ustawić częstotliwość przeszukiwania.

Częstotliwość przeszukiwania jest automatycznie ustawiana na 5 minut w ustawieniach konfiguracji środowiska chmury. Możesz zmienić tę wartość w dowolnym momencie i ustawić inny terminarz. Nie jest zalecane konfigurowanie wykonywania przeszukiwania z częstotliwością większą niż co 5 minut, ponieważ może to prowadzić do błędów w działaniu AWS API.

W celu skonfigurowania terminarza przeszukiwania segmentu chmury:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Chmura**.
2. W otwartym oknie kliknij **Właściwości**.
3. W oknie **Ustawienia**, które zostanie otwarte, kliknij nazwę segmentu, dla którego chcesz skonfigurować terminarz przeszukiwania.

   To spowoduje otwarcie okna **Ustawienia segmentu chmury**.
4. W oknie **Ustawienia segmentu chmury** kliknij przycisk **Ustaw terminarz przeszukiwania**.

   Zostanie otwarte okno **Terminarz**.
5. W oknie **Terminarz** określ następujące ustawienia:

   - **Zaplanowane uruchomienie**

Dostępne są następujące opcje terminarza przeszukiwania:

- **Co N dni**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

  Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- Co N minut

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

  Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

- Według dni tygodnia

  Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- Co miesiąc, w określone dni wybranych tygodni

  Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Czas uruchomienia**

  Określ, co oznacza N (minuty lub dni).

- **Począwszy od**

  Określ, kiedy rozpocząć pierwsze przeszukiwanie.

- **Uruchom pominięte zadania**

  Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

  Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

  Domyślnie opcja ta jest włączona.

6. Zapisz zmiany.

Terminarz przeszukiwania dla segmentu zostaje skonfigurowany i zapisany.

Przeglądanie wyników przeszukiwania segmentu chmury za pośrednictwem Kaspersky Security Center Web Console

Możesz przejrzeć wyniki przeszukiwania segmentu chmury, przejrzyj listę urządzeń w chmurze, zarządzanych przez Serwer administracyjny.

W celu przejrzenia wyników przeszukiwania segmentu chmury:

W menu głównym przejdź do **Wykrywanie i wdrażanie → Wykrywanie → Chmura**.

Spowoduje to wyświetlenie segmentów chmury dostępnych do przeszukania.

Przeglądanie właściwości urządzeń w chmurze za pośrednictwem Kaspersky Security Center Web Console

Możesz przejrzeć właściwości każdego urządzenia w chmurze.

W celu przejrzenia właściwości urządzenia w chmurze:

1. W menu głównym przejdź do **Zasoby (urządzenia) → Zarządzane urządzenia**.
2. Kliknij nazwę urządzenia, którego właściwości chcesz przejrzeć.

   Zostanie otwarte okno właściwości na wybranej sekcji **Ogólne**.
3. Jeśli chcesz przejrzeć właściwości charakterystyczne dla urządzeń w chmurze, w oknie właściwości wybierz sekcję **System**.

   Właściwości są wyświetlane w zależności od platformy w chmurze urządzenia.

   Dla urządzeń w AWS wyświetlane są następujące właściwości:

   - **Urządzenie wykryte przy pomocy API** (wartość: **AWS**)
   - **Region chmury**
   - **Cloud VPC**
   - **Strefa dostępności chmury**
   - **Podsieć chmury**
   - **Grupa położenia w chmurze** (ta jednostka jest wyświetlana tylko wtedy, gdy instancja należy do grupy położenia; w innym przypadku nie jest wyświetlana)

   Dla urządzeń w Azure wyświetlane są następujące właściwości:

   - **Urządzenie wykryte przy pomocy API** (wartość: **Microsoft Azure**)
   - **Region chmury**
   - **Podsieć chmury**

   Dla urządzeń w Google Cloud wyświetlane są następujące właściwości:

   - **Urządzenie wykryte przy pomocy API** (wartość: **Google Cloud**)
   - **Region chmury**
   - **Cloud VPC**

- **Strefa dostępności chmury**
- **Podsieć chmury**

Synchronizacja z chmurą: konfigurowanie reguły przenoszenia

Podczas operacji Konfiguruj środowisko chmurowe automatycznie tworzona jest reguła Synchronizuj z chmurą. Ta reguła umożliwia automatyczne przenoszenie urządzeń, wykrytych przy każdym przeszukiwaniu, z grupy Urządzenia nieprzypisane do grupy Zarządzane urządzenia\Chmura, aby te urządzenia stały się dostępne dla scentralizowanego zarządzania. Domyślnie, reguła jest aktywna po utworzeniu. Regułę można wyłączyć, zmodyfikować lub wymusić w dowolnym momencie.

W celu zmodyfikowania właściwości reguły Synchronizuj z chmurą i/lub wymuszenia reguły:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Reguły przenoszenia**.

   Spowoduje to otwarcie listy reguł przenoszenia.

2. Na liście reguł przenoszenia wybierz **Synchronizuj z chmurą**.

   Spowoduje to otwarcie okna właściwości reguły.

3. Jeśli to konieczne, określ następujące ustawienia na zakładce **Warunki reguły**, na zakładce **Segmenty chmury**:

   - **Urządzenie znajduje się w segmencie chmury**

     Reguła jest tylko stosowana do urządzeń, które znajdują się w wybranym segmencie chmury. W innej sytuacji reguła będzie stosowana do wszystkich urządzeń, które zostały wykryte.

     Domyślnie opcja ta jest zaznaczona.

   - **Włączając obiekty potomne**

     Reguła będzie stosowana do wszystkich urządzeń w wybranym segmencie i we wszystkich zagnieżdżonych podsekcjach chmury. W innym przypadku reguła jest tylko stosowana do urządzeń, które znajdują się w głównym segmencie.

     Domyślnie opcja ta jest zaznaczona.

   - **Przenieś urządzenia z obiektów zagnieżdżonych do odpowiednich podgrup**

     Jeśli ta opcja jest włączona, urządzenia z obiektów zagnieżdżonych zostaną automatycznie przeniesione do podgrup, które odpowiadają ich strukturze.

     Jeśli ta opcja jest wyłączona, urządzenia z obiektów zagnieżdżonych zostaną automatycznie przeniesione do głównej podgrupy Chmura bez dalszego rozdzielania.

     Domyślnie opcja ta jest włączona.

   - **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń**

     Jeśli ta opcja jest włączona, gdy struktura grupy **Zarządzane urządzenia\Chmura** nie posiada podgrup, które będą odpowiadały sekcji zawierającej urządzenie, Kaspersky Security Center utworzy takie podgrupy. Na przykład, jeśli nowa podsieć zostanie wykryta podczas wyszukiwania urządzeń, nowa grupa z taką samą nazwą zostanie utworzona w grupie **Zarządzane urządzenia\Chmura**.

     Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie tworzy żadnych nowych podgrup. Na przykład, jeśli nowa podsieć zostanie wykryta podczas przeszukiwania sieci, nowa grupa o tej samej nazwie nie zostanie utworzona w grupie **Zarządzane urządzenia\Chmura**, a urządzenia, które są w tej podsieci, zostaną przeniesione do grupy **Zarządzane urządzenia\Chmura**.

Domyślnie opcja ta jest włączona.

- **Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury**

  Jeśli ta opcja jest włączona, aplikacja usunie z grupy Chmura wszystkie podgrupy, które nie odpowiadają żadnym istniejącym obiektom chmury.

  Jeśli ta opcja jest wyłączona, podgrupy, które nie odpowiadają żadnym istniejącym obiektom chmury, zostaną zachowane.

  Domyślnie opcja ta jest włączona.

Jeśli podczas korzystania z kreatora konfiguracji środowiska chmury włączono opcję **Synchronizuj grupy administracyjne ze strukturą chmury**, reguła **Synchronizuj z chmurą** zostanie utworzona z włączonymi opcjami **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń** i **Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury**.

Jeśli nie włączyłeś opcji **Synchronizuj grupy administracyjne ze strukturą chmury**, reguła **Synchronizuj z chmurą** zostanie utworzona z wyłączonymi (odznaczonymi) tymi opcjami. Jeśli Twoja praca z Kaspersky Security Center wymaga, aby struktura podgrup w podgrupie **Zarządzane urządzenia** \ **Chmura** odpowiadała strukturze segmentów chmury, włącz opcje **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń** i **Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury** we właściwościach reguły, a następnie wymuś regułę.

4. Z listy rozwijalnej **Urządzenie wykryte przy pomocy API** wybierz jedną z następujących wartości:

   - **Nie**. Urządzenie nie może zostać wykryte przy użyciu AWS, Azure lub Google API, co oznacza, że znajduje się poza środowiskiem chmury lub znajduje się w środowisku chmury, ale z jakiegoś powodu nie może zostać wykryte przy użyciu API.

   - **AWS**. Urządzenie jest wykrywane przy pomocy AWS API, co oznacza, że urządzenie znajduje się w środowisku chmury AWS.

   - **Azure**. Urządzenie jest wykrywane przy pomocy Azure API, co oznacza, że urządzenie znajduje się w środowisku chmury Azure.

   - **Google Cloud**. Urządzenie jest wykrywane przy pomocy Google API, co oznacza, że urządzenie znajduje się w środowisku chmury Google.

   - Brak wartości. To kryterium nie może zostać zastosowane.

5. Jeśli to konieczne, skonfiguruj inne właściwości reguły w innych sekcjach.

Reguła przenoszenia została skonfigurowana.

Zdalna instalacja aplikacji na maszynach wirtualnych Azure

Aby zainstalować aplikacje na maszynach wirtualnych Microsoft Azure, musisz mieć ważną licencję.

Kaspersky Security Center obsługuje następujące scenariusze:

- Urządzenie klienckie jest wykrywane przy użyciu Azure API; instalacja odbywa się również przy użyciu API. Korzystanie z Azure API oznacza, że możesz zainstalować tylko następujące aplikacje:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- Urządzenie klienckie jest wykrywane za pomocą Azure API; instalacja odbywa się za pośrednictwem punktu dystrybucji lub w przypadku braku punktów dystrybucji ręcznie przy użyciu samodzielnych pakietów instalacyjnych. W ten sposób możesz zainstalować dowolną aplikację obsługiwaną przez Kaspersky Security Center.

Aby utworzyć zadanie zdalnej instalacji aplikacji na maszynach wirtualnych Azure:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. Postępuj zgodnie z instrukcjami kreatora:

   a. Wybierz opcję **Zdalna instalacja aplikacji** jako typ zadania.

   b. Na stronie **Pakiety instalacyjne** wybierz opcję **Zdalna instalacja przez Microsoft Azure API**.

   c. Wybierając konto, aby uzyskać dostęp do urządzeń, użyj istniejącego konta Azure lub kliknij **Dodaj** i wprowadź poświadczenia swojego konta Azure:

   - **Nazwa konta Azure**

     Wprowadź dowolną nazwę dla określonych poświadczeń. Ta nazwa pojawi się na liście kont do uruchomienia zadania.

   - **ID aplikacji Azure**

     Ten ID aplikacji utworzyłeś na portalu Azure.

     Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

   - **Hasło do aplikacji Azure**

     Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

     Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

   d. Wybierz odpowiednie urządzenia z grupy **Zarządzane urządzenia** \ **Chmura**.

Po zakończeniu pracy kreatora, zadanie zdalnej instalacji aplikacji pojawi się na liście zadań.

Tworzenie zadania Utwórz kopię zapasową danych Serwera administracyjnego przy użyciu systemu DBMS w chmurze

Zadania tworzenia kopii zapasowej są zadaniami Serwera administracyjnego. Tworzysz zadanie tworzenia kopii zapasowej, jeśli chcesz użyć systemu DBMS znajdującego się w środowisku chmury (AWS lub Azure).

W celu utworzenia zadania kopii zapasowej danych Serwera administracyjnego:

1. W menu głównym przejdź do **Zasoby (urządzenia)** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W pierwszym kroku kreatora, na liście **Aplikacja** wybierz **Kaspersky Security Center 15.1**, a na liście **Typ zadania** wybierz **Kopia zapasowa danych Serwera administracyjnego**.
4. W odpowiednim kroku kreatora określ następujące informacje:

   - Jeśli pracujesz z bazami danych w AWS:

     - **Nazwa komory S3**

       Nazwa komory S3, którą utworzyłeś dla Kopii zapasowej.

     - **Identyfikator klucza dostępu**

       Identyfikator klucza (sekwencja znaków alfanumerycznych) uzyskałeś podczas tworzenia konta użytkownika IAM do pracy z instancją magazynu komory S3.

       Pole jest dostępne, jeśli w komorze S3 wybrałeś bazę danych RDS.

     - **Tajny klucz**

       Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

       Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

       Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

   - Jeśli pracujesz z bazami danych w Microsoft Azure:

     - **Nazwa konta magazynu Azure**

       Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

     - **ID subskrypcji Azure**

       Subskrypcję utworzyłeś na portalu Azure.

     - **Hasło Azure**

       Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

- **ID aplikacji Azure**

  Ten ID aplikacji utworzyłeś na portalu Azure.

  Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **Nazwa serwera Azure SQL**

  Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

- **Grupa zasobów serwera Azure SQL**

  Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

- **Klucz dostępu do magazynu Azure**

  Dostępne we właściwościach Twojego konta magazynu, w sekcji Klucze dostępu. Możesz użyć dowolnego klucza (key1 lub key2).

Zadanie zostanie utworzone i będzie wyświetlane na liście zadań. Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, możesz zmodyfikować domyślne ustawienia zadania od razu po utworzeniu zadania. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

Zdalna diagnostyka urządzeń klienckich

Możesz użyć zdalnej diagnostyki do zdalnego wykonania następujących operacji na urządzeniach klienckich z systemem Windows i z systemem Linux:

- Włączania i wyłączania śledzenia, zmieniania poziomu śledzenia i pobierania pliku śledzenia
- Pobierania informacji o systemie i ustawień aplikacji
- Pobierania dzienników zdarzeń
- Generowania pliku zrzutu dla aplikacji
- Uruchamiania diagnostyki i pobierania jej raportów
- Uruchamianie, zatrzymywanie i ponowne uruchamianie aplikacji

Możesz użyć dzienników zdarzeń i raportów diagnostycznych pobranych z urządzenia klienckiego do samodzielnego rozwiązania problemów. Dodatkowo, jeśli skontaktujesz się z działem pomocy technicznej Kaspersky, specjalista z pomocy technicznej może poprosić o pobranie plików śledzenia, plików zrzutu pamięci, dzienników zdarzeń, a także raportów diagnostycznych z urządzenia klienckiego w celu przeprowadzenia dalszej analizy w Kaspersky.

Otwieranie okna zdalnej diagnostyki

Aby przeprowadzić zdalną diagnostykę na urządzeniach klienckich z systemem Windows i systemem Linux, należy najpierw otworzyć okno zdalnej diagnostyki.

W celu otwarcia okna zdalnej diagnostyki:

1. W celu wybrania urządzenia, dla którego chcesz otworzyć okno zdalnej diagnostyki, wykonaj jedną z następujących czynności:

   - Jeśli urządzenie należy do grupy administracyjnej, w menu głównym przejdź do **Zasoby (urządzenia)** → **Zarządzane urządzenia**.
   - Jeśli urządzenie należy do grupy Urządzenia nieprzypisane, w menu głównym przejdź do **Wykrywanie i wdrażanie** → **Urządzenia nieprzypisane**.

2. Kliknij nazwę żądanego urządzenia.
3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Zaawansowane**.
4. W otwartym oknie kliknij opcję **Zdalna diagnostyka**.

   Spowoduje to otwarcie okna **Zdalna diagnostyka** urządzenia klienckiego. Jeżeli połączenie między Serwerem administracyjnym a urządzeniem klienckim nie zostanie nawiązane, zostanie wyświetlony komunikat o błędzie.

Alternatywnie, jeśli chcesz uzyskać jednocześnie wszystkie informacje diagnostyczne na temat urządzenia klienckiego z systemem Linux, możesz uruchomić na tym urządzeniu skrypt collect.sh.

Włączanie i wyłączanie śledzenia dla aplikacji

Możesz włączyć i wyłączyć śledzenie aplikacji, w tym śledzenie Xperf.

Włączanie i wyłączanie śledzenia

W celu włączenia lub wyłączenia śledzenia na zdalnym urządzeniu:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.

   W sekcji **Zarządzanie aplikacjami** wyświetlana jest lista aplikacji Kaspersky zainstalowanych na urządzeniu.

3. Na liście aplikacji wybierz aplikację, dla której chcesz włączyć lub wyłączyć śledzenie.

   Zostanie otwarta lista opcji zdalnej diagnostyki.

4. Jeśli chcesz włączyć śledzenie:

   a. W sekcji **Śledzenie** kliknij **Włącz śledzenie**.

   b. W otwartym oknie **Modyfikuj poziom śledzenia** zalecane jest zachowanie domyślnych wartości ustawień. Jeśli jest to wymagane, specjalista z pomocy technicznej przeprowadzi Cię przez proces konfiguracji. Dostępne są następujące ustawienia:

   - **Poziom śledzenia**

     Poziom śledzenia definiuje ilość szczegółów, jaką plik śledzenia zawiera.

   - **Śledzenie z rotacją plików**

     Aplikacja nadpisuje informacje o śledzeniu, aby zapobiec nadmiernemu zwiększeniu rozmiaru pliku śledzenia. Określ maksymalną liczbę plików, jaka będzie używana do przechowywania informacji o śledzeniu, a także maksymalny rozmiar każdego pliku. Jeśli zostanie zapisana maksymalna liczba plików śledzenia o maksymalnym rozmiarze, najstarszy plik śledzenia zostanie usunięty, aby mógł zostać zapisany nowy plik śledzenia.

     To ustawienie jest dostępne tylko dla Kaspersky Endpoint Security.

   c. Kliknij **Zapisz**.

   Śledzenie jest włączone dla wybranej aplikacji. W niektórych przypadkach, aby włączyć śledzenie, konieczne jest ponowne uruchomienie aplikacji zabezpieczającej i jej zadania.

   > Na urządzeniach klienckich z systemem Linux śledzenie dla komponentu Updater of Network Agent jest regulowane przez ustawienia Agenta sieciowego. Dlatego opcje **Włącz śledzenie** i **Modyfikuj poziom śledzenia** są wyłączone dla tego modułu na urządzeniach klienckich z systemem Linux.

5. Jeśli chcesz wyłączyć śledzenie dla wybranej aplikacji, kliknij przycisk **Wyłącz śledzenie**.

   Śledzenie jest wyłączone dla wybranej aplikacji.

Włączanie śledzenia Xperf

W przypadku Kaspersky Endpoint Security specjalista z pomocy technicznej może poprosić o włączenie śledzenia Xperf dla informacji o działaniu systemu.

Aby włączyć i skonfigurować śledzenie Xperf lub je wyłączyć:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.

2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.

   W sekcji **Zarządzanie aplikacjami** wyświetlana jest lista aplikacji Kaspersky zainstalowanych na urządzeniu.

3. Na liście aplikacji wybierz Kaspersky Endpoint Security for Windows.

   Zostanie wyświetlona lista opcji zdalnej diagnostyki dla Kaspersky Endpoint Security for Windows.

4. W sekcji **Śledzenie Xperf** kliknij opcję **Włącz śledzenie Xperf**.

   Jeśli śledzenie Xperf jest już włączone, zamiast tego zostanie wyświetlony przycisk **Wyłącz śledzenie Xperf**. Kliknij ten przycisk, jeśli chcesz wyłączyć śledzenie Xperf dla Kaspersky Endpoint Security for Windows.

5. W otwartym oknie **Zmień poziom śledzenia Xperf**, w zależności od odpowiedzi od specjalisty z pomocy technicznej, wykonaj jedną z następujących czynności:

   a. Wybierz jeden z następujących poziomów śledzenia:

   - **Niski**

     Plik śledzenia tego typu zawiera minimalną ilość informacji o systemie.

     Domyślnie opcja ta jest zaznaczona.

   - **Głęboki**

     Plik śledzenia tego typu zawiera bardziej szczegółowe informacje niż pliki śledzenia typu *Niski* i specjaliści z pomocy technicznej mogą poprosić o nie, gdy plik śledzenia typu *Niski* nie jest wystarczający do oceny działania. *Głęboki* plik śledzenia zawiera informacje techniczne o systemie, w tym informacje o sprzęcie, systemie operacyjnym, listę uruchomionych i zakończonych procesów i aplikacji, zdarzeń użytych do oceny działania, a także zdarzeń z Narzędzia do oceny wydajności systemu Windows.

   b. Wybierz jeden z następujących typów śledzenia Xperf:

   - **Podstawowy**

     Informacje o śledzeniu są otrzymywane podczas działania aplikacji Kaspersky Endpoint Security.

     Domyślnie opcja ta jest zaznaczona.

   - **Po ponownym uruchomieniu**

     Informacje o śledzeniu są otrzymywane, gdy system operacyjny jest uruchamiany na zarządzanym urządzeniu. Ten typ śledzenia jest efektywny, gdy problem, który wpływa na działanie systemu, pojawi się po włączeniu urządzenia, a przed uruchomieniem Kaspersky Endpoint Security.

   Możesz także zostać poproszony o włączenie opcji **Rozmiar pliku, po którym nastąpi nadpisanie, w MB**, aby zapobiec nadmiernemu zwiększeniu rozmiaru pliku śledzenia. Następnie określ maksymalny rozmiar pliku śledzenia. Jeśli plik osiągnie maksymalny rozmiar, najstarsze informacje śledzenia zostaną nadpisane nowymi informacjami.

   c. Zdefiniuj rozmiar pliku rotacji.

   d. Kliknij **Zapisz**.

   Śledzenie Xperf jest włączone i skonfigurowane.

6. Jeśli chcesz wyłączyć śledzenie Xperf dla Kaspersky Endpoint Security for Windows, kliknij opcję **Wyłącz śledzenie Xperf** w sekcji **Śledzenie Xperf**.

   Śledzenie Xperf jest wyłączone.

Pobieranie plików śledzenia aplikacji

W celu pobrania pliku śledzenia aplikacji:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.

   W sekcji **Zarządzanie aplikacjami** wyświetlana jest lista aplikacji Kaspersky zainstalowanych na urządzeniu.
3. Na liście aplikacji wybierz aplikację, dla której chcesz pobrać plik śledzenia.
4. W sekcji **Śledzenie** kliknij przycisk **Pliki śledzenia**.

   To spowoduje otwarcie okna **Dzienniki śledzenia urządzenia**, w którym wyświetlana jest lista plików śledzenia.
5. Z listy plików śledzenia wybierz plik, który chcesz pobrać.
6. Wykonaj jedną z poniższych czynności:

   - Pobierz wybrany plik, klikając **Pobierz**. Możesz wybrać jeden lub kilka plików do pobrania.
   - Pobierz porcję wybranego pliku:

     a. Kliknij **Pobierz część**.

     Nie można jednocześnie pobierać części kilku plików. Jeśli wybierzesz więcej niż jeden plik śledzenia, przycisk **Pobierz część** będzie nieaktywny.

     b. W otwartym oknie określ nazwę i fragment pliku do pobrania, zgodnie ze swoimi potrzebami.

     W przypadku urządzeń z systemem Linux edytowanie nazwy części pliku nie jest dostępne.

     c. Kliknij **Pobierz**.

Wybrany plik lub jego porcja zostają pobrane do lokalizacji, którą określiłeś.

Usuwanie plików śledzenia

Możesz usunąć pliki śledzenia, które nie są już potrzebne.

W celu usunięcia pliku śledzenia:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W otwartym oknie zdalnej diagnostyki wybierz kartę **Dzienniki zdarzeń**.
3. W sekcji **Pliki śledzenia** kliknij opcję **Raporty usługi Windows Update** lub **Raporty zdalnej instalacji** w zależności od plików śledzenia, które chcesz usunąć.

   Odnośnik **Raporty usługi Windows Update** jest dostępny tylko dla urządzeń klienckich z systemem Windows.

To spowoduje otwarcie okna **Dzienniki śledzenia urządzenia**, w którym wyświetlana jest lista plików śledzenia.

4. Z listy plików śledzenia wybierz jeden lub większą liczbę plików, które chcesz usunąć.
5. Kliknij przycisk **Usuń**.

Wybrane pliki śledzenia zostaną usunięte.

Pobierania ustawień aplikacji

W celu pobrania ustawień aplikacji z urządzenia klienckiego:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.
3. W sekcji **Ustawienia aplikacji** kliknij przycisk **Pobierz**, aby pobrać informacje o ustawieniach aplikacji zainstalowanych na urządzeniu klienckim.

Archiwum ZIP z informacjami zostanie pobrane do określonej lokalizacji.

Pobierania dzienników zdarzeń

W celu pobrania dziennika zdarzeń ze zdalnego urządzenia:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki, na karcie **Dzienniki zdarzeń** kliknij **Wszystkie dzienniki urządzenia**.
3. W oknie **Wszystkie dzienniki urządzenia** wybierz jeden lub kilka dzienników.
4. Wykonaj jedną z poniższych czynności:
   - Pobierz wybrany plik, klikając **Pobierz cały plik**.
   - Pobierz porcję wybranego dziennika:
     a. Kliknij **Pobierz część**.
     Nie można jednocześnie pobierać części kilku dzienników. Jeśli wybierzesz więcej niż jeden dziennik zdarzeń, przycisk **Pobierz część** będzie nieaktywny.
     b. W otwartym oknie określ nazwę i część pliku do pobrania, odpowiednio do potrzeb.
     W przypadku urządzeń z systemem Linux funkcja edytowania nazwy części dziennika nie jest dostępna.
     c. Kliknij **Pobierz**.

Wybrany dziennik zdarzeń lub jego część zostają pobrane do określonej lokalizacji.

Uruchamianie, zatrzymywanie, ponowne uruchamianie aplikacji

Aplikację można uruchomić, zatrzymać lub uruchomić ponownie.

W celu uruchomienia, zatrzymania lub ponownego uruchomienia aplikacji:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.

   W sekcji **Zarządzanie aplikacjami** wyświetlana jest lista aplikacji Kaspersky zainstalowanych na urządzeniu.
3. Na liście aplikacji wybierz aplikację, którą chcesz uruchomić, zatrzymać lub uruchomić ponownie.
4. Wybierz akcję, klikając jeden z następujących przycisków:

   - **Zatrzymaj aplikację**

     Ten przycisk jest dostępny tylko wtedy, gdy aplikacja jest aktualnie uruchomiona.
   - **Uruchom aplikację ponownie**

     Ten przycisk jest dostępny tylko wtedy, gdy aplikacja jest aktualnie uruchomiona.
   - **Uruchom aplikację**

     Ten przycisk jest dostępny tylko wtedy, gdy aplikacja nie jest aktualnie uruchomiona.

   W zależności od wybranej akcji, wymagana aplikacja zostanie uruchomiona, zatrzymana lub uruchomiona ponownie na urządzeniu klienckim.

Jeśli uruchomisz ponownie Agenta sieciowego, zostanie wyświetlona wiadomość informująca, że bieżące połączenie urządzenia z Serwerem administracyjnym zostanie utracone.

Uruchamianie zdalnej diagnostyki agenta sieciowego Kaspersky Security Center i pobieranie wyników

Aby rozpocząć diagnostykę Agenta sieciowego Kaspersky Security Center na urządzeniu zdalnym i pobrać wyniki:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Aplikacje Kaspersky**.

   W sekcji **Zarządzanie aplikacjami** wyświetlana jest lista aplikacji Kaspersky zainstalowanych na urządzeniu.
3. Na liście aplikacji wybierz opcję **Agent sieciowy Kaspersky Security Center**.

   Zostanie otwarta lista opcji zdalnej diagnostyki.

4. W sekcji **Raport diagnostyczny** kliknij przycisk **Uruchom diagnostykę**.

   Spowoduje to uruchomienie procesu zdalnej diagnostyki i wygenerowanie raportu diagnostycznego. Po zakończeniu procesu diagnostyki, przycisk **Pobierz raport diagnostyczny** stanie się dostępny.

5. Kliknij przycisk **Pobierz raport diagnostyczny**, aby pobrać raport.

Raport zostanie pobrany do określonej lokalizacji.

Uruchamianie aplikacji na urządzeniu klienckim

Konieczne może być uruchomienie aplikacji na urządzeniu klienckim, jeśli specjalista z pomocy technicznej firmy Kaspersky poprosi o to. Nie trzeba instalować aplikacji na tym urządzeniu.

W celu uruchomienia aplikacji na urządzeniu klienckim:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Uruchamianie aplikacji zdalnej**.
3. W sekcji **Pliki aplikacji** kliknij przycisk **Przeglądaj**, aby wybrać archiwum ZIP zawierające aplikację, którą chcesz uruchomić na urządzeniu klienckim.

   Archiwum ZIP musi zawierać folder z narzędziami. Ten folder zawiera plik wykonywalny do uruchomienia na urządzeniu zdalnym.

   W razie potrzeby można określić nazwę pliku wykonywalnego i w razie potrzeby argumenty wiersza polecenia. W tym celu należy wypełnić **pole Plik wykonywalny w archiwum do uruchomienia na urządzeniu zdalnym** oraz pola **Argumenty wiersza polecenia**.
4. Kliknij przycisk **Wczytaj i uruchom**, aby uruchomić określoną aplikację na urządzeniu klienckim.
5. Postępuj zgodnie z instrukcjami specjalisty działu pomocy Kaspersky.

Generowania pliku zrzutu dla aplikacji

Plik zrzutu dla aplikacji umożliwia przeglądanie parametrów aplikacji uruchomionej na urządzeniu klienckim w danym momencie. Ten plik zawiera również informacje o modułach, które zostały załadowane dla aplikacji.

Zbieranie plików zrzutu z urządzeń z systemem Linux nie jest obsługiwane.

Do zbierania plików zrzutu za pomocą zdalnej diagnostyki używane jest narzędzie kldumper. Narzędzie to jest przeznaczone do zbierania plików zrzutu procesów aplikacji Kaspersky na prośbę specjalistów pomocy technicznej. Szczegółowe informacje na temat wymagań dotyczących korzystania z narzędzia kldumper można znaleźć w bazie wiedzy Kaspersky Security Center.

Tworzenie pliku zrzutu dla aplikacji:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie zdalnej diagnostyki wybierz kartę **Uruchamianie aplikacji zdalnej**.
3. W sekcji **Generowanie plik zrzutu procesu** określ plik wykonywalny aplikacji, dla której chcesz wygenerować plik zrzutu.
4. Kliknij przycisk **Pobierz plik zrzutu**.

   Pobierane jest archiwum z plikiem zrzutu dla określonej aplikacji.

   Jeśli wskazana aplikacja nie jest uruchomiona na urządzeniu klienckim, folder „result" zawarty w pobranym archiwum będzie pusty.

   Jeśli określona aplikacja jest uruchomiona, ale pobieranie kończy się niepowodzeniem z powodu błędu lub folder „wynik" zawarty w pobranym archiwum jest pusty, zapoznaj się z bazą wiedzy Kaspersky Security Center.

Uruchamianie zdalnej diagnostyki na urządzeniu klienckim z systemem Linux

Kaspersky Security Center umożliwia pobranie podstawowych informacji diagnostycznych z urządzenia klienckiego. Alternatywnie możesz uzyskać informacje diagnostyczne na temat urządzenia z systemem Linux, korzystając ze skryptu collect.sh firmy Kaspersky. Ten skrypt jest uruchamiany na urządzeniu klienckim z systemem Linux, które wymaga diagnozy, a następnie generuje plik zawierający informacje diagnostyczne, informacje o systemie o tym urządzeniu, pliki śledzenia aplikacji, dzienniki urządzenia i plik zrzutu dla aplikacji zakończonych awaryjnie.

Zalecamy użycie skryptu collect.sh w celu jednoczesnego uzyskania wszystkich informacji diagnostycznych na temat urządzenia klienckiego z systemem Linux. Jeśli pobierasz informacje diagnostyczne zdalnie poprzez Kaspersky Security Center, będziesz musiał przejść przez wszystkie sekcje interfejsu zdalnej diagnostyki. Prawdopodobnie nie zostaną uzyskane w całości informacje diagnostyczne dla urządzenia opartego na systemie Linux.

Jeśli chcesz wysłać wygenerowany plik z informacjami diagnostycznymi do pomocy technicznej Kaspersky, przed wysłaniem pliku usuń wszystkie poufne informacje.

Aby pobrać informacje diagnostyczne z urządzenia klienckiego z systemem Linux za pomocą skryptu collect.sh:

1. Pobierz skryptcollect.sh spakowane w archiwum collect.tar.gz.
2. Skopiuj pobrane archiwum na urządzenie klienckie z systemem Linux, które wymaga diagnozy.
3. Uruchom następujące polecenie, aby rozpakować archiwum collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```
4. Uruchom następujące polecenie, aby określić uprawnienia do wykonywania skryptu:

   ```
   # chmod +x collect.sh
   ```
5. Uruchom skrypt collect.sh, korzystając z konta z uprawnieniami administratora:

   ```
   # ./collect.sh
   ```

Generowany jest plik z informacjami diagnostycznymi, który jest zapisywany w folderze /tmp/$HOST_NAME-collect.tar.gz.

Pobieranie i usuwanie plików z Kwarantanny i Kopia zapasowa

Ta sekcja zawiera informacje na temat pobierania i usuwania plików z Kwarantanny i Kopia zapasowa w Kaspersky Security Center Web Console.

Pobieranie plików z Kwarantanny i Kopii zapasowej

Pliki można pobierać z kwarantanny lub kopii zapasowej tylko wtedy, gdy spełniony jest jeden z dwóch warunków: albo opcja **Nie odłączaj od Serwera administracyjnego** jest włączona w ustawieniach urządzenia lub używana jest brama połączenia. W przeciwnym razie pobieranie nie będzie możliwe.

W celu zapisania kopii pliku z Kwarantanny lub Kopia zapasowa na dysku twardym:

1. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz zapisać kopię pliku z Kwarantanny, w menu głównym przejdź do **Operacje → Repozytoria → Kwarantanna**.

   - Jeśli chcesz zapisać kopię pliku z Kopii zapasowej, w menu głównym przejdź do **Operacje → Repozytoria → Kopia zapasowa**.

2. W otwartym oknie wybierz plik, który chcesz pobrać, i kliknij **Pobierz**.

   Rozpocznie się pobieranie. Kopia pliku, który został umieszczony w Kwarantannie na urządzeniu klienckim, jest zapisywana w określonym folderze.

Zmiana języka interfejsu oprogramowania Kaspersky Security Center Web Console

Możesz wybrać język interfejsu Kaspersky Security Center Web Console.

Aby zmienić język interfejsu:

1. W menu głównym przejdź do sekcji **Ustawienia → Język**.

2. Wybierz jeden z obsługiwanych języków lokalizacji.

Dokumentacja API

Ta Dokumentacja OpenAPI Kaspersky Security Center ma na celu pomóc w następujących zadaniach:

- Automatyzacja i personalizacja. Możesz zautomatyzować zadania, których możesz nie chcieć obsługiwać ręcznie, przy użyciu Konsoli administracyjnej. Możesz także zaimplementować scenariusze niestandardowe, które nie są jeszcze obsługiwane w Konsoli administracyjnej. Na przykład, jako administrator możesz użyć Kaspersky Security Center OpenAPI do tworzenia i uruchamiania skryptów, które ułatwią tworzenie struktury grup administracyjnych i jej aktualizowanie.

- Niestandardowy rozwój. Na przykład, można opracować dla klientów alternatywną Konsolę administracyjną opartą na konsoli MMC, która zezwala na ograniczony zestaw działań.

W przewodniku informacyjnym interfejsu OpenAPI możesz użyć pola wyszukiwania w prawej części ekranu, aby znaleźć potrzebne informacje.

PRZEWODNIK PO OPENAPI

Próbki skryptów

Dokumentacja OpenAPI zawiera przykłady skryptów Pythona wymienionych w poniższej tabeli. Przykłady pokazują, w jaki sposób można wywoływać metody OpenAPI i automatycznie wykonywać różne zadania w celu ochrony sieci, na przykład utworzyć hierarchię "podstawowa/dodatkowa", uruchamiać zadania w Kaspersky Security Center lub przypisywać punkty dystrybucji. Możesz uruchamiać próbki bez zmian lub tworzyć własne skrypty na ich podstawie.

Wywoływanie metody OpenAPI i uruchamianie skryptów:

1. Pobierz archiwum KlAkOAPI.tar.gz. To archiwum zawiera pakiet KlAkOAPI i próbki (możesz je skopiować z archiwum lub z Dokumentacji OpenAPI). Archiwum KlAkOAPI.tar.gz znajduje się również w folderze instalacyjnym Kaspersky Security Center.

2. Zainstaluj pakiet KlakOAPI z archiwum KlAkOAPI.tar.gz na urządzeniu, na którym zainstalowany jest Serwer administracyjny.

   Możesz wywoływać metody OpenAPI, uruchamiać przykłady i własne skrypty tylko na urządzeniach, na których zainstalowany jest Serwer administracyjny i pakiet KlAkOAPI.

Dopasowywanie scenariuszy użytkowników i próbek metod Kaspersky Security Center OpenAPI

Próbka	Cel próbki	Scenariusz
Zarejestruj KlAkParams	Możesz wyodrębniać i przetwarzać dane za pomocą struktury danych `KlAkParams`. Przykład pokazuje, jak pracować z tą strukturą danych. Przykładowe dane wyjściowe mogą być prezentowane na różne sposoby. Możesz uzyskać dane, aby wysłać metodę HTTP lub użyć ich w swoim kodzie.	Monitorowanie i raportowanie
Utwórz i usuń hierarchię "główny/podrzędny"	Możesz dodać podrzędny Serwer administracyjny i utworzyć hierarchię „główny/podrzędny". Alternatywnie, możesz odłączyć podrzędny Serwer administracyjny od hierarchii.	• Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego Serwera administracyjnego • Usuwanie hierarchii Serwerów administracyjnych

Próbka	Cel próbki	Scenariusz
Utwórz hierarchię grup ze strukturą opartą na jednostce Active Directory	Możesz przeszukać jednostkę Active Directory i utworzyć hierarchię wykrytych grup urządzeń.	Tworzenie grup administracyjnych
Utwórz hierarchię grup ze strukturą opartą na buforowanej jednostce Active Directory	Możesz utworzyć hierarchię zarządzanych grup urządzeń w oparciu o wcześniej przeszukiwaną jednostkę Active Directory. Jeśli po ostatnim przeszukiwaniu w Active Directory pojawią się nowe urządzenia, nie zostaną dodane do grupy, ponieważ nie znajdują się w zapisanych wynikach przeszukiwania.	Tworzenie grup administracyjnych
Pobierz pliki listy sieci przez bramę połączenia do określonego urządzenia	Możesz nawiązać połączenie z Agentem sieciowym na żądanym urządzeniu za pomocą bramy połączenia, a następnie pobrać plik z listą sieci na swoje urządzenie.	Dostosowanie punktów dystrybucji i bram połączenia
Zainstaluj klucz licencyjny przechowywany w głównym repozytorium Serwera administracyjnego na podrzędnych Serwerach administracyjnych	Możesz połączyć się z głównym Serwerem administracyjnym, pobrać z niego wymagany klucz licencyjny i przesłać go do wszystkich pomocniczych Serwerów administracyjnych znajdujących się w hierarchii.	Licencjonowanie zarządzanych aplikacji
Utwórz raport obowiązujących uprawnień użytkownika	Możesz utworzyć różne raporty. Na przykład, korzystając z tego przykładu, można wygenerować raport o obowiązujących uprawnieniach użytkownika. Ten raport opisuje uprawnienia, jakie użytkownik posiada, w zależności od jego grupy i roli. Raport można pobrać w formacie HTML, PDF lub Excel.	Generowanie i przeglądanie raportu
Rozpocznij zadanie dla urządzenia	Możesz nawiązać połączenie z Agentem sieciowym na żądanym urządzeniu za pomocą bramy połączenia, a następnie pobrać żądane zadanie.	Ręczne uruchamianie zadania
Utwórz podsieci IP w oparciu o witrynę i usługi Active Directory	Podsieć IP można utworzyć na podstawie używanej jednostki Active Directory. Przykład uruchamia przeszukiwanie określonego zakresu adresów IP i usuwa wykryte podsieci, aby uniknąć ich konfliktu z nową podsiecią. Dlatego nie uruchamiaj tego przykładu w sieci, w której ważne jest zapisanie podsieci. Po przeszukaniu próbka odwołuje się do Active Directory, sprawdza każde znajdujące się w nim urządzenie i tworzy podsieć IP. W tym celu próbka używa masek i adresów IP wszystkich urządzeń.	Konfigurowanie ochrony sieci
Zarejestruj punkty dystrybucji dla urządzeń w grupie	Zarządzane urządzenia można przypisać jako punkty dystrybucji (wcześniej nazywane agentami aktualizacji).	Aktualizowanie baz danych i aplikacji Kaspersky
Wylicz wszystkie grupy	Na grupach administracyjnych możesz wykonać różne akcje. Przykład pokazuje, jak wykonać następujące czynności: • Uzyskaj identyfikator grupy głównej „Zarządzane urządzenia” • Poruszaj się po hierarchii grupy • Pobierz pełną, rozszerzoną hierarchię grup wraz z ich nazwami i zagnieżdżeniem	Konfigurowanie Serwera administracyjnego
Wylicz zadania, przeszukaj statystyki zadań i uruchom zadanie	Możesz znaleźć następujące informacje: • Historia postępu zadania • Aktualny stan zadania • Liczba zadań z różnymi stanami Możesz także uruchomić zadanie. Domyślnie próbka uruchamia zadanie po wygenerowaniu statystyk.	Monitorowanie wykonywania zadania
Utwórz i uruchom zadanie	Możesz utworzyć zadanie. W przykładzie określ następujące parametry zadania: • Typ • Metoda uruchamiania • Nazwa • Grupa urządzeń, dla której będzie używane zadanie Domyślnie, przykład tworzy zadanie typu „Pokaż wiadomość”. Możesz uruchomić to zadanie dla wszystkich zarządzanych urządzeń Serwera administracyjnego. W razie potrzeby możesz określić własne parametry zadania.	Tworzenie zadania

Próbka	Cel próbki	Scenariusz
Wylicz klucze licencyjne	Możesz uzyskać listę wszystkich aktywnych kluczy licencyjnych dla aplikacji Kaspersky zainstalowanych na zarządzanych urządzeniach Serwera administracyjnego. Lista zawiera szczegółowe dane o każdym kluczu licencyjnym, takim jak nazwa, typ lub data wygaśnięcia.	Wyświetlanie informacji o używanych kluczach licencyjnych
Utwórz i znajdź użytkownika wewnętrznego	Możesz utworzyć konto do dalszej pracy.	Wybieranie konta do uruchamiania Serwera administracyjnego
Utwórz kategorię niestandardową	Możesz utworzyć kategorię aplikacji z potrzebnymi parametrami.	Tworzenie kategorii aplikacji z zawartością dodaną ręcznie
Wylicz użytkowników przy użyciu SrvView	Możesz użyć klasy SrvView, aby zażądać szczegółowych informacji z serwera administracyjnego. Na przykład, możesz uzyskać listę użytkowników, korzystając z tego przykładu.	Zarządzanie kontami użytkowników

Aplikacje współpracujące z Kaspersky Security Center poprzez interfejs OpenAPI

Niektóre aplikacje współpracują z Kaspersky Security Center poprzez interfejs OpenAPI. Do takich aplikacji należą na przykład Kaspersky Anti Targeted Attack Platform lub Kaspersky Security for Virtualization. Może to być również niestandardowa aplikacja kliencka utworzona przez Ciebie w oparciu o OpenAPI.

Aplikacje współpracujące z Kaspersky Security Center poprzez interfejs OpenAPI łączą się z serwerem administracyjnym. Jeżeli skonfigurowano listę zezwolonych adresów IP do łączenia się z serwerem administracyjnym, dodaj adresy IP urządzeń, na których zainstalowane są aplikacje korzystające z Kaspersky Security Center OpenAPI. Aby dowiedzieć się, czy aplikacja, z której korzystasz, działa z interfejsem OpenAPI, zapoznaj się z sekcją pomocy dla tej aplikacji.

Praktyczne zastosowanie aplikacji dla dostawców usługi

Niniejsza sekcja zawiera informacje dotyczące konfiguracji i korzystania z Kaspersky Security Center.

Ta sekcja zawiera zalecenia dotyczące instalacji, konfiguracji i korzystania z aplikacji, a także opisuje sposoby rozwiązywania typowych problemów występujących podczas działania aplikacji.

Planowanie instalacji Kaspersky Security Center

Podczas planowania instalacji komponentów Kaspersky Security Center w sieci organizacji należy uwzględnić rozmiar i obszar projektu, a zwłaszcza poniższe czynniki:

- Całkowitą liczbę urządzeń
- Liczbę klientów MSP

Jeden Serwer administracyjny może obsługiwać maksymalnie 100 000 urządzeń. Jeśli całkowita liczba urządzeń w sieci organizacji przekroczy 100 000, wówczas po stronie dostawcy usługi należy zainstalować kilka Serwerów administracyjnych i połączyć je w hierarchię w celu uproszczenia scentralizowanego zarządzania.

Na jednym Serwerze administracyjnym można utworzyć do 500 serwerów wirtualnych, czyli dla każdej grupy 500 klientów MSP potrzebny jest jeden Serwer administracyjny.

Na etapie planowania wdrożenia należy rozważyć przydzielenie do Serwera administracyjnego specjalnego certyfikatu X.509. Przydzielenie certyfikatu X.509 do Serwera administracyjnego może być przydatne między innymi do:

- Sprawdzania ruchu SSL poprzez kończenie żądań SSL na serwerze proxy
- Określenia wymaganych wartości w polach certyfikatu
- Zapewnienia wymaganej siły szyfrowania certyfikatu

Umożliwianie uzyskania dostępu do Serwera administracyjnego przez Internet

Aby zezwolić urządzeniom w sieci klienckiej na dostęp do Serwera administracyjnego poprzez internet, należy udostępnić następujące porty Serwera administracyjnego:

- 13000 TCP — port TLS Serwera administracyjnego do podłączania Agentów sieciowych zainstalowanych w sieci klienckiej
- 8061 TCP — port HTTPS do publikowania pakietów autonomicznych przy użyciu narzędzi Konsoli administracyjnej

- 8060 TCP — port HTTP do publikowania pakietów autonomicznych przy użyciu narzędzi Konsoli administracyjnej
- 13292 TCP — port TLS wymagany tylko tam, gdzie konieczne jest zarządzanie urządzeniami mobilnymi

Jeśli potrzebujesz zapewnić klientom podstawowe opcje zarządzania siecią poprzez Kaspersky Security Center Web Console, należy także otworzyć port 8080 TCP (port HTTPS) Kaspersky Security Center Web Console.

Standardowa konfiguracja Kaspersky Security Center

Jeden lub kilka Serwerów administracyjnych jest instalowanych na serwerach MSP. Liczba Serwerów administracyjnych może zostać wybrana w oparciu o dostępny sprzęt, całkowitą liczbę obsługiwanych klientów MSP lub całkowitą liczbę zarządzanych urządzeń.

Jeden Serwer administracyjny może obsługiwać maksymalnie 100 000 urządzeń. Należy rozważyć możliwość zwiększenia liczby zarządzanych urządzeń w najbliższej przyszłości: wygodniejsze może być podłączenie do jednego Serwera administracyjnego mniejszej liczby urządzeń.

Na jednym Serwerze administracyjnym można utworzyć do 500 serwerów wirtualnych, czyli dla każdej grupy 500 klientów MSP potrzebny jest jeden Serwer administracyjny.

Jeśli jest używanych kilka Serwerów, zalecane jest połączenie ich w hierarchię. Korzystanie z hierarchii Serwerów administracyjnych pozwala uniknąć mieszania zasad i zadań, zarządzać całym zbiorem zarządzanych urządzeń tak, jak by były zarządzane przez jeden Serwer administracyjny, czyli wyszukiwać urządzenia, tworzyć wybory urządzeń oraz generować raporty.

Na każdym serwerze wirtualnym, który odpowiada klientowi MSP, należy wskazać jeden lub kilka punktów dystrybucji. Jeśli klienci MSP i Serwer administracyjny są połączone przez Internet, przydatne może być utworzenie zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla punktów dystrybucji, aby mogły one pobierać uaktualnienia bezpośrednio z serwerów Kaspersky, a nie z Serwera administracyjnego.

Jeśli niektóre urządzenia w sieci klienckiej MSP nie mają bezpośredniego dostępu do Internetu, należy przełączyć punkty dystrybucji do trybu bramy połączenia. W tym przypadku Agenty sieciowe na urządzeniach w sieci klienckiej MSP zostaną połączone, w celu dalszej synchronizacji, z Serwerem administracyjnym, ale poprzez bramę, a nie bezpośrednio.

Ponieważ Serwer administracyjny najprawdopodobniej nie będzie mógł przeszukać sieci klienckiej MSP, zalecane jest przekazanie tej funkcji punktowi dystrybucji.

Serwer administracyjny nie będzie mógł wysyłać powiadomień poprzez port UDP o numerze 15000 na zarządzane urządzenia znajdujące się poza NAT w sieci klienckiej MSP. Aby rozwiązać ten problem, we właściwościach urządzeń pełniących rolę punktów dystrybucji i działających w trybie bramy połączenia należy włączyć tryb stałego połączenia z Serwerem administracyjnym (pole **Nie odłączaj od Serwera administracyjnego**). Tryb stałego połączenia jest dostępny, jeśli całkowita liczba punktów dystrybucji nie przekracza 300.

Informacje o punktach dystrybucji

Urządzenie z zainstalowanym Agentem sieciowym mogą być używane jako punkt dystrybucji. W tym trybie Agent sieciowy może wykonywać następujące funkcje:

- Przesyłać pliki na urządzenia klienckie, w tym:
  - Aktualizacje baz danych i modułów oprogramowania Kaspersky

    Uaktualnienia mogą być pobierane z Serwera administracyjnego lub z serwerów Kaspersky. W drugim przypadku należy utworzyć zadanie *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla urządzenia pełniącego rolę punktu dystrybucji.
  - Instalowanie aktualizacji oprogramowania firm trzecich
  - Pakiety instalacyjne
  - Aktualizacje systemu Windows w przypadku używania Serwera administracyjnego jako serwera WSUS
- Instalować oprogramowanie (włączając w to wstępną instalację Agentów sieciowych) na pozostałych urządzeniach.
- Przeszukiwać sieć w celu odnalezienia nowych urządzeń i zaktualizowania informacji o tych istniejących. Punkt dystrybucji może stosować te same metody wykrywania urządzeń co Serwer administracyjny.

Instalacja punktów dystrybucji w sieci organizacji realizuje następujące cele:

- Zmniejsza obciążenie na Serwerze administracyjnym, jeśli działa jako źródło uaktualnień.
- Optymalizuje ruch internetowy, ponieważ, w tym przypadku, każde urządzenie w sieci klienckiej MSP nie musi uzyskać dostępu do serwerów Kaspersky lub Serwera administracyjnego w celu pobrania uaktualnień.
- Zapewnia Serwerowi administracyjnemu dostęp do urządzeń poza NAT (względem Serwera administracyjnego) sieci klienckiej MSP, co umożliwia Serwerowi administracyjnemu wykonanie następujących działań:
  - Wysyłanie powiadomień do urządzeń przez UDP w sieci IPv4 lub IPv6
  - Przeszukiwanie sieci IPv4 lub IPv6
  - Przeprowadzanie wstępnego wdrożenia
  - Pełnienie funkcji serwera push

Punkt dystrybucji jest przydzielony do grupy administracyjnej. W tym przypadku zakres działania punktu dystrybucji obejmuje wszystkie urządzenia w grupie administracyjnej i jej podgrupach. Jednakże urządzenie pełniące funkcję punktu dystrybucji nie musi znajdować się w grupie administracyjnej, do której zostało przydzielone.

Możesz sprawić, że punkt dystrybucji będzie działał jako brama połączenia. W tym przypadku urządzenia objęte zakresem działania tego punktu dystrybucji będą łączyły się z Serwerem administracyjnym poprzez bramę, a nie bezpośrednio. Możesz użyć tego trybu w scenariuszach, które nie zezwalają na nawiązywanie bezpośredniego połączenia między urządzeniami a Agentem sieciowym i Serwerem administracyjnym.

Urządzenia pełniące rolę punktów dystrybucji muszą być chronione, włączając w to ochronę fizyczną, przed wszelkim nieautoryzowanym dostępem.

Hierarchia Serwerów administracyjnych

W MSP może działać kilka Serwerów administracyjnych. Niewygodne może być zarządzanie kilkoma oddzielnymi Serwerami administracyjnymi, dlatego dobrym wyjściem jest utworzenie hierarchii. Zastosowanie konfiguracji „główny/podrzędny" dla dwóch Serwerów administracyjnych oferuje następujące możliwości:

- Podrzędny Serwer administracyjny dziedziczy zasady i zadania od głównego Serwera administracyjnego, zapobiegając dzięki temu powielaniu ustawień.
- Wybory urządzeń na głównym Serwerze administracyjnym mogą zawierać urządzenia z podrzędnych Serwerów administracyjnych.
- Raporty na głównym Serwerze administracyjnym mogą zawierać dane (w tym szczegółowe informacje) z podrzędnych Serwerów administracyjnych.

W zakresie wyżej wymienionych opcji główny Serwer administracyjny odbiera dane tylko z niewirtualnych podrzędnych Serwerów administracyjnych. To ograniczenie nie dotyczy wirtualnych Serwerów administracyjnych, które współdzielą bazę danych ze swoim głównym Serwerem administracyjnym.

Wirtualne Serwery administracyjne

W oparciu o fizyczny Serwer administracyjny można utworzyć kilka wirtualnych Serwerów administracyjnych, które będą podobne do podrzędnych Serwerów administracyjnych. W przeciwieństwie do trybu poufnego dostępu, który jest oparty na listach kontroli dostępu (ACL), tryb wirtualnego Serwera administracyjnego jest bardziej funkcjonalny i zapewnia większy stopień izolacji. Jako dodatek do dedykowanej struktury grup administracyjnych dla przypisanych urządzeń z zasadami i zadaniami, każdy wirtualny Serwer administracyjny zawiera swoją grupę nieprzypisanych urządzeń, własne zestawy raportów, wybranych urządzeń i zdarzeń, pakietów instalacyjnych, reguł przenoszenia itd. Dla maksymalnej wspólnej izolacji klientów MSP zalecane jest wybranie wirtualnych Serwerów administracyjnych jako funkcjonalności, która ma zostać użyta. Dodatkowo, utworzenie wirtualnego Serwera administracyjnego dla każdego klienta MSP umożliwia zapewnienie klientom podstawowych opcji zarządzania siecią za pośrednictwem Kaspersky Security Center Web Console.

Wirtualne Serwery administracyjne są bardzo podobne do podrzędnych Serwerów administracyjnych, jednakże posiadają pewne różnice:

- Wirtualny Serwer administracyjny nie posiada większości ustawień globalnych i swoich własnych portów TCP.
- Wirtualny Serwer administracyjny nie posiada podrzędnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny nie posiada innych wirtualnych Serwerów administracyjnych.
- Fizyczny Serwer administracyjny wyświetla urządzenia, grupy, zdarzenia i obiekty na zarządzanych urządzeniach (elementy w Kwarantannie, rejestrze aplikacji itd.) ze wszystkich swoich wirtualnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny może skanować sieć wyłącznie przy podłączonych punktach dystrybucji.

Zarządzanie urządzeniami mobilnymi z zainstalowanym programem Kaspersky Endpoint Security for Android

Urządzenia mobilne z zainstalowanym programem Kaspersky Endpoint Security for Android™ (zwane dalej "urządzenia KES") są zarządzane przy użyciu Serwera administracyjnego. Kaspersky Security Center obsługuje następujące funkcje zarządzania urządzeniami KES:

- Zarządzanie urządzeniami mobilnymi jak urządzeniami klienckimi:
  - Członkostwo w grupach administracyjnych
  - Monitorowanie, takie jak przeglądanie stanów, zdarzeń i raportów
  - Modyfikowanie ustawień lokalnych i przydzielanie zasad dla Kaspersky Endpoint Security for Android
- Wysyłanie poleceń w sposób scentralizowany
- Zdalne instalowanie pakietów aplikacji mobilnych

Serwer administracyjny zarządza urządzeniami KES przez TLS, port TCP 13292.

Instalacja i wstępna konfiguracja

Kaspersky Security Center jest aplikacją oferującą wiele funkcji. Kaspersky Security Center zawiera następujące komponenty:

- Serwer administracyjny—główny komponent, zaprojektowany do zarządzania urządzeniami w organizacji i przechowywania danych w DBMS.
- Konsola administracyjna—podstawowe narzędzie administratora. Konsola administracyjna jest dostarczana wraz z Serwerem administracyjnym, ale można ją także zainstalować oddzielnie na jednym lub kilku urządzeniach administratora.
- Kaspersky Security Center Web Console to interfejs sieciowy dla Serwera administracyjnego, zaprojektowany do wykonywania podstawowych działań. Możesz zainstalować ten komponent na dowolnym urządzeniu, które spełnia wymagania sprzętowe i programowe.
- Agent sieciowy — zaprojektowany do zarządzania aplikacją zabezpieczającą, zainstalowaną na urządzeniu, a także do zbierania informacji o tym urządzeniu. Agenty sieciowe są instalowane na urządzeniach w organizacji.

Instalacja Kaspersky Security Center w sieci organizacji odbywa się w następujący sposób:

- Instalacja Serwera administracyjnego
- Instalacja Kaspersky Security Center Web Console
- Instalacja Konsoli administracyjnej na urządzeniu administratora
- Instalacja Agenta sieciowego i aplikacji zabezpieczającej na urządzeniach w firmie

Zalecenia dotyczące instalacji Serwera administracyjnego

Ta sekcja zawiera zalecenia dotyczące instalacji Serwera administracyjnego. Opisane są tu także scenariusze korzystania z folderu współdzielonego na urządzeniu z Serwerem administracyjnym w celu zainstalowania Agenta sieciowego na urządzeniach klienckich.

Tworzenie kont dla usług Serwera administracyjnego na klastrze typu failover

Domyślnie instalator automatycznie tworzy konta bez uprawnień dla usług Serwera administracyjnego. To zachowanie jest najwygodniejsze w przypadku instalacji Serwera administracyjnego na zwykłym urządzeniu.

Jednakże instalacja Serwera administracyjnego na klastrze typu failover wymaga innego scenariusza:

1. Dla usług Serwera administracyjnego utwórz konta domenowe bez uprawnień i przydziel je do globalnej grupy zabezpieczeń w domenie o nazwie KLAdmins.

2. W instalatorze Serwera administracyjnego określ konta domenowe, które zostały utworzone dla usług.

Wybieranie systemu zarządzania bazą danych

Podczas wybierania systemu zarządzania bazą danych (DBMS), który zostanie użyty przez Serwer administracyjny, należy brać pod uwagę liczbę urządzeń podlegających Serwerowi administracyjnemu.

Poniższa tabela zawiera listę prawidłowych opcji DBMS, a także zalecenia i ograniczenia dotyczące ich używania.

Zalecenia i ograniczenia dotyczące DBMS

DBMS	Zalecenia i ograniczenia
SQL Server Express Edition 2016 lub nowszy	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 10 000 urządzeń. Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasady Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach. Można ograniczyć maksymalną liczbę zdarzeń w repozytorium zdarzeń, aby zapobiec przepełnieniu bazy danych. Szczegółowe informacje można znaleźć w następującym temacie: Obliczanie miejsca na bazę danych. Jednoczesne korzystanie z systemu DBMS serwera SQL Server Express Edition przez Serwer administracyjny i inną aplikację jest surowo zabronione. Baza danych Microsoft SQL Express nie jest obsługiwana dla zadania **Wykonaj synchronizację Windows Update**.
Lokalny serwer SQL Server inny niż Express, 2016 lub nowszy	Brak ograniczeń.
Zdalny serwer SQL Server inny niż Express, 2016 lub nowszy	Ważne tylko wtedy, gdy oba urządzenia są w tej samej domenie Windows®; jeśli domeny są inne, należy nawiązać między nimi obustronną relację zaufania.
Lokalny lub zdalny MySQL 5.5, 5.6 lub 5.7 (MySQL w wersjach 5.5.1, 5.5.2, 5.5.3, 5.5.4 i 5.5.5 nie jest już obsługiwany)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 10 000 urządzeń. Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasady Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach. Szczegółowe informacje można znaleźć w następującym temacie: Obliczanie miejsca na bazę danych.

DBMS	Zalecenia i ograniczenia
Lokalny lub zdalny MySQL 8.0.20 lub nowszy	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 50 000 urządzeń. Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasady Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach. Szczegółowe informacje można znaleźć w następującym temacie: Obliczanie miejsca na bazę danych.
Lokalny lub zdalny MariaDB (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny dla mniej niż 20 000 urządzeń. Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasady Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach. Szczegółowe informacje można znaleźć w następującym temacie: Obliczanie miejsca na bazę danych.
PostgreSQL, Postgres Pro (zobacz obsługiwane wersje)	Użyj jednego z tych DBMS, jeśli zamierzasz uruchomić jeden Serwer administracyjny dla mniej niż 50 000 urządzeń. Zaleca się wyłączenie zadania Inwentaryzacja oprogramowania i wyłączenie (w ustawieniach zasady Kaspersky Endpoint Security) powiadomień Serwera administracyjnego o uruchomionych aplikacjach. Szczegółowe informacje można znaleźć w następującym temacie: Obliczanie miejsca na bazę danych.

Jeśli wybierzesz MSSQL 2019, musisz użyć zbiorczej poprawki CU12 lub nowszej. Pozwoli to uniknąć błędów i przeciążenia systemu, które mogą wystąpić.

Jeśli używasz systemu PostgreSQL, MariaDB lub MySQL DBMS, karta **Zdarzenia** może wyświetlać niekompletną listę zdarzeń dla wybranego urządzenia klienckiego. Dzieje się tak, gdy system DBMS przechowuje bardzo dużą liczbę zdarzeń. Liczbę wyświetlanych zdarzeń można zwiększyć, wykonując jedną z następujących czynności:

- Usuwanie niepotrzebnych zdarzeń.
- Skrócenie okresu przechowywania niepotrzebnych zdarzeń.

Aby zobaczyć pełną listę zdarzeń zarejestrowanych na Serwerze administracyjnym dla danego urządzenia, należy użyć opcji Raporty.

Określanie adresu Serwera administracyjnego

Podczas instalacji Serwera administracyjnego należy określić zewnętrzny adres Serwera administracyjnego. Podczas tworzenia pakietów instalacyjnych Agenta sieciowego ten adres będzie używany jako domyślny. Wówczas możliwa będzie zmiana adresu komputera z Serwerem administracyjnym przy użyciu narzędzi Konsoli administracyjnej; adres nie zostanie zmieniony automatycznie w już utworzonych pakietach instalacyjnych Agenta sieciowego.

Konfigurowanie ochrony w sieci organizacji klienta

Po zakończeniu instalacji Serwera administracyjnego, zostaje uruchomiona Konsola administracyjna, która oferuje przeprowadzenie wstępnej konfiguracji przy użyciu odpowiedniego kreatora. Jeśli kreator wstępnej konfiguracji jest uruchomiony, w głównej grupie administracyjnej tworzone są następujące zasady i zadania:

- Zasada Kaspersky Endpoint Security
- Grupowe zadanie aktualizacji Kaspersky Endpoint Security

- Grupowe zadanie skanowania urządzenia z zainstalowanym programem Kaspersky Endpoint Security
- Zasada Agenta sieciowego
- Zadanie wykrywania luk (zadanie Agenta sieciowego)
- Zadanie instalacji uaktualnień i naprawy luk (zadanie Agenta sieciowego)

Zasady i zadania są tworzone z domyślnymi ustawieniami, które mogą okazać się nieoptymalne lub nawet niedopuszczalne dla organizacji. Dlatego też należy sprawdzić właściwości utworzonych obiektów i zmodyfikować je ręcznie (jeśli zajdzie taka konieczność).

Ta sekcja zawiera informacje dotyczące ręcznej konfiguracji zasad, zadań i innych ustawień Serwera administracyjnego, a także informacje o punkcie dystrybucji, tworzeniu struktury grup administracyjnych i hierarchii zadań oraz innych ustawień.

Ręczna konfiguracja zasady Kaspersky Endpoint Security

W tej sekcji można znaleźć zalecenia dotyczące konfiguracji zasady Kaspersky Endpoint Security, który jest tworzony przez Kreator wstępnej konfiguracji. Możesz przeprowadzić konfigurację w oknie właściwości zasady.

Podczas modyfikowania ustawień należy pamiętać o kliknięciu ikony blokady nad odpowiednim ustawieniem, aby umożliwić jego użycie na stacji roboczej.

Konfigurowanie zasady w sekcji Zaawansowana ochrona przed zagrożeniami

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Zaawansowana ochrona przed zagrożeniami** możesz skonfigurować używanie Kaspersky Security Network dla Kaspersky Endpoint Security for Windows. Możesz także skonfigurować moduły Kaspersky Endpoint Security for Windows, takie jak Wykrywanie zachowań, Ochrona przed exploitami, Ochrona przed włamaniami oraz Silnik korygujący.

W podsekcji **Kaspersky Security Network** zalecane jest włączenie opcji **Kaspersky Security Network**. Użyj tej opcji do redystrybucji i optymalizacji ruchu w sieci. Jeśli opcja **Kaspersky Security Network** jest wyłączona, możesz włączyć bezpośrednie korzystanie z serwerów KSN.

Konfigurowanie zasady w sekcji Podstawowa ochrona przed zagrożeniami

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Podstawowa ochrona przed zagrożeniami** okna właściwości zasad, zalecamy określenie dodatkowych ustawień w podsekcjach **Zapora sieciowa** i **Ochrona plików**.

Podsekcja **Zapora sieciowa** zawiera ustawienia, które pozwalają kontrolować aktywność sieciową aplikacji na urządzeniach klienckich. Urządzenie klienckie korzysta z sieci, do której przypisany jest jeden z następujących statusów: publiczny, lokalny lub zaufany. W zależności od stanu sieci, Kaspersky Endpoint Security może zezwolić na aktywność sieciową na urządzeniu lub jej zabronić. Gdy dodajesz nową sieć do swojej organizacji, musisz przypisać jej odpowiedni status sieci. Na przykład, jeśli urządzeniem klienckim jest laptop, zalecamy, aby to urządzenie korzystało z sieci publicznej lub zaufanej, ponieważ laptop nie zawsze jest podłączony do sieci lokalnej. W podsekcji **Zapora sieciowa** możesz sprawdzić, czy prawidłowo przypisano stany do sieci używanych w Twojej organizacji.

W celu sprawdzenia listy sieci:

1. We właściwościach zasady przejdź do **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa**.
2. W sekcji **Dostępne sieci** kliknij przycisk **Ustawienia**.
3. W **Zapora sieciowa**, które zostanie otwarte, przejdź do zakładki **Sieci**, aby wyświetlić listę sieci.

W podsekcji **Ochrona plików** możesz wyłączyć skanowanie dysków sieciowych. Skanowanie dysków sieciowych może spowodować znaczne obciążenie dysków sieciowych. Praktyczniejsze jest wykonywanie bezpośredniego skanowania na serwerach plików.

W celu wyłączenia skanowania dysków sieciowych:

1. We właściwościach zasady przejdź do **Podstawowa ochrona przed zagrożeniami → Ochrona plików**.
2. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
3. W otwartym oknie **Ochrona plików**, na zakładce **Ogólne** odznacz pole **Wszystkie dyski sieciowe**.

Konfigurowanie zasady w sekcji Ustawienia ogólne

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security.

Poniżej opisano zaawansowane działania, które zalecamy wykonać w oknie właściwości zasady programu Kaspersky Endpoint Security w sekcji **Ustawienia ogólne**.

Sekcja Ustawienia ogólne, podsekcja Raporty i pliki danych

W sekcji **Transfer danych do Serwera administracyjnego** zaznacz pole **Informacje o uruchomionych aplikacjach**. Jeśli to pole jest zaznaczone, bazy danych Serwera administracyjnego zapisują informacje o wszystkich wersjach wszystkich modułów oprogramowania na urządzeniach w sieci. Informacje mogą wymagać znaczącej ilości miejsca na dysku dla bazy danych Kaspersky Security Center (kilkadziesiąt gigabajtów). Dlatego, jeśli pole **Informacje o uruchomionych aplikacjach** jest cały czas zaznaczone w zasadzie o najwyższym poziomie, musi ono zostać odznaczone.

Sekcja Ustawienia ogólne, podsekcja Interfejs

Jeśli ochrona antywirusowa w sieci organizacji musi być zarządzana w sposób scentralizowany poprzez Konsolę administracyjną, musisz wyłączyć wyświetlanie interfejsu Kaspersky Endpoint Security na stacjach roboczych (odznaczając pole **Wyświetl interfejs aplikacji** w sekcji **Interakcja z użytkownikiem**) oraz włączyć na nich ochronę hasłem (zaznaczając pole **Włącz ochronę hasłem** w sekcji **Ochrona hasłem**).

Konfigurowanie zasad w sekcji Konfiguracja zdarzenia

W sekcji **Konfiguracja zdarzenia** należy wyłączyć zapisywanie wszystkich zdarzeń na Serwerze administracyjnym, za wyjątkiem następujących:

- Na zakładce **Krytyczny**:
  - *Automatyczne uruchamianie aplikacji jest wyłączone*
  - *Dostęp zabroniony*
  - *Zabroniono uruchomienia aplikacji*
  - *Leczenie nie jest możliwe*
  - *Naruszenie umowy licencyjnej użytkownika końcowego*
  - *Nie można wczytać modułu szyfrującego*
  - *Nie można uruchomić dwóch zadań w tym samym czasie*
  - *Wykryto aktywne zagrożenie. Należy uruchomić zaawansowane leczenie*
  - *Wykryto atak sieciowy*
  - *Nie wszystkie składniki zostały zaktualizowane*
  - *Błąd aktywacji*
  - *Błąd podczas włączania trybu przenośnego*
  - *Błąd współdziałania z Kaspersky Security Center*
  - *Błąd podczas wyłączania trybu przenośnego*
  - *Błąd podczas zmiany składników aplikacji*
  - *Błąd podczas stosowania reguł szyfrowania/odszyfrowywania pliku*
  - *Zasada nie może zostać zastosowana*
  - *Działanie procesu zostało zakończone*
  - *Aktywność sieciowa jest zablokowana*
- Na zakładce **Błąd funkcjonalny**: *Nieprawidłowe ustawienia zadania. Ustawienia nie zostały zastosowane*

- Na karcie **Ostrzeżenie**:
  - *Autoochrona jest wyłączona*
  - *Nieprawidłowy klucz zapasowy*
  - *Użytkownik zrezygnował z zasady szyfrowania*
- Na karcie **Informacja**: *Zabroniono uruchomienia aplikacji w trybie testowym*

Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security

Jeśli Serwer administracyjny pełni rolę źródła uaktualnień, optymalną i zalecaną opcją terminarza dla Kaspersky Endpoint Security jest **Po pobraniu nowych uaktualnień do repozytorium**, gdy zaznaczone jest pole **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Jeśli lokalne zadanie pobierania uaktualnień z serwerów Kaspersky do repozytorium jest tworzone na każdym punkcie dystrybucji, okresowe planowanie będzie optymalne i zalecane dla grupowego zadania aktualizacji Kaspersky Endpoint Security. W tym przypadku, dla przedziału randomizacji należy wybrać wartość - 1 godzina.

Ręczna konfiguracja grupowego zadania skanowania urządzeń z zainstalowanym programem Kaspersky Endpoint Security

Kreator wstępnej konfiguracji tworzy grupowe zadanie skanowania urządzeń. Domyślnie skonfigurowano terminarz **uruchamiania zadania w piątki o godzinie 19:00** z automatyczną randomizacją i odznaczonym polem **Uruchom pominięte zadania**.

Oznacza to, że jeśli urządzenia w organizacji są wyłączone w piątki, na przykład o godzinie 18:30, zadanie skanowania urządzeń nigdy nie zostanie uruchomione. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego zadanie *Wyszukiwanie luk i wymaganych aktualizacji.* Domyślnie skonfigurowano terminarz **uruchamiania zadania we wtorki o godzinie 19:00** z automatyczną randomizacją i zaznaczonym polem **Uruchom pominięte zadania**.

Jeśli zasady obowiązujące w organizacji nakazują wyłączenie wszystkich urządzeń w tym czasie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* zostanie uruchomione, gdy urządzenia znowu zostaną włączone, czyli w środę rano. Takie działanie nie jest wskazane, ponieważ wykrywanie luk może zwiększać zużycie procesora i obciążenie podsystemów dysku. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Ręczna konfiguracja grupowego zadania instalacji uaktualnień i naprawy luk

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego grupowe zadanie instalacji uaktualnień i naprawy luk. Domyślnie skonfigurowano terminarz uruchamiania zadania codziennie o godzinie 01:00 z automatyczną randomizacją i wyłączoną opcją **Uruchom pominięte zadania**.

Jeśli reguły obowiązujące w organizacji nakazują wyłączanie urządzeń na noc, zadanie instalacji uaktualnień nigdy nie zostanie uruchomione. Terminarz dla zadania wykrywania luk należy skonfigurować w oparciu o zasady obowiązujące w organizacji. Należy pamiętać, że zadanie instalacji uaktualnień może wymagać ponownego uruchomienia urządzenia.

Tworzenie struktury grup administracyjnych i przydzielanie punktów dystrybucji

Struktura grup administracyjnych w Kaspersky Security Center pełni następujące funkcje:

- Tworzy zakres zasad.

  Istnieje alternatywny sposób stosowania odpowiednich ustawień na urządzeniach przy użyciu profili zasad. W tym przypadku zakres zasad jest tworzony, na przykład, ze znacznikami, lokalizacjami urządzeń w jednostkach organizacyjnych Active Directory, członkostwem w grupach zabezpieczeń Active Directory.

- Tworzy zakres zadań grupowych.

  Istnieje sposób określania zakresu zadań grupowych, który nie jest oparty na hierarchii grup administracyjnych: korzystanie z zadań dla wyboru urządzeń oraz z zadań dla określonych urządzeń.

- Nadaje urządzeniom, wirtualnym Serwerom administracyjnym oraz podrzędnym Serwerom administracyjnym prawa dostępu.

- Przypisuje punkty dystrybucji.

Podczas tworzenia struktury grup administracyjnych należy wziąć pod uwagę topologię sieci organizacji dla optymalnego przydzielenia punktów dystrybucji. Optymalne przydzielenie punktów dystrybucji pozwala na zmniejszenie ruchu w sieci organizacji.

W zależności od schematu organizacyjnego oraz topologii sieci zaadaptowanej przez klienta MSP, w strukturze grup administracyjnych można zastosować następujące standardowe konfiguracje:

- Jedno biuro

- Wiele małych, oddzielonych od siebie biur

Standardowa konfiguracja klienta MSP: Jedno biuro

W standardowej konfiguracji „jedno biuro” wszystkie urządzenia znajdują się w obrębie sieci organizacji i są dla siebie widoczne. Sieć organizacji może zawierać kilka oddzielnych części (sieci lub fragmentów sieci) połączonych ze sobą wąskimi kanałami.

Dostępne są następujące metody tworzenia struktury grup administracyjnych:

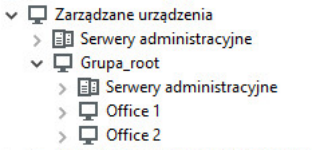
- Tworzenie struktury grup administracyjnych z uwzględnieniem topologii sieci. Struktura grup administracyjnych nie musi odzwierciedlać topologii sieci z absolutną dokładnością. Wystarczy dopasowanie oddzielnych części sieci i pewnych grup administracyjnych. Możesz skorzystać z automatycznego przydzielenia punktów dystrybucji lub zrobić to ręcznie.

- Tworzenie struktury grup administracyjnych bez uwzględnienia topologii sieci. W tym przypadku należy wyłączyć automatyczne przydzielanie punktów dystrybucji, a następnie wskazać jedno lub kilka urządzeń jako punkty dystrybucji dla głównej grupy administracyjnej w każdej z oddzielnych części sieci, na przykład dla grupy **Zarządzane urządzenia**. Wszystkie punkty dystrybucji będą na tym samym poziomie i będą obejmować ten sam obszar, uwzględniając wszystkie urządzenia w sieci organizacji. W takim przypadku każdy z Agentów sieciowych połączy się z punktem dystrybucji o najkrótszej trasie. Trasę do punktu dystrybucji można ustalić za pomocą narzędzia tracert.

Standardowa konfiguracja klienta MSP: Wiele małych, zdalnych biur

Ta standardowa konfiguracja została utworzona z myślą o małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem Internetu. Każde zdalne biuro znajduje się poza NAT, czyli połączenie jednego zdalnego biura z innym jest niemożliwe, gdyż biura są od siebie odizolowane.

Konfiguracja musi być odzwierciedlona w strukturze grup administracyjnych: dla każdego zdalnego biura musi zostać utworzona oddzielna grupa administracyjna (grupy **Office 1** i **Office 2** na rysunku poniżej).



Zdalne biura uwzględnione w strukturze grupy administracyjnej

Do każdej grupy administracyjnej odpowiadającej biuru należy przydzielić jeden lub kilka punktów dystrybucji. Punktami dystrybucji muszą być urządzenia w zdalnym biurze, które posiadają wystarczającą ilość wolnego miejsca na dysku. Urządzenia z grupy **Office 1** będą, na przykład, łączyć się z punktami dystrybucji przydzielonymi do grupy administracyjnej **Office 1**.

Jeśli niektórzy użytkownicy poruszają się między biurami ze swoimi laptopami, w każdym zdalnym biurze, dla grupy administracyjnej najwyższego poziomu (**Główna grupa dla biur** na poniższym rysunku) należy wskazać dwa lub więcej urządzeń jako punkty dystrybucji (oprócz już istniejących punktów dystrybucji).

Na przykład: Laptop znajduje się w grupie administracyjnej **Office 1**, a następnie zostaje fizycznie przeniesiony do biura, które odpowiada grupie administracyjnej **Office 2**. Po przeniesieniu laptopa, Agent sieciowy spróbuje połączyć się z punktami dystrybucji przypisanymi do grupy **Office 1**, ale te punkty dystrybucji są niedostępne. Następnie Agent sieciowy próbuje połączyć się z punktami dystrybucji, które zostały przypisane do **Głównej grupy dla biur**. Ponieważ zdalne biura są odizolowane od siebie, próby nawiązania połączenia z punktami dystrybucji przypisanymi do grupy administracyjnej **Główna grupa dla biur** zakończą się pomyślnie tylko wtedy, gdy Agent sieciowy spróbuje połączyć się z punktami dystrybucji w grupie **Office 2**. Oznacza to, że laptop pozostanie w grupie administracyjnej, która odpowiada pierwszemu biuru, ale będzie korzystał z punktu dystrybucji biura, w którym aktualnie się znajduje.

Hierarchia zasad i korzystanie z zasad

W tej sekcji można znaleźć informacje dotyczące stosowania zasad do urządzeń w grupach administracyjnych. Ta sekcja zawiera również informacje o profilach zasad.

Hierarchia zasad

W Kaspersky Security Center zasad są używane do określenia jednego zestawu ustawień dla kilku urządzeń. Na przykład, obszar zasady aplikacji P zdefiniowanej dla grupy administracyjnej G zawiera zarządzane urządzenia z zainstalowaną aplikacją P, które zostały dodane do grupy G i wszystkich jej podgrup, za wyjątkiem podgrup, we właściwościach których odznaczono opcję **Dziedzicz z grupy nadrzędnej**.

Zasadę można odróżnić od lokalnego ustawienia po ikonach kłódki (🔒) obok jej ustawień. Jeśli ustawienie (lub grupa ustawień) jest zablokowane we właściwościach zasady, w pierwszej kolejności należy użyć tego ustawienia (lub grupy ustawień) podczas tworzenia obowiązującego ustawienia, a następnie należy zapisać ustawienie (lub grupę ustawień) do zasady podrzędnej.

Tworzenie obowiązujących ustawień można opisać w następujący sposób: wartości wszystkich ustawień, które nie zostały zablokowane, są kopiowane z zasady, a następnie są nadpisywane przez wartości ustawień lokalnych, a w kolejnym etapie wartości wynikowe są nadpisywane przez zablokowane ustawienia pobrane z zasady.

Zasady tej samej aplikacji oddziałują na siebie poprzez hierarchię grup administracyjnych: Zablokowane ustawienia z zasady nadrzędnej nadpisują te same ustawienia z zasady podrzędnej.

Dla użytkowników mobilnych istnieje specjalna zasada. Ta zasada jest aktywowana na urządzeniu, gdy to przełącza się do trybu użytkownika mobilnego. Zasady użytkowników mobilnych nie oddziałują na inne zasady poprzez hierarchię grup administracyjnych.

Profile zasad

Stosowanie zasad na urządzeniach tylko poprzez hierarchię grup administracyjnych może być niewygodne tylko w kilku przypadkach. Konieczne może być utworzenie kilku instancji jednej zasady, które różnią się jednym lub dwoma ustawieniami dla różnych grup administracyjnych, oraz zsynchronizowanie zawartości tych zasad w przyszłości.

Aby pomóc Ci uniknąć takich problemów, Kaspersky Security Center obsługuje *profile zasad*. Profil zasad jest to inaczej podzbiór ustawień zasady. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z zasadą i uzupełnia go zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowej" zasady, która jest aktywna na urządzeniu klienckim (komputerze lub urządzeniu mobilnym). Aktywacja profilu zmodyfikuje ustawienia zasad, które były aktywne na urządzeniu przed aktywacją profilu. Te ustawienia przyjmują wartości określone w profilu.

Aktualnie na profile zasad nałożone są następujące ograniczenia:

- Zasada może zawierać maksymalnie 100 profili.
- Profil zasad nie może zawierać innych profili.
- Profil zasad nie może zawierać ustawień powiadamiania.

Zawartość profilu

Profil zasad zawiera następujące elementy:

- Nazwa. Profile z takimi samymi nazwami wpływają na siebie poprzez hierarchię grup administracyjnych ze wspólnymi regułami.
- Podzbiór ustawień zasady. Profil zawiera tylko aktualnie wymagane ustawienia (ustawienia zablokowane).
- Warunek aktywacji to wyrażenie logiczne z właściwościami urządzenia. Profil jest aktywny (uzupełnia zasadę) tylko wtedy, gdy warunek aktywacji profilu jest prawdziwy. We wszystkich pozostałych przypadkach profil jest nieaktywny i jest ignorowany. W wyrażeniu logicznym mogą być uwzględnione następujące właściwości urządzenia:
  - Stan trybu użytkownika mobilnego.
  - Właściwości środowiska sieciowego — nazwa aktywnej reguły dla połączenia z Agentem sieciowym.
  - Obecność lub brak określonych znaczników na urządzeniu.
  - Lokalizacja urządzenia w jednostce Active Directory: jawna (urządzenie znajduje się w określonej jednostce OU) lub niejawna (urządzenie jest w jednostce OU, która znajduje się w określonej jednostce OU na dowolnym poziomie zagnieżdżenia).
  - Członkostwo urządzenia w grupie zabezpieczeń Active Directory (jawne lub niejawne).
  - Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory (jawne lub niejawne).
- Pole wyłączające profil. Wyłączone profile są zawsze ignorowane, a ich odpowiednie warunki aktywacji nie są sprawdzane.
- Priorytet profilu. Warunki aktywacji różnych profili są niezależne, a więc można aktywować kilka profili jednocześnie. Jeśli aktywne profile zawierają nienakładające się na siebie zbiory ustawień, nie pojawi się żaden problem. Jednakże dwa aktywne profile zawierające różne wartości tego samego ustawienia spowodują niejednoznaczność. Tę niejednoznaczność można wyeliminować poprzez priorytety profilu: Wartość niejednoznacznej zmiennej zostanie pobrana z profilu, który ma wyższy priorytet (ten, który znajduje się wyżej na liście profili).

Zachowanie profili, gdy zasady oddziałują na siebie poprzez hierarchię

Profile o tych samych nazwach zostają scalone zgodnie z regułami scalania zasad. Profile zasady nadrzędnej mają wyższy priorytet niż zasady podrzędnej. Jeśli modyfikowanie ustawień jest zabronione w zasadzie nadrzędnej (są zablokowane), zasada podrzędna używa warunków aktywacji profilu z zasady nadrzędnej. Jeśli modyfikowanie ustawień jest dozwolone w zasadzie nadrzędnej, używane są warunki aktywacji profilu z zasady podrzędnej.

Ponieważ w swoim warunku aktywacji profil zasad może zawierać opcję **Urządzenie jest w trybie offline**, profile całkowicie zastępują funkcję zasad dla użytkowników mobilnych, które nie będą już obsługiwane.

Zasada dla użytkowników mobilnych może zawierać profile, ale te profile mogą zostać aktywowane dopiero po przełączeniu urządzenia w tryb użytkownika mobilnego.

Zadania

Kaspersky Security Center zarządza aplikacjami zabezpieczającymi Kaspersky, zainstalowanymi na urządzeniach poprzez tworzenie i uruchamianie *zadań*. Zadania są potrzebne do instalowania, uruchamiania i zatrzymywania działania aplikacji, skanowania plików, aktualizowania baz danych i modułów aplikacji, a także wykonywania innych działań na aplikacjach.

Zadania dla określonej aplikacji mogą być tworzone tylko wtedy, gdy zainstalowana jest wtyczka zarządzająca dla tej aplikacji.

Zadania mogą być wykonywane na Serwerze administracyjnym i na urządzeniach.

Na Serwerze administracyjnym wykonywane są następujące zadania:

- Automatyczne rozsyłanie raportów
- Pobieranie uaktualnień do repozytorium Serwera administracyjnego
- Tworzenie kopii zapasowych danych Serwera administracyjnego
- Obsługa baz danych
- Synchronizacja Windows Update
- Tworzenie pakietów instalacyjnych w oparciu o obraz systemu operacyjnego odpowiedniego urządzenia

Na urządzeniach wykonywane są następujące typy zadań:

- *Zadania lokalne*—zadania wykonywane na określonym urządzeniu

  Zadania lokalne mogą zostać zmodyfikowane przez administratora przy użyciu narzędzi Konsoli administracyjnej lub przez użytkownika zdalnego urządzenia (na przykład, z poziomu interfejsu aplikacji zabezpieczającej). Jeśli zadanie lokalne zostało zmodyfikowane jednocześnie przez administratora i użytkownika zarządzanego urządzenia, zostaną zastosowane zmiany wprowadzone przez administratora, ponieważ mają wyższy priorytet.

- *Zadania grupowe*—zadania wykonywane na wszystkich urządzeniach określonej grupy

  Dopóki nie określono inaczej we właściwościach zadania, zadanie grupowe także wpływa na wszystkie podgrupy wybranej grupy. Zadanie grupowe także może wpływać (opcjonalnie) na urządzenia, które zostały podłączone do podrzędnych i wirtualnych Serwerów administracyjnych zainstalowanych w grupie lub w jej dowolnej podgrupie.

- *Zadania globalne*—zadania wykonywane na zbiorze urządzeń, niezależnie od tego, czy znajdują się w jakiejkolwiek grupie

Dla każdej aplikacji można utworzyć dowolną liczbę zadań grupowych, zadań globalnych lub zadań lokalnych.

Możesz wprowadzać zmiany w ustawieniach zadań, przeglądać postęp ich wykonywania, a także kopiować, eksportować, importować i usuwać zadania.

Zadanie jest uruchamiane na urządzeniu tylko wtedy, gdy uruchomiona jest aplikacja, dla której utworzono zadanie.

Wyniki zadań są zapisywane w dzienniku zdarzeń systemu Microsoft Windows oraz w raporcie zdarzeń Kaspersky Security Center na Serwerze administracyjnym i lokalnie na każdym urządzeniu.

Nie używaj prywatnych danych w ustawieniach zadania. Na przykład, unikaj określania hasła administratora domeny.

Reguły przenoszenia urządzeń

Zalecane jest automatyczne przydzielenie urządzeń do grup administracyjnych na serwerze wirtualnym, odpowiadającemu klientowi MSP, przy użyciu *reguł przenoszenia urządzeń*. Reguła przenoszenia urządzeń składa się z trzech głównych części: nazwy, warunku wykonania (wyrażenie logiczne z atrybutami urządzenia) oraz docelowej grupy administracyjnej. Reguła przenosi urządzenie do docelowej grupy administracyjnej, jeśli atrybuty urządzenia spełniają warunek wykonania reguły.

Wszystkie reguły przenoszenia urządzeń posiadają priorytety. Serwer administracyjny sprawdza, czy atrybuty urządzenia spełniają warunek wykonania każdej reguły, w rosnącej kolejności priorytetów. Jeśli atrybuty urządzenia spełniają warunek wykonania reguły, urządzenie zostaje przeniesione do grupy docelowej, a przetwarzanie reguły zostanie zakończone dla tego urządzenia. Jeśli atrybuty urządzenia spełniają warunki kilku reguł, urządzenie zostanie przeniesione do grupy docelowej reguły z najwyższym priorytetem (czyli tej, która znajduje się najwyżej na liście).

Reguły przenoszenia urządzeń mogą być tworzone pośrednio. Na przykład, we właściwościach pakietu instalacyjnego lub zadania zdalnej instalacji możesz określić grupę administracyjną, do której urządzenie musi zostać przeniesione po zainstalowaniu na nim Agenta sieciowego. Reguły przenoszenia urządzeń mogą być tworzone także bezpośrednio przez administratora Kaspersky Security Center na liście reguł przenoszenia. Lista ta znajduje się w Konsoli administracyjnej, we właściwościach grupy **Urządzenia nieprzypisane**.

Domyślnie reguła przenoszenia urządzeń jest przeznaczona do jednorazowego, wstępnego przydzielenia urządzeń do grup administracyjnych. Reguła przenosi urządzenia z grupy **Urządzenia nieprzypisane** tylko raz. Jeśli urządzenie był już raz przeniesione przy użyciu tej reguły, reguła ta nie przeniesie go już nawet wtedy, gdy ręcznie przeniesiesz urządzenie z powrotem do grupy **Urządzenia nieprzypisane**. Jest to zalecany sposób stosowania reguł przenoszenia.

Możesz przenieść urządzenia, które już zostały przydzielone do niektórych grup administracyjnych. W tym celu, we właściwościach reguły odznacz pole **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**.

Stosowanie reguł przenoszenia do urządzeń, które już zostały przydzielone do niektórych grup administracyjnych, znacząco zwiększa obciążenie na Serwerze administracyjnym.

Możesz utworzyć regułę przenoszenia, która będzie nieprzerwanie oddziaływać na jedno urządzenie.

Szczególnie zalecane jest unikanie ciągłego przenoszenia jednego urządzenia z jednej grupy do drugiej (na przykład, w celu zastosowania specjalnej zasady do tego urządzenia, uruchomienia specjalnego zadania grupowego lub zaktualizowania urządzenia poprzez punkt dystrybucji).

Takie scenariusze nie są obsługiwane, ponieważ w bardzo dużym stopniu zwiększają obciążenie na Serwerze administracyjnym oraz ruch sieciowy. Te scenariusze doprowadzają też do konfliktu z zasadami działania Kaspersky Security Center (szczególnie w obszarze uprawnień dostępu, zdarzeń i raportów). Należy znaleźć inne rozwiązanie, na przykład, poprzez użycie profili zasad, zadań dla wyborów urządzeń, przydzielania Agentów sieciowych zgodnie ze standardowym scenariuszem itd.

Kategoryzacja oprogramowania

Głównym narzędziem do monitorowania uruchomień aplikacji są *kategorie Kaspersky* (zwane dalej *Kategorie KL*). Kategorie KL umożliwiają administratorom Kaspersky Security Center uproszczenie obsługi kategoryzacji oprogramowania i zminimalizowanie ruchu sieciowego skierowanego do zarządzanych urządzeń.

Kategorie użytkownika powinny być tworzone tylko dla aplikacji, których nie można zaklasyfikować do żadnej z istniejących kategorii KL (na przykład, dla oprogramowania wykonanego na zamówienie użytkownika). Kategorie użytkownika są tworzone na podstawie pakietu instalacyjnego aplikacji (MSI) lub folderu z pakietami instalacyjnymi.

Jeśli dostępna jest duża ilość programów, które nie zostały skategoryzowane poprzez kategorie KL, można utworzyć automatycznie aktualizowaną kategorię. Sumy kontrolne plików wykonywalnych będą automatycznie dodawane do tej kategorii po każdej modyfikacji folderu zawierającego pakiety dystrybucyjne.

Nie twórz automatycznie aktualizowanych kategorii oprogramowania dla folderów Moje dokumenty, %windir%, %Pliki programów% i %Pliki programów(x86)%. Pula plików w tych folderach podlega częstym zmianom, co prowadzi do zwiększonego obciążenia na Serwerze administracyjnym i zwiększonego ruchu sieciowego. Należy utworzyć dedykowany folder ze zbiorem oprogramowania i okresowo dodawać do niego nowe elementy.

Informacje o aplikacjach wielodostępowych

Kaspersky Security Center umożliwia administratorom dostawców usług i administratorom dzierżawy używanie aplikacji Kaspersky z obsługą wielodostępności. Po zainstalowaniu aplikacji wielodostępowej firmy Kaspersky w infrastrukturze dostawcy usługi, dzierżawcy mogą rozpocząć korzystanie z aplikacji.

Aby oddzielić zadania i zasady dotyczące różnych dzierżawców, musisz utworzyć dedykowany wirtualny Serwer administracyjny w Kaspersky Security Center dla każdego dzierżawcy. Wszystkie zadania i zasady dla aplikacji wielodostępowych uruchomionych dla dzierżawcy muszą zostać utworzone dla grupy administracyjnej Zarządzane urządzenia wirtualnego Serwera administracyjnego odpowiadającego temu dzierżawcy. Zadania utworzone dla grup administracyjnych dotyczących głównego Serwera administracyjnego nie wpływają na urządzenia dzierżawców.

W przeciwieństwie do administratorów dostawcy usługi, administrator dzierżawy może tworzyć i przeglądać zadania i zasady aplikacji tylko dla urządzeń odpowiedniego dzierżawcy. Zestawy ustawień zadań i zasad dostępne dla administratorów dostawcy usługi i administratorów dzierżawy różnią się między sobą. Niektóre zestawy ustawień zadań i zasad nie są dostępne dla administratorów dzierżawy.

W obrębie hierarchicznej struktury dzierżawy zasady utworzone dla aplikacji wielodostępowych są dziedziczone przez grupy administracyjne niższego poziomu, a także przez grupy administracyjne wyższego poziomu: zasada jest przesyłana do wszystkich urządzeń klienckich, które należą do dzierżawcy.

Tworzenie kopii zapasowej i przywracanie ustawień Serwera administracyjnego

Tworzenie kopii zapasowej ustawień Serwera administracyjnego i jego baz danych odbywa się przy użyciu zadania tworzenia kopii zapasowej oraz narzędzia klbackup. Kopia zapasowa zawiera wszystkie główne ustawienia i obiekty dotyczące Serwera administracyjnego, takie jak certyfikaty, klucze główne do szyfrowania dysków na zarządzanych urządzeniach, klucze dla różnych licencji, strukturę grup administracyjnych z całą ich zawartością, zadaniami, zasadami itd. Przy pomocy kopii zapasowej można przywrócić działanie Serwera administracyjnego tak szybko, jak to możliwe, poświęcając na to od kilkunastu minut do kilku godzin.

Jeśli nie ma dostępnej kopii zapasowej, błąd może doprowadzić do bezpowrotnej utraty certyfikatów i wszystkich ustawień Serwera administracyjnego. Będzie to wymagało przeprowadzenia konfiguracji Kaspersky Security Center od początku oraz ponownego zainstalowania Agenta sieciowego w sieci organizacji. Wszystkie klucze główne do szyfrowania dysków na zarządzanych urządzeniach zostaną utracone, co spowoduje ryzyko utraty zaszyfrowanych danych na urządzeniach z zainstalowanym programem Kaspersky Endpoint Security. Dlatego też nigdy nie rezygnuj z regularnego wykonywania kopii zapasowej Serwera administracyjnego przy użyciu standardowego zadania tworzenia kopii zapasowej.

Kreator wstępnej konfiguracji tworzy zadanie wykonywania kopii zapasowej dla ustawień Serwera administracyjnego i ustawia jego codzienne wykonywanie na godzinę 4:00. Kopie zapasowe są domyślnie zapisywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskySC.

Jeśli serwer Microsoft SQL Server, zainstalowany na innym urządzeniu, jest używany jako DBMS, należy zmodyfikować zadanie tworzenia kopii zapasowej, określając jako folder do przechowywania kopii zapasowych ścieżkę UNC, która jest używana do zapisywania usługi Serwera administracyjnego oraz usługi SQL Server. To wymaganie wynika ze specyfiki specjalnej funkcji kopii zapasowej w systemie DBMS serwera Microsoft SQL Server.

Jeśli jako system DBMS używana jest lokalna instancja serwera Microsoft SQL Server, zalecane jest zapisanie kopii zapasowych na dedykowanym nośniku w celu zabezpieczenia ich przed uszkodzeniem wraz z Serwerem administracyjnym.

Ponieważ kopia zapasowa zawiera ważne dane, zadanie tworzenia kopii zapasowej oraz narzędzie klbackup oferują ochronę kopii zapasowej przy użyciu hasła. Domyślnie zadanie tworzenia kopii zapasowej wykonuje kopię zapasową z pustym hasłem. Hasło należy ustawić we właściwościach zadania tworzenia kopii zapasowej. Pominięcie tego wymagania doprowadza do sytuacji, w której wszystkie klucze certyfikatów Serwera administracyjnego, klucze dla licencji oraz klucze główne dla szyfrowania dysków na zarządzanych urządzeniach pozostaną niezaszyfrowane.

Oprócz regularnych kopii zapasowych, kopie zapasowe należy tworzyć także przed każdą znaczącą zmianą, w tym instalacją aktualizacji i łat Serwera administracyjnego.

Jeśli używasz Microsoft SQL Server jako DBMS, możesz zminimalizować rozmiar kopii zapasowych. W tym celu włącz opcję **Kompresuj kopię zapasową** w ustawieniach SQL Server.

Przywracanie kopii zapasowej odbywa się przy użyciu narzędzia klbackup na działającej instancji Serwera administracyjnego, który został właśnie zainstalowany i posiada tę samą wersję (lub nowszą), dla której kopia zapasowa została utworzona.

Instancja Serwera administracyjnego, na którym kopia zapasowa ma zostać przywrócona, musi korzystać z systemu DBMS tego samego typu (na przykład ten sam SQL Server lub MariaDB) i tej samej lub nowszej wersji. Wersja Serwera administracyjnego może być taka sama (z tą samą lub późniejszą łatą) lub nowsza.

Sekcja opisuje standardowe scenariusze przywracania ustawień i obiektów Serwera administracyjnego.

Urządzenie z zainstalowanym Serwerem administracyjnym nie działa

Jeśli urządzenie, na którym jest zainstalowany Serwer administracyjny, nie działa z powodu błędu, zalecane jest wykonanie następujących działań:

- Nowy Serwer administracyjny musi posiadać ten sam adres: nazwę NetBIOS, nazwę FQDN lub statyczny adres IP (w zależności od tego, co zostało ustawione podczas instalacji Agentów sieciowych).
- Zainstaluj Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą lub nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu kreatora.
- W menu **Start** uruchom narzędzie klbackup i wykonaj przywracanie.

Ustawienia Serwera administracyjnego lub bazy danych są uszkodzone

Jeżeli Serwer administracyjny nie działa ze względu na uszkodzone ustawienia lub bazę danych (na przykład, w wyniku przepięcia), zalecane jest użycie następujących scenariuszy:

1. Przeskanuj system plików na uszkodzonym urządzeniu.
2. Odinstaluj niedziałającą wersję Systemu operacyjnego.
3. Zainstaluj ponownie Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej (lub nowszej) wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą lub nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu kreatora.
4. Z poziomu menu **Start** uruchom narzędzie klbackup i przywróć kopię zapasową.

Zabronione jest przywracanie Serwera administracyjnego w sposób inny niż przy użyciu narzędzia klbackup.

Wszelkie próby przywrócenia Serwera administracyjnego przy użyciu oprogramowania firm trzecich doprowadzą do desynchronizacji danych na węzłach aplikacji Kaspersky Security Center i w konsekwencji - do niepoprawnego działania aplikacji.

Instalowanie Agenta sieciowego i aplikacji zabezpieczającej

Aby zarządzać urządzeniami w organizacji, na każdym z nich należy zainstalować Agenta sieciowego. Zdalna instalacja aplikacji Kaspersky Security Center na urządzeniach w firmie zazwyczaj rozpoczyna się od zainstalowania na nich Agenta sieciowego.

W systemie Microsoft Windows XP Agent sieciowy może nie wykonać poprawnie następujących działań: pobranie uaktualnień bezpośrednio z serwerów Kaspersky (jako punkt dystrybucji); działanie jako serwer proxy KSN (jako punkt dystrybucji); oraz wykrywanie luk firm trzecich (jeśli używane jest Zarządzanie lukami i poprawkami).

Wstępne wdrożenie

Jeśli Agent sieciowy został już zainstalowany na urządzeniu, zdalna instalacja aplikacji na tym urządzeniu odbywa się poprzez Agenta sieciowego. Pakiet dystrybucyjny aplikacji, która ma zostać zainstalowana, jest przesyłany za pośrednictwem kanałów komunikacji pomiędzy Agentami sieciowymi i Serwerem administracyjnym wraz z ustawieniami instalacji, zdefiniowanymi przez administratora. Aby przesłać pakiet dystrybucyjny, możesz użyć węzłów pośredniczących, na przykład, punktów dystrybucji, dostarczania multiemisyjnego itd. Więcej informacji dotyczących instalacji aplikacji na zarządzanych urządzeniach, na których jest już zainstalowany Agent sieciowy, można znaleźć poniżej.

Możesz przeprowadzić wstępną instalację Agenta sieciowego na urządzeniach działających pod kontrolą systemu Windows, korzystając z jednej z następujących metod:

- Używając narzędzi firm trzecich do zdalnej instalacji aplikacji.
- Korzystając z zasad grupy w systemie Windows: używając standardowych narzędzi do zarządzania systemu Windows dla zasad grupy.
- W trybie wymuszonym, korzystając ze specjalnych opcji w zadaniu zdalnej instalacji programu Kaspersky Security Center.
- Wysyłając do użytkowników urządzeń odnośniki do pakietów autonomicznych, wygenerowanych przez Kaspersky Security Center. Pakiety autonomiczne to moduły wykonywalne, które zawierają pakiety dystrybucyjne wybranych aplikacji wraz ze zdefiniowanymi ustawieniami.
- Ręcznie, poprzez uruchomienie instalatorów aplikacji na urządzeniach.

Na platformach innych niż Microsoft Windows należy przeprowadzić wstępną instalację Agenta sieciowego na zarządzanych urządzeniach przy użyciu istniejących narzędzi firm trzecich lub ręcznie, poprzez wysłanie do użytkowników archiwów ze wstępnie skonfigurowanym pakietem dystrybucyjnym. Na platformach innych niż Windows możesz uaktualnić Agenta sieciowego do nowej wersji lub zainstalować inne aplikacje firmy Kaspersky, korzystając z Agentów sieciowych (już zainstalowanych na urządzeniach) przeznaczonych do wykonywania zadań zdalnej instalacji. W tym przypadku instalacja przebiega identycznie jak instalacja na urządzeniach działających pod kontrolą systemu Microsoft Windows.

Podczas wybierania metody i strategii wdrożenia aplikacji w zarządzanej sieci należy mieć na uwadze kilka czynników (częściowa lista):

- Konfiguracja sieci korporacyjnej
- Całkowitą liczbę urządzeń
- Obecność domen Windows w zarządzanej sieci, możliwość modyfikacji zasady grupy Active Directory w tych domenach
- Wykrywanie kont użytkowników z uprawnieniami lokalnego administratora na urządzeniach, na których została zaplanowana wstępna zdalna instalacja aplikacji firmy Kaspersky (dostępność konta użytkownika domeny z uprawnieniami lokalnego administratora lub obecność ujednoliconych lokalnych kont użytkowników z uprawnieniami administratora na tych urządzeniach)

- Typ połączenia i przepustowość kanału sieciowego pomiędzy Serwerem administracyjnym a sieciami klienckimi MSP, a także przepustowość kanałów w tych sieciach

- Ustawienia zabezpieczeń zastosowane na zdalnych urządzeniach w momencie uruchomienia zdalnej instalacji (na przykład, użycie UAC lub Prostego udostępniania plików)

Konfigurowanie instalatorów

Przed uruchomieniem wdrożenia aplikacji Kaspersky w sieci, należy określić ustawienia instalacji (ustawienia definiowane podczas instalacji aplikacji). Podczas instalacji Agenta sieciowego należy określić przynajmniej adres połączenia z Serwerem administracyjnym i ustawienia proxy; niektóre ustawienia zaawansowane też mogą być wymagane. W zależności od wybranej metody instalacji, ustawienia można zdefiniować w różny sposób. W najprostszym przypadku (ręczna interaktywna instalacja na wybranym urządzeniu) wszystkie odpowiednie ustawienia można zdefiniować w interfejsie instalatora, co oznacza, że w niektórych sytuacjach wstępna instalacja może być wykonana nawet poprzez wysłanie do użytkownika odnośnika do pakietu dystrybucyjnego Agenta sieciowego wraz z ustawieniami (adres Serwera administracyjnego itd.), które użytkownik powinien wprowadzić w interfejsie instalatora.

Ta metoda nie jest zalecana, ponieważ jest ona niewygodna dla użytkowników i wiąże się z wysokim ryzykiem błędów podczas ręcznego definiowania ustawień; nie nadaje się również do cichej instalacji aplikacji na grupach urządzeń. Na ogół administrator musi określić wartości dla ustawień w sposób scentralizowany; te wartości mogą być następnie użyte podczas tworzenia pakietów autonomicznych. Pakiety autonomiczne to samorozpakowujące się archiwa, które zawierają pakiety dystrybucyjne z ustawieniami zdefiniowanymi przez administratora. Pakiety autonomiczne mogą znajdować się w zasobach, z których mogą pobierać użytkownicy końcowi (na przykład na serwerze Kaspersky Security Center Web Server) i które umożliwiają przeprowadzenie cichej instalacji na wybranych urządzeniach w sieci.

Pakiety instalacyjne

Pierwsza i główna metoda definiowania ustawień instalacji aplikacji jest uniwersalna i tym samym jest odpowiednia dla wszystkich metod instalacji: przy użyciu narzędzi Kaspersky Security Center oraz większości narzędzi firm trzecich. Ta metoda obejmuje utworzenie pakietów instalacyjnych aplikacji w Kaspersky Security Center.

Pakiety instalacyjne są generowane przy użyciu następujących metod:

- Automatycznie, z określonych pakietów dystrybucyjnych, na podstawie załączonych *deskryptorów* (pliki z rozszerzeniem .kud, które zawierają reguły dla instalacji, wyniki analizy oraz inne informacje)

- Z plików wykonywalnych instalatorów lub z instalatorów w formacie Microsoft Windows Installer (MSI), które są dla standardowych lub obsługiwanych aplikacji

Wygenerowane pakiety instalacyjne są zorganizowane hierarchicznie jako foldery z podfolderami i plikami. Oprócz oryginalnego pakietu dystrybucyjnego, pakiet instalacyjny zawiera ustawienia dostępne do modyfikacji (w tym ustawienia instalatora oraz reguły przetwarzania dla takich sytuacji, jak konieczność ponownego uruchomienia systemu operacyjnego w celu zakończenia instalacji), a także drobne moduły pomocnicze.

Wartości ustawień instalacji, które są określone dla wybranej obsługiwanej aplikacji, można zdefiniować w interfejsie Konsoli administracyjnej podczas tworzenia pakietu instalacyjnego (więcej ustawień można znaleźć we właściwościach już utworzonego pakietu instalacyjnego). Podczas zdalnej instalacji aplikacji przy użyciu narzędzi Kaspersky Security Center pakiety instalacyjne są dostarczane na urządzenia docelowe, dzięki czemu uruchomienie instalatora aplikacji udostępni dla tej aplikacji wszystkie ustawienia zdefiniowane przez administratora. Jeśli do zainstalowania aplikacji firmy Kaspersky używasz narzędzi firm trzecich, musisz zapewnić dostępność całego pakietu instalacyjnego na urządzeniu docelowym, czyli pakietu dystrybucyjnego i jego ustawień. Pakiety instalacyjne są tworzone i przechowywane przez Kaspersky Security Center w dedykowanym podfolderze udostępnionego folderu danych.

W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.

Instrukcje dotyczące korzystania z tej metody konfiguracji dla aplikacji Kaspersky przed ich zainstalowaniem przy użyciu narzędzi firm trzecich można znaleźć w sekcji „Zdalna instalacja przy użyciu zasad grupy Microsoft Windows".

Natychmiast po zainstalowaniu programu Kaspersky Security Center, automatycznie zostaje wygenerowanych kilka pakietów instalacyjnych. Pakiety te są gotowe do zainstalowania i zawierają pakiety Agenta sieciowego oraz pakiety aplikacji zabezpieczających dla Microsoft Windows.

W niektórych przypadkach używanie pakietów instalacyjnych do zdalnego instalowania aplikacji w sieci klienckiej MSP oznacza konieczność utworzenia pakietów instalacyjnych na Serwerach wirtualnych, które odpowiadają klientom MSP. Utworzenie pakietów instalacyjnych na Serwerach wirtualnych umożliwia użycie różnych ustawień instalacji dla różnych klientów MSP. W pierwszej instancji jest to przydatne podczas zarządzania pakietami instalacyjnymi Agentów sieciowych, gdyż Agenty sieciowe zainstalowane w sieciach różnych klientów MSP używają różnych adresów do nawiązywania połączenia z Serwerem administracyjnym. Adres połączenia określa Serwer, z którym łączy się Agent sieciowy.

Oprócz możliwości natychmiastowego utworzenia nowych pakietów instalacyjnych na wirtualnym Serwerze administracyjnym, główny tryb działania dla pakietów instalacyjnych na wirtualnych Serwerach administracyjnych to „rozesłanie" pakietów instalacyjnych z głównego Serwera administracyjnego do Serwerów wirtualnych. Możesz rozesłać wybrane (lub wszystkie) pakiety instalacyjne na wybrane wirtualne Serwery administracyjne (w tym wszystkie Serwery w obrębie wybranej grupy administracyjnej) przy użyciu odpowiedniego zadania Serwera administracyjnego. Dodatkowo, podczas tworzenia nowego wirtualnego Serwera administracyjnego możesz wybrać listę pakietów instalacyjnych głównego Serwera administracyjnego. Wybrane pakiety zostaną natychmiast rozesłane do nowo utworzonego wirtualnego Serwera administracyjnego.

Podczas rozsyłania pakietu instalacyjnego jego zawartość nie jest kopiowana w całości. Repozytorium plików na wirtualnym Serwerze administracyjnym, który odpowiada rozsyłanemu pakietowi instalacyjnemu, przechowuje tylko pliki z ustawieniami określonymi dla tego Serwera wirtualnego. Główna część pakietu instalacyjnego (w tym pakiet dystrybucyjny instalowanej aplikacji) pozostanie niezmieniona. Jest ona przechowywana tylko w repozytorium głównego Serwera administracyjnego. Umożliwia to drastyczne zwiększenie wydajności systemu i zmniejszenie wymaganej przestrzeni na dysku. Podczas zarządzania pakietami instalacyjnymi rozsyłanymi do wirtualnych Serwerów administracyjnych (czyli podczas uruchamiania zadań zdalnej instalacji lub tworzenia autonomicznych pakietów instalacyjnych) dane z oryginalnego pakietu instalacyjnego głównego Serwera administracyjnego zostają „scalone" z plikami ustawień, które odpowiadają pakietowi przesłanemu na wirtualny Serwer administracyjny.

Klucz licencyjny dla aplikacji może zostać określony we właściwościach pakietu instalacyjnego, ale zalecane jest unikanie tej metody dystrybucji licencji, ponieważ łatwo jest uzyskać dostęp do odczytu plików w folderze. Dla kluczy licencyjnych należy używać zadań automatycznego rozsyłania kluczy licencyjnych lub instalacji.

Właściwości MSI i pliki transformacji

Innym sposobem skonfigurowania instalacji na platformie Windows jest zdefiniowanie właściwości MSI i plików transformacji. Ta metoda może być używana podczas instalacji przy użyciu narzędzi firm trzecich przeznaczonych dla instalatorów w formacie Microsoft Installer, a także podczas instalacji poprzez zasady grupy systemu Windows przy użyciu standardowych narzędzi Microsoft lub narzędzi innych firm przeznaczonych do zarządzania zasadami grupy systemu Windows.

Zdalna instalacja przy użyciu narzędzi firm trzecich

Jeśli w organizacji dostępne są jakiekolwiek narzędzia do zdalnej instalacji aplikacji (na przykład, Microsoft System Center), wygodnym rozwiązaniem będzie przeprowadzenie wstępnej zdalnej instalacji przy użyciu tych narzędzi.

Należy wykonać następujące czynności:

- Wybierz metodę konfiguracji instalacji, która najbardziej odpowiada używanemu narzędziu do zdalnej instalacji.
- Zdefiniuj mechanizm synchronizacji pomiędzy modyfikacją ustawień pakietów instalacyjnych (poprzez interfejs Konsoli administracyjnej) a działaniem wybranych narzędzi firm trzecich, używanych do zdalnej instalacji aplikacji z pakietu instalacyjnego.

Informacje ogólne o zadaniach zdalnej instalacji w Kaspersky Security Center

Kaspersky Security Center oferuje szeroki zakres metod zdalnej instalacji aplikacji, które są zaimplementowane pod postacią zadań zdalnej instalacji. Możesz utworzyć zadanie zdalnej instalacji dla określonej grupy administracyjnej oraz dla wskazanych urządzeń lub wyboru urządzeń (takie zadania są wyświetlane w Konsoli administracyjnej, w folderze **Zadania**). Podczas tworzenia zadania możesz wybrać pakiety instalacyjne (Agenta sieciowego i / lub innej aplikacji), które zostaną zainstalowane w obrębie tego zadania, a także określić pewne ustawienia, które definiują metodę zdalnej instalacji.

Zadania dla grup administracyjnych dotyczą urządzeń znajdujących się w określonej grupie oraz wszystkich urządzeń we wszystkich podgrupach tej grupy administracyjnej. Zadanie obejmuje urządzenia podrzędnych Serwerów administracyjnych znajdujących się w grupie lub jej dowolnych podgrupach, jeśli odpowiednie ustawienie zostało włączone w zadaniu.

Zadania dla określonych urządzeń aktualizują listę urządzeń klienckich przy każdym uruchomieniu zgodnie z zawartością wyborów w momencie uruchomienia zadania. Jeśli wybór zawiera urządzenia, które zostały połączone z podrzędnymi Serwerami administracyjnymi, zadanie zostanie uruchomione także na tych urządzeniach.

Aby zapewnić pomyślne działanie zadania zdalnej instalacji na urządzeniach połączonych z podrzędnymi Serwerami administracyjnymi, należy użyć zadania dystrybucji do przekazania pakietów instalacyjnych używanych przez zadanie użytkownika do odpowiednich podrzędnych Serwerów administracyjnych.

Zdalna instalacja przy użyciu zasad grupy Microsoft Windows

Przeprowadzenie wstępnej instalacji Agentów sieciowych poprzez zasady grupy Microsoft Windows jest zalecane wtedy, gdy spełnione są następujące warunki:

- Urządzenie należy do domeny Active Directory.
- Dostęp do kontrolera domeny zostaje nadany z uprawnieniami administratora, dzięki czemu możliwe jest utworzenie i zmodyfikowanie zasad grupy Active Directory.
- Skonfigurowane pakiety instalacyjne można przenieść do sieci, w której znajdują się zarządzane urządzenia docelowe (do folderu współdzielonego, dostępnego do odczytu dla wszystkich urządzeń docelowych).
- Schemat zdalnej instalacji umożliwia zaczekanie na kolejne rutynowe ponowne uruchomienie urządzeń docelowych przed rozpoczęciem zdalnej instalacji Agentów sieciowych na tych urządzeniach (lub można wymusić zastosowanie na tych urządzeniach zasady grupy systemu Windows).

Ten schemat instalacji charakteryzuje się następującymi cechami:

- Pakiet dystrybucyjny aplikacji w formacie Microsoft Installer (pakiet MSI) znajduje się w folderze współdzielonym (folder, w którym konta SystemLokalny urządzeń docelowych mają uprawnienia do odczytu).
- W zasadzie grupy Active Directory, dla pakietu dystrybucyjnego tworzony jest obiekt instalacji.
- Obszar instalacji jest ustawiany poprzez określenie jednostki organizacyjnej (OU) i/lub grupy zabezpieczeń, która zawiera urządzenia docelowe.
- Następnym razem, gdy urządzenie docelowe zaloguje się do domeny (przed zalogowaniem się użytkowników do systemu), wszystkie zainstalowane aplikacje są sprawdzane pod kątem żądanej aplikacji. Jeśli żądana aplikacja nie zostanie odnaleziona, pakiet dystrybucyjny zostanie pobrany z zasobu określonego w zasadzie, a następnie zostanie zainstalowany.

Ten schemat zdalnej instalacji niesie za sobą korzyść, jaką jest instalowanie przypisanych aplikacji na urządzeniach docelowych podczas ładowania systemu operacyjnego, czyli nawet przed zalogowaniem się użytkownika do systemu. Nawet jeśli użytkownik, który nie ma wystarczających uprawnień, usunie aplikację, zostanie ona ponownie zainstalowana przy kolejnym uruchomieniu systemu operacyjnego. Wadą tego schematu wdrożenia jest fakt, że zmiany w zasadzie grupowej, które zostały wprowadzone przez administratora, nie zostaną zastosowane, aż do ponownego uruchomienia urządzenia (jeśli nie są używane narzędzia dodatkowe).

Zasady grupy można użyć do zainstalowania Agenta sieciowego oraz innych aplikacji, jeśli ich instalatory są w formacie Windows Installer.

> Instalacja Agenta sieciowego z pakietu MSI możliwa jest tylko w trybie cichym, instalacja interaktywna z pakietu MSI nie jest obsługiwana.

Poza tym, jeśli wybierzesz tę metodę wdrożenia, musisz mieć na uwadze obciążenie zasobu plików, z którego pliki zostaną skopiowane na urządzenia docelowe po zastosowaniu zasad grupy systemu Windows. Musisz także wybrać metodę dostarczenia skonfigurowanego pakietu instalacyjnego do tego zasobu, a także metodę synchronizacji odpowiednich zmian w jego ustawieniach.

Zarządzanie zasadami Microsoft Windows przy użyciu zadania zdalnej instalacji z programu Kaspersky Security Center

Ta metoda zdalnej instalacji jest dostępna tylko wtedy, gdy dostęp do kontrolera domeny, który zawiera urządzenia docelowe, jest możliwy z poziomu urządzenia z Serwerem administracyjnym, a także możliwy jest dostęp do odczytu folderu współdzielonego Serwera administracyjnego (tego, w którym znajdują się pakiety instalacyjne) z poziomu urządzeń docelowych. Ze względu na wyżej wspomniane przyczyny, ta metoda zdalnej instalacji nie jest stosowana do MSP.

Samodzielna instalacja aplikacji przy użyciu zasad Microsoft Windows

Administrator może tworzyć obiekty wymagane do zainstalowania w zasadach grupy systemu Windows w swoim imieniu. W tym przypadku pakiety należy przesłać na autonomiczny serwer plików i udostępnić odnośnik do nich.

Dostępne są następujące scenariusze instalacji:

- Administrator tworzy pakiet instalacyjny i konfiguruje jego ustawienia w Konsoli administracyjnej. Następnie administrator kopiuje cały podfolder EXEC tego pakietu z folderu współdzielonego Kaspersky Security Center do folderu w dedykowanym zasobie plików w organizacji. Obiekt zasad grupy zawiera odnośnik do pliku MSI tego pakietu, który jest przechowywany w podfolderze w dedykowanym zasobie plików w organizacji.

- Administrator pobiera pakiet dystrybucyjny aplikacji (w tym pakiet Agenta sieciowego) z Internetu i wysyła go do dedykowanego zasobu plików w organizacji. Obiekt zasad grupy zawiera odnośnik do pliku MSI tego pakietu, który jest przechowywany w podfolderze w dedykowanym zasobie plików w organizacji. Ustawienia instalacji są definiowane poprzez konfigurowanie właściwości MSI lub poprzez konfigurowanie plików transformacji MST.

Wymuszona zdalna instalacja przy użyciu zadania zdalnej instalacji z Kaspersky Security Center

Aby wykonać wstępne wdrożenie Agenta sieciowego lub innych aplikacji, możesz wymusić instalację wybranych pakietów instalacyjnych, korzystając z zadania zdalnej instalacji programu Kaspersky Security Center — pod warunkiem, że każde urządzenie ma konto(-a) użytkownika z uprawnieniami administratora lokalnego.

Instalacja wymuszona może być zastosowana także wtedy, gdy urządzenia nie są dostępne bezpośrednio dla Serwera administracyjnego, na przykład: urządzenia znajdują się w odizolowanych sieciach lub urządzenia są w sieci lokalnej, a Serwer administracyjny znajduje się w strefie DMZ.

W przypadku wdrożenia początkowego Agent sieciowy nie jest instalowany. Dlatego w ustawieniach zadania zdalnej instalacji nie można wybrać opcji dystrybucji plików wymaganych do instalacji aplikacji za pomocą Agenta sieciowego. Dystrybucję plików można przeprowadzić wyłącznie za pośrednictwem zasobów systemu operacyjnego, za pośrednictwem Serwera administracyjnego lub punktów dystrybucji.

Usługa Serwera administracyjnego musi być uruchomiona na koncie posiadającym uprawnienia administracyjne na urządzeniach docelowych. Alternatywnie możesz określić konto, które ma dostęp do części admin$ w ustawieniach ogólnych zadania zdalnej instalacji.

Należy pamiętać, że domyślnie zadanie zdalnej instalacji łączy się z urządzeniami przy użyciu danych logowania konta, na którym uruchomiony jest Serwer administracyjny, tj. konta dostępu do udziału admin$. To konto należy określić w ustawieniach zadania zdalnej instalacji tylko wtedy, gdy Agent sieciowy nie jest zainstalowany na urządzeniach docelowych.
Podczas tworzenia zadania zdalnej instalacji, które ma zostać uruchomione na urządzeniach z systemem Linux, należy zawsze określić konto do nawiązania połączenia SSH.

Możesz bezpośrednio wskazać urządzenia docelowe, wybrać grupę administracyjną Kaspersky Security Center, do której należą; lub utworzyć wybór urządzeń w oparciu o określone kryterium. Instalacja rozpoczyna się zgodnie z terminarzem zadania. Jeśli we właściwościach zadania włączone jest ustawienie **Uruchom pominięte zadania**, zadanie może zostać uruchomione albo natychmiast po włączeniu urządzeń docelowych, albo po ich przeniesieniu do docelowej grupy administracyjnej.

Instalacja wymuszona obejmuje dostarczenie pakietów instalacyjnych do urządzeń docelowych, skopiowanie plików do zasobu admin$ na każdym urządzeniu docelowym, a także zdalną rejestrację usług pomocniczych na tych urządzeniach. Dostarczenie pakietów instalacyjnych do punktów dystrybucji odbywa się poprzez funkcję Kaspersky Security Center zapewniającą interakcję z siecią. W tym przypadku muszą być spełnione następujące warunki:

- Dostęp do urządzeń docelowych jest możliwy od strony Serwera administracyjnego lub od strony punktu dystrybucji.
- Rozwiązywanie nazw urządzeń docelowych działa poprawnie w sieci.
- Zasób administracyjny (admin$) pozostanie włączony na urządzeniach docelowych.
- Na urządzeniach docelowych uruchomione są następujące usługi systemowe:
  - Serwer (LanmanServer)

    Domyślnie ta usługa jest uruchomiona.
  - Program uruchamiający procesy serwera DCOM (DcomLaunch)
  - Mapowanie punktów końcowych RPC (RpcEptMapper)
  - Zdalne wywoływanie procedur (RpcSs)
- Port TCP 445 jest otwarty na urządzeniach docelowych, aby umożliwić zdalny dostęp za pomocą narzędzi systemu Windows.

  > Protokoły TCP 139, UDP 137 i UDP 138 są używane przez starsze protokoły i nie są już potrzebne w obecnych aplikacjach.

  W zaporze sieciowej muszą być dozwolone dynamiczne porty dostępu wychodzącego w celu nawiązywania połączeń z Serwera administracyjnego i punktów dystrybucji do urządzeń docelowych.
- Ustawienia zabezpieczeń zasad domeny usługi Active Directory umożliwiają działanie protokołu NTLM podczas wdrażania Agenta Sieciowego.
- Na urządzeniach docelowych z systemem Microsoft Windows XP tryb Proste udostępnianie plików jest wyłączony.

- Na urządzeniach docelowych model współdzielenia dostępu i zabezpieczeń jest ustawiony jako *Klasyczny – lokalni użytkownicy uwierzytelniają się jako oni sami*. W żadnym wypadku nie może to być *tylko Gość – lokalni użytkownicy uwierzytelniają się jako Gość*.

- Urządzenia docelowe są członkami domeny lub wcześniej są tworzone na urządzeniach docelowych jednakowe konta z uprawnieniami administratora.

Aby pomyślnie zainstalować Agenta sieciowego lub inne aplikacje na urządzeniu, które nie jest przyłączone do domeny Active Directory systemu Windows Server 2003 lub nowszego, należy wyłączyć zdalną kontrolę konta użytkownika (UAC) na tym urządzeniu. Zdalna kontrola konta użytkownika (UAC) jest jednym z powodów uniemożliwiających lokalnym kontom administracyjnym dostęp do admin$, który jest konieczny do wymuszonej instalacji Agenta sieciowego lub innych aplikacji. Wyłączenie zdalnej kontroli konta użytkownika (UAC) nie ma wpływu na lokalną UAC.

Podczas instalacji na nowych urządzeniach, które jeszcze nie zostały przydzielone do żadnej grupy administracyjnej Kaspersky Security Center, możesz otworzyć właściwości zadania zdalnej instalacji i określić grupę administracyjną, do której urządzenia zostaną przeniesione po zakończeniu instalacji Agenta sieciowego.

Podczas tworzenia zadania grupowego należy pamiętać, że każde zadanie grupowe ma wpływ na wszystkie urządzenia we wszystkich grupach zagnieżdżonych w wybranej grupie. Dlatego też należy unikać powielania zadań instalacji w podgrupach.

Prostszym sposobem tworzenia zadań wymuszonej instalacji aplikacji jest instalacja automatyczna. We właściwościach grupy administracyjnej należy otworzyć listę pakietów instalacyjnych a następnie wybrać te, które muszą zostać zainstalowane na urządzeniach w tej grupie. W rezultacie, wybrane pakiety instalacyjne zostaną automatycznie zainstalowane na wszystkich urządzeniach w tej grupie i wszystkich jej podgrupach. Przedział czasu, w trakcie którego pakiety zostaną zainstalowane, zależy od przepustowości sieci i całkowitej liczby urządzeń w sieci.

Aby zmniejszyć obciążenie Serwera administracyjnego podczas dostarczania pakietów instalacyjnych do urządzeń docelowych, w zadaniu instalacji można wybrać instalację za pośrednictwem punktów dystrybucji. Należy zauważyć, że ta metoda instalacji powoduje duże obciążenie urządzeń pełniących role punktów dystrybucji. W związku z tym zaleca się wybór urządzeń spełniających wymagania stawiane punktom dystrybucji. Jeśli korzystasz z punktów dystrybucji, upewnij się, że znajdują się one w każdej z odizolowanych podsieci, w których znajdują się urządzenia docelowe.

Korzystanie z punktów dystrybucji jako lokalnych centrów instalacji jest dobrym rozwiązaniem, gdy instalacja na urządzeniach w podsieciach komunikujących się z Serwerem administracyjnym odbywa się poprzez kanały o małej przepustowości, a pomiędzy urządzeniami w tej samej podsieci dostępny jest szeroki kanał.

Co więcej, wolna przestrzeń na dysku w partycji, na której znajduje się folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit, musi wielokrotnie przekraczać całkowity rozmiar pakietów dystrybucyjnych instalowanych aplikacji.

Uruchamianie pakietów autonomicznych utworzonych przez Kaspersky Security Center

Powyżej opisane metody wstępnej zdalnej instalacji Agenta sieciowego i innych aplikacji nie zawsze będą mogły zostać zaimplementowane, gdyż nie jest możliwe spełnienie wszystkich wymaganych warunków. W takich przypadkach można utworzyć standardowy plik wykonywalny zwany *autonomicznym pakietem instalacyjnym* poprzez Kaspersky Security Center, korzystając z pakietów instalacyjnych z odpowiednimi ustawieniami instalacji, które zostały przygotowane przez administratora. Autonomiczny pakiet instalacyjny może zostać opublikowany na wewnętrznym serwerze WWW (znajdującym się w Kaspersky Security Center), jeśli będzie to uzasadnione (zewnętrzny dostęp do tego serwera WWW został skonfigurowany dla użytkowników urządzeń docelowych), lub na specjalnie wdrożonym serwerze WWW znajdującym się w Kaspersky Security Center Web Console. Możesz także skopiować pakiety autonomiczne na inny serwer WWW.

Korzystając z Kaspersky Security Center, możesz wysłać do wybranych użytkowników wiadomość e-mail zawierającą odnośnik do pliku pakietu autonomicznego na aktualnie używanym serwerze WWW oraz prośbę o jego uruchomienie (w trybie interaktywnym lub z przełącznikiem "-s" dla cichej instalacji). Do wiadomości e-mail możesz załączyć autonomiczny pakiet instalacyjny, a następnie wysłać ją do użytkowników urządzeń, którzy nie mają dostępu do serwera WWW. Administrator może także skopiować pakiet autonomiczny na urządzenie zewnętrzne, dostarczyć go na odpowiednie urządzenie, a następnie uruchomić go.

Pakiet autonomiczny można utworzyć z pakietu Agenta sieciowego, pakietu innej aplikacji (na przykład, zabezpieczającej) lub z obu pakietów. Jeśli pakiet autonomiczny został utworzony z pakietu Agenta sieciowego i innej aplikacji, instalacja rozpocznie się z Agenta sieciowego.

Podczas tworzenia pakietu autonomicznego z pakietu Agenta sieciowego możesz określić grupę administracyjną, do której nowe urządzenia (te, które nie zostały przydzielone do żadnej grup administracyjnych) zostaną automatycznie przeniesione po zakończeniu instalacji Agenta sieciowego na tych urządzeniach.

Pakiety autonomiczne mogą być uruchomione w trybie interaktywnym (opcja domyślna), wyświetlając wynik instalacji aplikacji, które zawierają, lub mogą być uruchomione w trybie cichym (z kluczem "-s"). Tryb cichy może zostać użyty dla instalacji ze skryptów, na przykład, ze skryptów skonfigurowanych do uruchamiania po wdrożeniu obrazu systemu operacyjnego. Wynik instalacji w trybie cichym jest determinowany przez kod zwrotny procesu.

Opcje ręcznej instalacji aplikacji

Administratorzy lub doświadczeni użytkownicy mogą zainstalować aplikacje ręcznie w trybie interaktywnym. Mogą oni użyć oryginalnych pakietów dystrybucyjnych lub wygenerowanych z nich pakietów instalacyjnych, które są przechowywane w folderze współdzielonym Kaspersky Security Center. Domyślnie instalatory są uruchamiane w trybie interaktywnym i wyświetlają użytkownikom komunikaty z pytaniami o podanie wszystkich wymaganych wartości. Jednakże podczas uruchamiania procesu setup.exe z katalogu głównego pakietu instalacyjnego z przełącznikiem "-s", instalator zostanie uruchomiony w trybie cichym i z ustawieniami, które zostały określone podczas konfiguracji pakietu instalacyjnego.

Podczas uruchamiania procesu setup.exe z katalogu głównego pakietu instalacyjnego, pakiet zostanie najpierw skopiowany do tymczasowego folderu lokalnego, a następnie instalator aplikacji zostanie uruchomiony z folderu lokalnego.

Zdalna instalacja aplikacji na urządzeniach z zainstalowanym Agentem sieciowym

Jeśli na urządzeniu jest zainstalowany działający Agent sieciowy, połączony z głównym Serwerem administracyjnym (lub jednym z jego Serwerów podrzędnych), możesz zaktualizować Agenta sieciowego na tym urządzeniu, a także zainstalować, zaktualizować lub usunąć dowolne obsługiwane aplikacje poprzez Agenta sieciowego.

Możesz włączyć tę opcję, zaznaczając pole **Przy użyciu Agenta sieciowego** we właściwościach zadania zdalnej instalacji.

Jeśli to pole jest zaznaczone, pakiety instalacyjne z ustawieniami instalacji, zdefiniowanymi przez administratora, zostaną przesłane na urządzenia docelowe poprzez kanały komunikacyjne między Agentem sieciowym a Serwerem administracyjnym.

Aby zoptymalizować obciążenie na Serwerze administracyjnym oraz zminimalizować ruch pomiędzy Serwerem administracyjnym a urządzeniami, należy wskazać punkty dystrybucji w każdej sieci zdalnej lub domenie rozgłoszeniowej (sekcja Informacje o punktach dystrybucji oraz sekcja Tworzenie struktury grup administracyjnych i przydzielanie punktów dystrybucji). W tym przypadku pakiety instalacyjne oraz ustawienia instalatora są rozsyłane z Serwera administracyjnego na urządzenia docelowe poprzez punkty dystrybucji.

Co więcej, możliwe jest użycie punktów dystrybucji do transmisyjnego (multiemisja) dostarczania pakietów instalacyjnych, co pozwala znacząco zmniejszyć ruch sieciowy podczas zdalnej instalacji aplikacji.

Podczas wysyłania pakietów instalacyjnych na urządzenia docelowe poprzez kanały komunikacyjne między Agentami sieciowymi a Serwerem administracyjnym, wszystkie pakiety instalacyjne, które zostały przygotowane do wysłania, zostaną także zbuforowane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Jeśli używanych jest kilka dużych pakietów instalacyjnych różnych typów oraz wykorzystywana jest duża liczba punktów dystrybucji, rozmiar tego folderu może drastycznie się powiększyć.

Nie można ręcznie usunąć plików z folderu FTServer. Jeśli oryginalne pakiety instalacyjne zostaną usunięte, odpowiednie dane zostaną automatycznie usunięte z folderu FTServer.

Wszystkie dane otrzymane po stronie punktów dystrybucji są zapisywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Nie można ręcznie usunąć plików z folderu $FTCITmp. Po zakończeniu działania zadań korzystających z danych z tego folderu, jego zawartość zostanie automatycznie usunięta.

Ponieważ pakiety instalacyjne są rozsyłane poprzez kanały komunikacyjne między Serwerem administracyjnym a Agentami sieciowymi z repozytorium pośredniczącego w formacie zoptymalizowanym dla transferów sieciowych, nie można wprowadzać żadnych zmian w pakietach instalacyjnych, przechowywanych w oryginalnym folderze każdego pakietu instalacyjnego. Takie zmiany nie zostałyby automatycznie zarejestrowane przez Serwer administracyjny. Jeśli chcesz ręcznie zmodyfikować pliki pakietów instalacyjnych (chociaż zalecane jest unikanie takiego rozwiązania), należy zmodyfikować dowolne ustawienia pakietu instalacyjnego w Konsoli administracyjnej. Zmodyfikowanie ustawień pakietu instalacyjnego w Konsoli administracyjnej spowoduje, że Serwer administracyjny zaktualizuje obraz pakietu w pamięci podręcznej, który został przygotowany do przesłania na urządzenia docelowe.

Zarządzanie ponownym uruchamianiem urządzeń w zadaniu zdalnej instalacji

Aby zakończyć zdalną instalację aplikacji, często wymagane jest ponowne uruchomienie urządzeń (szczególnie w systemie Windows).

Jeśli korzystasz z zadania zdalnej instalacji z Kaspersky Security Center, w Kreatorze tworzenia nowego zadania lub w oknie właściwości zadania, które zostało utworzone (sekcja **Ponowne uruchomienie systemu operacyjnego**), możesz wybrać akcję, która zostanie wykonana, gdy urządzenie z systemem Windows wymaga ponownego uruchomienia:

- **Nie uruchamiaj ponownie urządzenia**. W tym przypadku komputer nie zostanie automatycznie uruchomiony ponownie. Aby zakończyć instalację, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań instalacji na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**. W tym przypadku urządzenie jest zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia instalacji. Opcja jest przydatna, gdy zadania instalacji są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**. W tym przypadku, na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Opcja **Pytaj użytkownika o akcję** jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia komputera.

Aktualizowanie baz danych w pakiecie instalacyjnym aplikacji antywirusowej

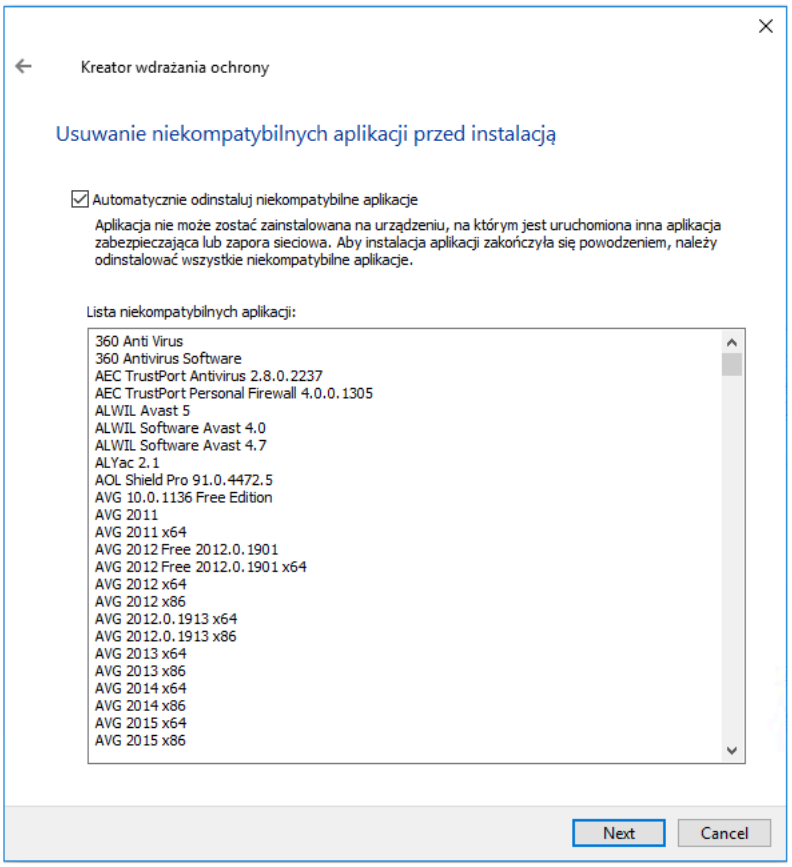
Przed rozpoczęciem wdrażania ochrony należy pamiętać o możliwości aktualizacji antywirusowych baz danych (w tym modułów i łat), dostarczanych wraz z pakietem dystrybucyjnym aplikacji zabezpieczającej. Dobrym rozwiązaniem jest zaktualizowanie baz danych w pakiecie instalacyjnym aplikacji przed rozpoczęciem wdrożenia (na przykład przy użyciu odpowiedniego polecenia z menu kontekstowego wybranego pakietu instalacyjnego). Zmniejszy to liczbę ponownych uruchomień wymaganych do zakończenia wdrożenia ochrony na urządzeniach docelowych. Jeśli zdalna instalacja wykorzystuje pakiety instalacyjne, które zostały przekazane do Serwerów wirtualnych z głównego Serwera administracyjnego, należy tylko zaktualizować bazy danych w oryginalnym pakiecie na Serwerze głównym. W tym przypadku nie ma konieczności aktualizowania baz danych w przekazanych pakietach na Serwerach wirtualnych.

Usuwanie niekompatybilnych aplikacji zabezpieczających firm trzecich

Instalacja aplikacji zabezpieczających firmy Kaspersky poprzez Kaspersky Security Center może wymagać usunięcia oprogramowania firmy trzeciej niekompatybilnego z instalowaną aplikacją. Istnieją dwa sposoby odinstalowania aplikacji innych firm.

Automatyczne usuwanie niekompatybilnych aplikacji przy użyciu instalatora

Po uruchomieniu instalatora wyświetla listę aplikacji, które nie są kompatybilne z aplikacją firmy Kaspersky:



Lista niekompatybilnych aplikacji wyświetlana w Kreatorze zdalnej instalacji

Kaspersky Security Center wykrywa niekompatybilne oprogramowanie. W związku z tym możesz zaznaczyć pole wyboru **Automatycznie odinstaluj niekompatybilne aplikacje**, aby kontynuować instalację. Jeśli usuniesz to pole wyboru i nie odinstalujesz niekompatybilnego oprogramowania, wystąpi błąd i aplikacja Kaspersky nie zostanie zainstalowana.

Automatyczne usuwanie niekompatybilnych aplikacji jest obsługiwane przez różne typy instalacji.

Dezinstalowanie niekompatybilnych aplikacji przy użyciu dedykowanego zadania

Aby usunąć niekompatybilne aplikacje, użyj zadania *Zdalna dezinstalacja aplikacji* Zadanie to powinno być uruchomione na urządzeniach przed zadaniem instalacji aplikacji zabezpieczającej. Na przykład, w zadaniu instalacji możesz wybrać opcję terminarza **Po zakończeniu wykonywania innego zadania**, gdzie inne zadanie to *Zdalna dezinstalacja aplikacji*

Ta metoda dezinstalacji jest przydatna, jeśli instalator aplikacji zabezpieczającej nie może skutecznie usunąć niekompatybilnej aplikacji.

Usuwanie Agenta sieciowego chronionego hasłem za pomocą wiersza poleceń

Aby zdalnie odinstalować Agenta sieciowego, dla którego ustawiłeś hasło dezinstalacyjne, możesz skorzystać z wiersza poleceń.

Jeśli zgubisz lub zapomnisz hasła do chronionego hasłem Agenta sieciowego zainstalowanego na urządzeniu, które nie jest już zarządzane przez Kaspersky Security Center, nie będziesz mógł usunąć Agenta sieciowego przy użyciu narzędzia klmover, narzędzia Cleaner (cleaner.exe) ani wiersza poleceń. W takim przypadku należy ponownie zainstalować system operacyjny na urządzeniu z zainstalowanym Agentem sieciowym chronionym hasłem.

Aby odinstalować Agenta sieciowego za pomocą wiersza poleceń:

1. Przekształć swoje hasło dezinstalacyjne w kod szesnastkowy.

   Skorzystaj z zasobów internetowych, środowiska programistycznego, edytora tekstu lub innego odpowiedniego narzędzia, aby zamienić swoje hasło na kod szesnastkowy.

   Upewnij się, że ogranicznik wyjściowy używany do rozdzielenia wygenerowanego kodu szesnastkowego na części jest ustawiony na `00`. Na przykład kod szesnastkowy `51 77 65 72 74 79` jest niepoprawny, a kod szesnastkowy `5100770065007200740079 00` jest poprawny.

2. Wpisz następujące polecenie w wierszu poleceń i naciśnij **ENTER**:

   ```
   msiexec.exe /x{<product code>} /qn KLUNINSTPASSWD=<hex code of your uninstallation password>
   ```

   Kod produktu swojego Agenta sieciowego możesz znaleźć w poniższej tabeli.

Kody produktów Agenta sieciowego

Lokalizacja	Kod produktu
arabskim	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}
bułgarskim	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
czeskim	{478A6A0B-D177-4402-B703-808C05C56B13}
angielskim	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
francuskim	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
niemieckim	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
węgierskim	{8899A4D4-D678-49F8-AD96-0B784F58D355}
włoskim	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
japońskim	{790C176F-7780-4C84-8B9C-455F5C0E61C5}
koreańskim	{70812A40-973B-4DA1-96B9-C2011280CD99}
polskim	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
portugalskim	{0F05E4E5-5A89-482C-9A62-47CC58643788}
rumuńskim	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
rosyjskim	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}
Chiński uproszczony	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}

hiszpańskim	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
hiszpańskim-mx	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}
Chiński tradycyjny	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
tureckim	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

Korzystanie z narzędzi do zdalnej instalacji aplikacji z Kaspersky Security Center do uruchamiania odpowiednich plików wykonywalnych na zarządzanych urządzeniach

Korzystając z Kreatora tworzenia nowego pakietu, możesz wybrać dowolny plik wykonywalny i zdefiniować dla niego ustawienia wiersza poleceń. W tym celu należy dodać do pakietu instalacyjnego sam wybrany plik lub cały folder, w którym ten plik się znajduje. Następnie konieczne jest utworzenie zadania zdalnej instalacji i wybranie utworzonego pakietu instalacyjnego.

Podczas wykonywania zadania, na urządzeniach docelowych zostanie uruchomiony określony plik wykonywalny ze zdefiniowanymi ustawieniami wiersza poleceń.

Jeśli używasz instalatorów w formacie Microsoft Windows Installer (MSI), Kaspersky Security Center przeanalizuje wyniki instalacji przy użyciu standardowych narzędzi.

Jeśli dostępna jest licencja Zarządzania lukami i poprawkami, Kaspersky Security Center (podczas tworzenia pakietu instalacyjnego dla dowolnej obsługiwanej aplikacji w środowisku korporacyjnym) użyje także reguł do zainstalowania i przeanalizowania wyników instalacji, które znajdują się w jego aktualizowanej bazie danych.

W innym przypadku domyślne zadanie dla plików wykonywalnych poczeka na zakończenie uruchomionych procesów i wszystkich jego procesów podrzędnych. Po zakończeniu wszystkich uruchomionych procesów, zadanie zostanie zakończone pomyślnie niezależnie od kodu zwrotnego procesu instalacji. Aby zmienić takie zachowanie tego zadania, przed utworzeniem zadania należy ręcznie zmodyfikować pliki .kpd, które zostały wygenerowane przez Kaspersky Security Center w folderze nowo utworzonego pakietu instalacyjnego i jego podfolderach.

Pliki .kpd używają kodowania ASCII. Pliki .kud używają kodowania Unicode.

Aby zadanie nie czekało na zakończenie uruchomionych procesów, w sekcji [SetupProcessResult] ustaw wartość ustawienia Wait na 0:

```
[SetupProcessResult]
Wait=0
```

Aby zadanie czekało tylko na zakończenie uruchomionych procesów w systemie Windows, a nie na zakończenie procesów podrzędnych, w sekcji [SetupProcessResult] ustaw wartość ustawienia WaitJob na 0, na przykład:

```
[SetupProcessResult]
WaitJob=0
```

Aby zadanie zostało pomyślnie ukończone lub zwróciło błąd, w zależności od kodu zwrotnego uruchomionego procesu, utwórz plik wykonywalny .bat, który zapisze kod błędu do pliku, na przykład:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
```

```
exit 0
```

Następnie zmodyfikuj pliki .kud wygenerowane przez Kaspersky Security Center w folderze nowo utworzonego pakietu instalacyjnego:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

W tym przypadku każdy kod inny niż te znajdujące się na liście będzie zwracany jako błąd.

W celu wyświetlenia wiersza z komentarzem na temat pomyślnego zakończenia zadania lub błędu w wynikach zadania, w sekcji [SetupProcessResult_SuccessCodes] i [SetupProcessResult_ErrorCodes] wpisz krótki opis błędów odpowiadających kodom zwrotnym procesu, na przykład:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A restart is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation canceled by the user
1603=Fatal error during installation
```

W celu użycia narzędzi Kaspersky Security Center do zarządzania ponownym uruchomieniem urządzenia (jeśli ponowne uruchomienie jest wymagane do zakończenia działania), w sekcji [SetupProcessResult_NeedReboot] umieść listę kodów zwrotnych procesu, które wskazują na konieczność ponownego uruchomienia komputera:

```
[SetupProcessResult_NeedReboot]
3010=
```

Monitorowanie wdrożenia

W celu monitorowania instalacji Kaspersky Security Center oraz upewnienia się, że aplikacja zabezpieczająca i Agent sieciowy są zainstalowane na zarządzanych urządzeniach należy sprawdzić wskaźnik w sekcji **Wdrażanie**. Wskaźnik ten zlokalizowany jest w obszarze roboczym węzła Serwera administracyjnego w oknie głównym Konsoli administracyjnej. Kolory wskaźnika odzwierciedlają bieżący stan zdalnej instalacji. Obok wskaźnika wyświetlana jest liczba urządzeń, na których jest zainstalowany Agent sieciowy i aplikacje zabezpieczające. Jeśli uruchomione są jakiekolwiek zadania instalacji, postęp ich wykonania możesz monitorować w tym miejscu. Jeśli wystąpią jakiekolwiek błędy instalacyjne, liczba błędów zostanie wyświetlona w tym miejscu. Szczegóły dotyczące błędów można wyświetlić, klikając odnośnik.

Możesz także wykorzystać schemat zdalnej instalacji z obszaru roboczego folderu **Zarządzane urządzenia** na zakładce **Grupy**. Wykres odzwierciedla proces zdalnej instalacji i wyświetla liczbę urządzeń bez Agenta sieciowego, z Agentem sieciowym lub z Agentem sieciowym i aplikacją zabezpieczającą.

Więcej informacji o postępie wykonania zdalnej instalacji (lub działaniu określonego zadania instalacji) można uzyskać, otwierając okno wyników odpowiedniego zadania zdalnej instalacji: Kliknij zadanie prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wyniki**. Okno będzie wyświetlało dwie listy: górna lista zawiera stany zadania na urządzeniach, natomiast dolna lista zawiera zdarzenia zadania na urządzeniu, które jest aktualnie wybrane na górnej liście.

Informacje o błędach zdalnej instalacji zostaną dodane do dziennika zdarzeń aplikacji Kaspersky na Serwerze administracyjnym. Informacje o błędach są także dostępne w odpowiednim wyborze zdarzeń, w folderze **Raporty i powiadomienia**, w podfolderze **Zdarzenia**.

Konfigurowanie instalatorów

Ta sekcja zawiera informacje na temat plików instalatorów Kaspersky Security Center i ustawień instalacji, a także zalecenia dotyczące instalacji Serwera administracyjnego i Agenta sieciowego w trybie cichym.

Informacje ogólne

Instalatory komponentów Kaspersky Security Center 15.1 (Serwer administracyjny, Agent sieciowy i Konsola administracyjna) bazują na technologii Instalatora Windows. Pakiet MSI jest podstawą instalatora. Ten format pakietów umożliwia wykorzystanie wszystkich korzyści oferowanych przez Instalator Windows: skalowalność, dostępność systemu poprawek, system transformacji, scentralizowana instalacja za pośrednictwem rozwiązań firm trzecich oraz niewidoczna rejestracja w systemie operacyjnym.

Instalacja w trybie cichym (z plikiem odpowiedzi)

Instalatory Serwera administracyjnego i Agenta sieciowego mogą pracować z plikiem odpowiedzi (ss_install.xml), w którym zintegrowane są parametry instalacji w trybie cichym bez udziału użytkownika. Plik ss_install.xml znajduje się w tym samym folderze co pakiet MSI. Jest on używany automatycznie podczas instalacji w trybie cichym. Możesz włączyć tryb cichej instalacji z użyciem klucza „/s" wiersza polecenia.

Na przykład:

```
setup.exe /s
```

Przed uruchomieniem instalatora w trybie cichym przeczytaj Umowę licencyjną użytkownika końcowego (EULA). Jeśli pakiet dystrybucyjny Kaspersky Security Center nie zawiera pliku TXT z treścią Umowy licencyjnej użytkownika końcowego, możesz pobrać ten plik ze strony internetowej Kaspersky.

Plik ss_install.xml jest wewnętrznym formatem parametrów instalatora Kaspersky Security Center. Pakiety dystrybucyjne zawierają plik ss_install.xml z domyślnymi parametrami.

Nie należy ręcznie modyfikować pliku ss_install.xml. Ten plik może być modyfikowany tylko przy użyciu narzędzi Kaspersky Security Center podczas edytowania parametrów pakietów instalacyjnych w Konsoli administracyjnej.

W celu zmodyfikowania pliku odpowiedzi dla instalacji Serwera administracyjnego:

1. Otwórz pakiet dystrybucyjny Kaspersky Security Center. Jeśli używasz pełnego pakietu pliku EXE, rozpakuj go.
2. Utwórz folder Serwer, otwórz wiersz polecenia, a następnie uruchom następujące polecenie:

   ```
   setup.exe /r ss_install.xml
   ```

   Plik instalacyjny Kaspersky Security Center uruchomi się.
3. Postępuj zgodnie z instrukcjami kreatora, aby skonfigurować instalację Kaspersky Security Center.

Po zakończeniu działania kreatora plik odpowiedzi jest automatycznie modyfikowany zgodnie z nowymi ustawieniami określonymi przez użytkownika.

Instalacja Agenta sieciowego w trybie cichym (bez pliku odpowiedzi)

Agenta sieciowego można zainstalować przy użyciu jednego pakietu .msi, określając wartości właściwości MSI w standardowy sposób. Ten scenariusz umożliwia zainstalowanie Agenta sieciowego przy użyciu zasad grupy.

Nie zmieniaj nazwy pakietu instalacyjnego Kaspersky Network Agent.msi. Zmiana nazwy tego pakietu może spowodować błędy instalacji podczas przyszłych aktualizacji Agenta sieciowego.

Aby uniknąć konfliktów pomiędzy parametrami zdefiniowanymi poprzez właściwości MSI a parametrami zdefiniowanymi w pliku odpowiedzi, możesz wyłączyć plik odpowiedzi, ustawiając właściwość `DONT_USE_ANSWER_FILE=1`. Plik MSI znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center, w folderze Packages\NetAgent\exec. Poniżej znajduje się przykład uruchomienia instalatora Agenta sieciowego z pakietem .msi.

Instalacja Agenta sieciowego w trybie cichym wymaga akceptacji warunków Umowy Licencyjnej Użytkownika Końcowego. Użyj parametru `EULA=1` tylko wtedy, gdy w pełni przeczytałeś, zrozumiałeś i zaakceptowałeś warunki Umowy licencyjnej użytkownika końcowego.

Na przykład:

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Możliwe jest także zdefiniowanie parametrów instalacji dla pakietu .msi poprzez wcześniejsze przygotowanie pliku odpowiedzi (z rozszerzeniem .mst). To polecenie wygląda następująco:

Na przykład:

```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

W jednym poleceniu można określić kilka plików odpowiedzi.

Jeśli chcesz uaktualnić Agenta sieciowego za pomocą Instalatora Windows, uruchom następujące polecenie:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Częściowa konfiguracja instalacji poprzez setup.exe

Podczas uruchamiania instalacji aplikacji z pliku setup.exe, do pakietu MSI możesz dodać wartości dowolnych właściwości MSI.

To polecenie wygląda następująco:

Na przykład:
`/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"`

Parametry instalacji Serwera administracyjnego

Poniższa tabela opisuje właściwości MSI, które można skonfigurować podczas instalacji Serwera administracyjnego. Wszystkie parametry są opcjonalne, za wyjątkiem EULA i PRIVACYPOLICY.

Parametry instalacji Serwera administracyjnego w trybie cichym

Właściwość MSI	Opis	Dostępne wartości
Umowa licencyjna użytkownika końcowego	Akceptacja postanowień i warunków Umowy licencyjnej (wymagana)	• 1—W pełni przeczytałem, rozumiem i akceptuję warunki Umowy licencyjnej. • Inna wartość lub brak wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
PRIVACYPOLICY	Akceptacja postanowień i warunków Polityki prywatności (wymagana)	• 1—Jestem świadomy i wyrażam zgodę na przetwarzanie oraz przesyłanie moich danych (również do innych krajów) zgodnie z Polityką prywatności. Potwierdzam, że w pełni przeczytałem(am) i rozumiem Politykę prywatności. • Inna wartość lub bez wartości — Nie akceptuję postanowień i warunków Polityki prywatności (instalacja nie zostanie wykonana).
INSTALLATIONMODETYPE	Typ instalacji Serwera administracyjnego	• Standardowa. • Niestandardowa.
INSTALLDIR	Folder instalacyjny aplikacji	Wartość wiersza.
ADDLOCAL	Lista komponentów przeznaczonych do zainstalowania (oddzielone przecinkami)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Minimalna lista komponentów wystarczających do poprawnego zainstalowania Serwera administracyjnego: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Rozmiar sieci	• NRT_1_100 — od 1 do 100 urządzeń. • NRT_100_1000 — od 101 do 1000 urządzeń. • NRT_GREATER_1000 — więcej niż 1000 urządzeń.
SRV_ACCOUNT_TYPE	Sposób określania użytkownika dla działania usługi Serwera administracyjnego	• SrvAccountDefault—konto użytkownika zostanie utworzone automatycznie • SrvAccountUser—konto użytkownika jest określane ręcznie
SERVERACCOUNTNAME	Nazwa użytkownika dla usługi	Wartość wiersza.
SERVERACCOUNTPWD	Hasło użytkownika dla usługi	Wartość wiersza.
DBTYPE	Typ bazy danych	• MySQL—używana będzie baza danych MySQL lub MariaDB. • MSSQL—używana będzie baza danych Microsoft SQL Server (SQL Express).
MYSQLSERVERNAME	Pełna nazwa serwera MySQL lub MariaDB	Wartość wiersza.
MYSQLSERVERPORT	Numer portu używanego do nawiązania połączenia z serwerem MySQL lub MariaDB	Wartość numeryczna.
MYSQLDBNAME	Nazwa bazy danych serwera MySQL lub MariaDB	Wartość wiersza.
MYSQLACCOUNTNAME	Nazwa użytkownika nawiązującego połączenie z bazą danych serwera MySQL lub MariaDB	Wartość wiersza.

Właściwość MSI	Opis	Dostępne wartości
MYSQLACCOUNTPWD	Hasło użytkownika nawiązującego połączenie z bazą danych serwera MySQL lub MariaDB	Wartość wiersza.
MSSQLCONNECTIONTYPE	Sposób użycia bazy danych MSSQL	• InstallMSSEE—instalacja z pakietu • ChooseExisting—użycie zainstalowanego serwera
MSSQLSERVERNAME	Pełna nazwa instancji serwera SQL	Wartość wiersza.
MSSQLDBNAME	Nazwa bazy danych serwera SQL	Wartość wiersza.
MSSQLAUTHTYPE	Metoda autoryzacji podczas nawiązywania połączenia z serwerem SQL	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Nazwa użytkownika nawiązującego połączenie z serwerem SQL w trybie SQLServer	Wartość wiersza.
MSSQLACCOUNTPWD	Hasło użytkownika nawiązującego połączenie z serwerem SQL w trybie SQLServer	Wartość wiersza.
CREATE_SHARE_TYPE	Metoda określania folderu współdzielonego	• Create—tworzy nowy folder współdzielony. W takim przypadku należy zdefiniować następujące właściwości: • SHARELOCALPATH—ścieżka dostępu do folderu lokalnego. • SHAREFOLDERNAME—nazwa sieciowa folderu. • Null—należy określić właściwość EXISTSHAREFOLDERNAME.
EXISTSHAREFOLDERNAME	Pełna ścieżka dostępu do istniejącego folderu współdzielonego	Wartość wiersza.
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	Wartość numeryczna.
SERVERSSLPORT	Numer portu używanego do nawiązania bezpiecznego połączenia SSL z Serwerem administracyjnym	Wartość numeryczna.
SERVERADDRESS	Adres Serwera administracyjnego	Wartość wiersza.
SERVERCERT2048BITS	Długość klucza certyfikatu Serwera administracyjnego (bity)	• 1—długość klucza certyfikatu Serwera administracyjnego wynosi 2048 bity. • 0 — długość klucza certyfikatu Serwera administracyjnego wynosi 1024 bity. • Jeśli nie określono wartości, długość klucza certyfikatu Serwera administracyjnego wynosi 2048 bity.
MOBILESERVERADDRESS	Adres Serwera administracyjnego do nawiązywania połączenia z urządzeniami mobilnymi; ignorowane, jeśli nie wybrano komponentu MobileSupport	Wartość wiersza.

Ustawienia pakietu instalacyjnego Agenta sieciowego

Poniższa tabela opisuje właściwości MSI, które można skonfigurować podczas instalacji Agenta sieciowego. Wszystkie parametry są opcjonalne, za wyjątkiem SERVERADDRESS.

Właściwości MSI

Właściwość MSI	Opis	Dostępne wartości
DONT_USE_ANSWER_FILE	Odczyt ustawień instalacji z pliku odpowiedzi	• 1 • Null
INSTALLDIR	Folder instalacyjny	
SERVERADDRESS	Adres Serwera administracyjnego (wymagane)	
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	

Właściwość MSI	Opis	Dostępne wartości
SERVERSSLPORT	Numer portu dla połączenia SSL	
USESSL	Czy użyć połączenia SSL	• 1 • Null
OPENUDPPORT	Czy otworzyć port UDP	• 1 • Null
UDPPORT	Numer portu UDP	
USEPROXY	Czy użyć serwera proxy	• 1 • Null
PROXYADDRESS	Adres Proxy	
PROXYPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	
PROXYLOGIN	Konto używane do nawiązywania połączenia z serwerem proxy	
PROXYPASSWORD	Hasło konta używanego do nawiązania połączenia z serwerem proxy. W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.	
GATEWAYMODE	Tryb użycia bramy połączenia	• 0 — nie używaj bramy połączenia • 1 — użyj tego Agenta sieciowego jako bramy połączenia • 2 — połącz z Serwerem administracyjnym przy użyciu bramy połączenia
GATEWAYADDRESS	Adres bramy połączenia	
CERTSELECTION	Metoda pobierania certyfikatu	• GetOnFirstConnection — uzyskaj certyfikat z Serwera administracyjnego. • GetExistent — wybierz istniejący certyfikat. Jeżeli ta opcja jest zaznaczona, właściwość CERTFILE musi być zdefiniowana.
CERTFILE	Ścieżka do pliku certyfikatu	
VMVDI	Włącz tryb dynamiczny dla VDI	• 1 • Null
LAUNCHPROGRAM	Czy uruchomić usługę Agenta sieciowego po instalacji	• 1 • Null

Infrastruktura wirtualna

Kaspersky Security Center obsługuje użycie maszyn wirtualnych. Możesz zainstalować Agenta sieciowego i aplikację zabezpieczającą na każdej maszynie wirtualnej, a także wdrożyć ochronę maszyn wirtualnych na poziomie hipernadzorcy. W pierwszym przypadku, do ochrony maszyn wirtualnych możesz użyć standardowej aplikacji zabezpieczającej lub Kaspersky Security for Virtualization Light Agent. W drugim przypadku możesz użyć Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center obsługuje przywracanie maszyn wirtualnych do ich poprzedniego stanu.

Wskazówki dotyczące zmniejszenia obciążenia na maszynach wirtualnych

Podczas instalacji Agenta sieciowego na maszynie wirtualnej zalecane jest rozważenie wyłączenia funkcji Kaspersky Security Center, które nie będą zbyt przydatne dla maszyn wirtualnych.

Podczas instalacji Agenta sieciowego na maszynie wirtualnej lub na szablonie przeznaczonym do wygenerowania maszyn wirtualnych, zalecane jest wykonanie następujących czynności:

- Jeśli uruchamiasz zdalną instalację, w oknie właściwości pakietu instalacyjnego Agenta sieciowego, w sekcji **Zaawansowane** zaznacz opcję **Optymalizuj ustawienia dla VDI**.
- Jeśli uruchamiasz instalację w trybie interaktywnym z udziałem kreatora, w oknie kreatora zaznacz opcję **Optymalizuj ustawienia Agenta sieciowego dla infrastruktury wirtualnej**.

Zaznaczenie tych opcji spowoduje zmianę ustawień Agenta sieciowego w taki sposób, że poniższe funkcje pozostaną domyślnie wyłączone (przed zastosowaniem zasady):

- Zbieranie informacji o zainstalowanym oprogramowaniu
- Zbieranie informacji o sprzęcie
- Zbieranie informacji o wykrytych lukach
- Zbieranie informacji o wymaganych aktualizacjach

Zazwyczaj te funkcje nie są potrzebne na maszynach wirtualnych, gdyż wykorzystują stałe oprogramowanie i sprzęt wirtualny.

Wyłączenie tych funkcji jest odwracalne. Jeśli jakakolwiek z wyłączonych funkcji jest potrzebna, możesz ją włączyć poprzez zasadę Agenta sieciowego lub poprzez ustawienia lokalne Agenta sieciowego. Ustawienia lokalne Agenta sieciowego są dostępne poprzez menu kontekstowe odpowiedniego urządzenia w Konsoli administracyjnej.

Obsługa dynamicznych maszyn wirtualnych

Kaspersky Security Center obsługuje dynamiczne maszyny wirtualne. Jeśli w sieci organizacji została wdrożona infrastruktura wirtualna, w pewnych przypadkach możliwe będzie korzystanie z dynamicznych (tymczasowych) maszyn wirtualnych. Dynamiczne maszyny wirtualne są tworzone pod unikatowymi nazwami w oparciu o szablony, które zostały przygotowane przez administratora. Użytkownik pracuje na maszynie wirtualnej przez jakiś czas, a następnie, po wyłączeniu maszyny zostanie ona usunięta z infrastruktury wirtualnej. Jeśli w sieci organizacji jest zainstalowany program Kaspersky Security Center, maszyna wirtualna z zainstalowanym Agentem sieciowym zostanie dodana do bazy danych Serwera administracyjnego. Po wyłączeniu maszyny wirtualnej, odpowiedni wpis musi także zostać usunięty z bazy danych Serwera administracyjnego.

Aby funkcja automatycznego usuwania wpisów na temat maszyn wirtualnych mogła działać, podczas instalacji Agenta sieciowego na szablonie dla dynamicznych maszyn wirtualnych wybierz opcję **Włącz tryb dynamiczny VDI**:

- Dla zdalnej instalacji—w oknie właściwości pakietu instalacyjnego Agenta sieciowego (sekcja **Zaawansowane**)
- Dla instalacji w trybie interaktywnym—w Kreatorze instalacji Agenta sieciowego

Staraj się unikać zaznaczania opcji **Włącz tryb dynamiczny VDI** podczas instalacji Agenta sieciowego na urządzeniach fizycznych.

Jeśli chcesz, żeby zdarzenia z dynamicznych maszyn wirtualnych były przechowywane na Serwerze administracyjnym przez jakiś czas po usunięciu tych maszyn wirtualnych, w oknie właściwości Serwera administracyjnego, w sekcji **Repozytorium zdarzeń** wybierz opcję **Przechowuj zdarzenia po usunięciu urządzeń** i określ maksymalny czas przechowywania zdarzeń (w dniach).

Nie zalecamy włączania szyfrowania dysku na dynamicznych maszynach wirtualnych.

Obsługa kopiowania maszyn wirtualnych

Kopiowanie maszyn wirtualnych z zainstalowanym Agentem sieciowym lub tworzenie maszyny wirtualnej z szablonu z zainstalowanym Agentem sieciowym odbywa się w ten sam sposób co zdalna instalacja Agenta sieciowego poprzez przechwycenie i skopiowanie obrazu dysku twardego. Oznacza to, że podczas kopiowania maszyn wirtualnych należy wykonać te same czynności, co podczas instalacji Agenta sieciowego poprzez skopiowanie obrazu dysku.

Jednakże dwa poniższe przypadki przedstawiają sytuacje, gdy Agent sieciowy automatycznie wykrywa kopiowanie. Dzięki temu nie ma potrzeby wykonywania wszystkich skomplikowanych działań wymienionych w sekcji "Wdrożenie poprzez przechwycenie i skopiowanie obrazu dysku twardego urządzenia":

- Opcja **Włącz tryb dynamiczny VDI** została wybrana po zainstalowaniu Agenta sieciowego - po każdym ponownym uruchomieniu systemu operacyjnego ta maszyna wirtualna będzie rozpoznawana jako nowe urządzenie, niezależnie od tego, czy została skopiowana.
- Używany jest jeden z następujących hipernadzorców: VMware™, HyperV® lub Xen®: Agent sieciowy wykrywa kopiowanie maszyny wirtualnej po zmienionych numerach ID sprzętu wirtualnego.

Analiza zmian w sprzęcie wirtualnym nie jest całkowicie wiarygodna. Przed szerszym zastosowaniem tej metody należy ją sprawdzić na małej puli maszyn wirtualnych dla wersji hipernadzorcy, który jest aktualnie używany w organizacji.

Obsługa przywracania systemu plików dla urządzeń z zainstalowanym Agentem sieciowym

Kaspersky Security Center jest aplikacją oferującą wiele funkcji. Przywrócenie poprzedniego stanu systemu plików na urządzeniu z zainstalowanym Agentem sieciowym doprowadzi do desynchronizacji danych i niepoprawnego działania Kaspersky Security Center.

Wycofanie systemu plików (lub jego części) może zostać wykonane w następujących przypadkach:

- Podczas kopiowania obrazu dysku twardego.
- Podczas przywracania stanu maszyny wirtualnej przy użyciu infrastruktury wirtualnej.
- Podczas przywracania danych z kopii zapasowej lub punktu odzyskiwania.

Scenariusze, w których oprogramowanie firm trzecich na urządzeniach z zainstalowanym Agentem sieciowym wpływa na zawartość folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\, są dla Kaspersky Security Center tylko krytycznymi scenariuszami. Dlatego też, jeśli to tylko możliwe, powinieneś zawsze wykluczać ten folder z procedury odzyskiwania.

Ponieważ zasady działania niektórych organizacji dopuszczają możliwość wycofania systemu plików urządzeń, obsługa wycofania systemu plików na urządzeniach z zainstalowanym Agentem sieciowym jest dostępna w Kaspersky Security Center od wersji 10 Maintenance Release 1 (Serwer administracyjny i Agenty sieciowe muszą być w wersjach 10 Maintenance Release 1 lub nowszych). Po wykryciu takich urządzeń są one automatycznie ponownie łączone z Serwerem administracyjnym z całkowitym wyczyszczeniem danych i pełną synchronizacją.

Domyślnie obsługa wykrywania wycofania systemu plików jest włączona w Kaspersky Security Center 15.1.

Jeśli jest to tylko możliwe, unikaj przywracania poprzedniego stanu folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ na urządzeniach z zainstalowanym Agentem sieciowym, gdyż całkowita ponowna synchronizacja danych zużywa dużą ilość zasobów.

Wycofanie stanu systemu jest całkowicie zabronione na urządzeniu z zainstalowanym Serwerem administracyjnym. Podobnie jest w przypadku wycofania baz danych używanych przez Serwer administracyjny.

Możesz przywrócić stan Serwera administracyjnego z kopii zapasowej tylko przy użyciu standardowego narzędzia klbackup.

Informacje o profilach połączenia dla użytkowników mobilnych

Mobilni użytkownicy laptopów (zwanych dalej również "urządzeniami") mogą potrzebować zmiany metody łączenia się z Serwerem administracyjnym lub przełączania pomiędzy Serwerami administracyjnymi w zależności od aktualnej lokalizacji urządzenia w sieci firmowej.

Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows i macOS.

Używanie różnych adresów jednego Serwera administracyjnego

Urządzenia z zainstalowanym Agentem sieciowym mogą łączyć się z Serwerem administracyjnym z poziomu wewnętrznej sieci organizacji lub internetu. W tej sytuacji wymagane może być, aby Agent sieciowy używał innych adresów do łączenia się z Serwerem administracyjnym: zewnętrznego adresu Serwera administracyjnego dla połączenia internetowego oraz wewnętrznego adresu Serwera administracyjnego dla wewnętrznego połączenia sieciowego.

W tym celu musisz dodać profil (dla połączenia z Serwerem administracyjnym z poziomu internetu) do zasady Agenta sieciowego. Dodaj profil we właściwościach zasady (sekcja **Łączność**, podsekcja **Profile połączenia**). W oknie tworzenia profilu należy wyłączyć opcję **Użyj tylko do pobierania uaktualnień** oraz wybrać opcję **Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu**. Jeśli do łączenia się z Serwerem administracyjnym używasz bramy połączenia (na przykład, w konfiguracji Kaspersky Security Center, opisanej w sekcji Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej), w odpowiednim polu profilu połączenia musisz określić adres bramy połączenia.

Przełączanie pomiędzy Serwerami administracyjnymi w zależności od aktualnej sieci

Jeśli organizacja posiada kilka biur z różnymi Serwerami administracyjnymi, a niektóre urządzenia z zainstalowanym Agentem sieciowym są przenoszone pomiędzy nimi, Agent sieciowy musi łączyć się z Serwerem administracyjnym sieci lokalnej w biurze, w którym znajduje się urządzenie.

W tej sytuacji konieczne jest utworzenie profilu dla połączenia z Serwerem administracyjnym we właściwościach zasady Agenta sieciowego dla każdego z biur, za wyjątkiem głównego biura, w którym znajduje się oryginalny macierzysty Serwer administracyjny. W profilach połączenia należy określić adresy Serwerów administracyjnych i włączyć lub wyłączyć opcję **Użyj tylko do pobierania uaktualnień**:

- Wybierz tę opcję, jeśli chcesz, aby Agent sieciowy zsynchronizował się z macierzystym Serwerem administracyjnym, a Serwer lokalny był używany tylko do pobierania uaktualnień.
- Wyłącz tę opcję, jeśli Agent sieciowy ma być całkowicie zarządzany przez lokalny Serwer administracyjny.

Następnie powinieneś ustalić warunki przełączania do nowo utworzonych profili: przynajmniej jeden warunek dla każdego z biur, za wyjątkiem głównego biura. Celem każdego warunku jest wykrycie elementów, które są specyficzne dla środowiska sieciowego w biurze. Jeśli warunek jest prawdziwy, odpowiedni profil zostaje aktywowany. Jeśli żaden z warunków nie jest prawdziwy, Agent sieciowy przełączy się do macierzystego Serwera administracyjnego.

Wdrażanie funkcji Zarządzanie urządzeniami mobilnymi

Ta sekcja zawiera informacje o wstępnej instalacji funkcji Zarządzanie urządzeniami mobilnymi.

Połączenie urządzeń KES z Serwerem administracyjnym

W zależności od metody używanej do łączenia urządzeń z Serwerem administracyjnym, dla Kaspersky Device Management for iOS istnieją dwa schematy zdalnej instalacji na urządzeniach KES:

- Schemat zdalnej instalacji z bezpośrednim połączeniem urządzeń z Serwerem administracyjnym
- Schemat wdrożenia obejmujący odwrotny serwer proxy obsługujący delegowanie protokołu Kerberos

Bezpośrednie połączenie urządzeń z Serwerem administracyjnym

Urządzenia KES mogą łączyć się bezpośrednio z portem 13292 Serwera administracyjnego.

W zależności od metody używanej do autoryzacji, dla połączenia urządzeń KES z Serwerem administracyjnym możliwe są dwie opcje:

- Łączenie urządzeń z użyciem certyfikatu użytkownika
- Łączenie urządzeń bez użycia certyfikatu użytkownika

Łączenie urządzeń z użyciem certyfikatu użytkownika

Podczas łączenia urządzeń z użyciem certyfikatu użytkownika, to urządzenie jest kojarzone z kontem użytkownika, do którego odpowiedni certyfikat został przypisany poprzez narzędzia Serwera administracyjnego.

W tym przypadku używane będzie dwukierunkowe uwierzytelnianie SSL (uwierzytelnianie obustronne). Serwer administracyjny i urządzenie będą uwierzytelniani przy użyciu certyfikatów.

Łączenie urządzeń bez użycia certyfikatu użytkownika

Podczas łączenia urządzenia bez użycia certyfikatu użytkownika, to urządzenie nie jest kojarzone z żadnym kontem użytkownika na Serwerze administracyjnym. Jednakże, gdy urządzenie pobierze dowolny certyfikat, to urządzenie zostanie skojarzone z kontem użytkownika, do którego odpowiedni certyfikat został przypisany poprzez narzędzia Serwera administracyjnego.

Podczas łączenia tego urządzenia z Serwerem administracyjnym zostanie zastosowane jednokierunkowe uwierzytelnianie SSL, co oznacza, że tylko Serwer administracyjny będzie uwierzytelniony przy użyciu certyfikatu. Po pobraniu przez urządzenie certyfikatu użytkownika, typ autoryzacji zmieni się na dwukierunkowe uwierzytelnianie SSL (uwierzytelnianie obustronne).

Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD)

Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD) uwzględnia:

- Integracja z odwrotnym serwerem proxy obsługującym KCD.
- Użycie delegowania protokołu Kerberos (zwane również KCD) do uwierzytelnia urządzeń mobilnych.
- Integrację z infrastrukturą kluczy publicznych (zwana również PKI) w celu zastosowania certyfikatów użytkownika.

Podczas korzystania z tego schematu połączenia należy pamiętać, że:

- Typem połączenia urządzeń KES z odwrotnym serwerem proxy ma być „dwukierunkowe uwierzytelnianie SSL", czyli urządzenie musi łączyć się z odwrotnym serwerem proxy poprzez swój własny certyfikat użytkownika. W tym celu należy zintegrować certyfikat użytkownika z pakietem instalacyjnym programu Kaspersky Endpoint Security for Android, który został zainstalowany na urządzeniu. Ten pakiet KES musi być utworzony przez Serwer administracyjny specjalnie dla tego urządzenia (użytkownika).
- Dla protokołu mobilnego powinieneś określić specjalny (niestandardowy) certyfikat zamiast domyślnego certyfikatu serwera:

  1. W oknie właściwości Serwera administracyjnego, w sekcji **Ustawienia** zaznacz pole **Otwórz port dla urządzeń mobilnych**, a następnie z listy rozwijalnej wybierz **Dodaj certyfikat**.
  2. W otwartym oknie określ ten sam certyfikat, który został ustawiony na odwrotnym serwerze proxy, gdy punkt dostępu do protokołu mobilnego został opublikowany na Serwerze administracyjnym.

- Certyfikaty użytkownika dla urządzeń KES muszą być wystawione przez urząd certyfikacji (CA) domeny. Należy pamiętać, że jeśli domena zawiera kilka głównych urzędów certyfikacji, certyfikaty użytkownika muszą być wystawione przez urząd certyfikacji, który został ustawiony w publikacji na odwrotnym serwerze proxy.

Możesz upewnić się, że certyfikat użytkownika jest zgodny z wyżej opisanymi wymaganiami przy użyciu jednej z następujących metod:

- Określ specjalny certyfikat użytkownika w kreatorze Nowego pakietu oraz kreatorze instalacji Certyfikatu.
- Zintegruj Serwer administracyjny z infrastrukturą kluczy publicznych domeny oraz zdefiniuj odpowiednie ustawienie w regułach wystawiania certyfikatów:

  1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.
  2. W obszarze roboczym folderu **Certyfikaty** kliknij przycisk **Konfiguruj reguły wydawania certyfikatów**, aby otworzyć okno **Reguły wydawania certyfikatu**.
  3. W sekcji **Integracja z PKI** skonfiguruj integrację z infrastrukturą kluczy publicznych.
  4. W sekcji **Wydawanie certyfikatów dla urządzeń mobilnych** określ źródło certyfikatów.

Poniżej znajduje się przykład konfiguracji delegowania protokołu Kerberos (KCD) z następującymi założeniami:

- Punkt dostępu do protokołu mobilnego na Serwerze administracyjnym jest ustawiony na porcie 13292.
- Nazwa urządzenia z odwrotnym serwerem proxy to firewall.mydom.local.
- Nazwa urządzenia z Serwerem administracyjnym to ksc.mydom.local.
- Nazwa zewnętrznej publikacji punktu dostępu do protokołu mobilnego to kes4mob.mydom.global.

Konto domeny dla Serwera administracyjnego

Należy utworzyć konto domeny (na przykład: KSCMobileSrvcUsr), z poziomu którego będzie uruchamiana usługa Serwera administracyjnego. Konto dla usługi Serwera administracyjnego można określić podczas instalacji Serwera administracyjnego lub poprzez narzędzie klsrvswch. Narzędzie klsrvswch znajduje się w folderze instalacyjnym Serwera administracyjnego. Domyślna ścieżka instalacji: <Disk>:\Program Files (x86)\ Kaspersky Lab\ Kaspersky Security Center.

Konto domeny musi zostać określone z następujących względów:

- Funkcja zarządzania urządzeniami KES jest integralną częścią Serwera administracyjnego.
- Aby zapewnić poprawne działanie delegowania protokołu Kerberos (KCD), strona odbierająca (czyli Serwer administracyjny) musi być uruchomiona z poziomu konta domeny.

Nazwa główna usługi dla http/kes4mob.mydom.local

W domenie, z poziomu konta KSCMobileSrvcUsr, dodaj SPN dla publikacji usługi protokołu mobilnego na porcie 13292 urządzenia z Serwerem administracyjnym. Dla urządzenia kes4mob.mydom.local z Serwerem administracyjnym będzie to wyglądało w następujący sposób:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Konfiguracja właściwości domeny urządzenia z odwrotnym serwerem proxy (firewall.mydom.local)

Aby przeprowadzić ruch sieciowy, przełącz urządzenie z odwrotnym serwerem proxy (firewall.mydom.local) do usługi, która jest definiowana po SPN (http/kes4mob.mydom.local:13292).

W celu przełączenia urządzenia z odwrotnym serwerem proxy do usługi definiowanej po SPN (http/kes4mob.mydom.local:13292), administrator musi wykonać następujące działania:

1. W przystawce Microsoft Management Console o nazwie „Użytkownicy i komputery usługi Active Directory" wybierz urządzenie z zainstalowanym odwrotnym serwerem proxy (firewall.mydom.local).

2. We właściwościach urządzenia, na zakładce **Delegowanie** ustaw przełącznik **Ufaj temu komputerowi w delegowaniu tylko do określonych usług** na **Użyj dowolnego protokołu uwierzytelniania**.

3. Na liście **Usługi, którym to konto może przedstawiać delegowane poświadczenia** dodaj SPN http/kes4mob.mydom.local:13292.

Specjalny (niestandardowy) certyfikat dla publikacji (kes4mob.mydom.global)

Aby opublikować protokół mobilny Serwera administracyjnego, należy wystawić specjalny (niestandardowy) certyfikat dla FQDN kes4mob.mydom.global, a także określić go w miejsce domyślnego certyfikatu serwera w ustawieniach protokołu mobilnego Serwera administracyjnego, w Konsoli administracyjnej. W tym celu, w oknie właściwości Serwera administracyjnego, w sekcji **Ustawienia** zaznacz pole **Otwórz port dla urządzeń mobilnych**, a następnie z listy rozwijalnej wybierz **Dodaj certyfikat**.

Należy pamiętać, że kontener certyfikatów serwera (plik z rozszerzeniem .p12 lub .pfx) musi także zawierać łańcuch certyfikatów głównych (klucze publiczne).

Konfiguracja publikacji na odwrotnym serwerze proxy

Na odwrotnym serwerze proxy, dla ruchu przechodzącego z urządzenia mobilnego do portu 13292 usługi kes4mob.mydom.global należy skonfigurować KCD na SPN (http/kes4mob.mydom.local:13292), korzystając z certyfikatu serwera opublikowanego dla FQDN kes4mob.mydom.global. Nie można zapominać, że publikacja oraz opublikowany punkt dostępu (port 13292 Serwera administracyjnego) powinny korzystać z tego samego certyfikatu serwera.

Korzystanie z Firebase Cloud Messaging

Aby zapewnić dostarczanie w odpowiednim momencie poleceń na urządzenia KES działające pod systemem operacyjnym Android, Kaspersky Security Center korzysta z mechanizmów powiadomień push. Powiadomienia push są wymieniane pomiędzy urządzeniami KES a Serwerem administracyjnym za pośrednictwem usługi Firebase Cloud Messaging (zwanej dalej FCM). W Konsoli administracyjnej Kaspersky Security Center możesz określić ustawienia Firebase Cloud Messaging do podłączania urządzeń KES do usługi.

Aby pobrać ustawienia Firebase Cloud Messaging, należy posiadać konto Google.

W celu włączenia korzystania z FCM:

1. W Konsoli administracyjnej wybierz węzeł **Zarządzanie urządzeniami mobilnymi** oraz folder **Urządzenia mobilne**.

2. Z otwartego menu kontekstowego folderu **Urządzenia mobilne** wybierz **Właściwości**.

3. We właściwościach folderu wybierz sekcję **Ustawienia Firebase Cloud Messaging**.

4. W polu **Numer projektu Firebase** podaj identyfikator nadawcy FCM.

5. W polu **Plik klucza prywatnego (w formacie JSON)** wybierz plik klucza prywatnego.

   Przy kolejnej synchronizacji z Serwerem administracyjnym, urządzenia KES, działające pod systemami operacyjnymi Android, zostaną połączone z Firebase Cloud Messaging.

Możesz zmodyfikować ustawienia Firebase Cloud Messaging, klikając przycisk **Resetuj ustawienia**.

Po przejściu do innego projektu Firebase musisz poczekać 10 minut na wznowienie FCM.

Usługa FCM działa w następujących zakresach adresów:

- Ze strony urządzenia KES dostęp jest wymagany do portów 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) oraz 5230 (HTTPS) dla następujących adresów:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Wszystkie adresy IP w ASN Google'a dla portu 15169
- Ze strony Serwera administracyjnego dostęp jest wymagany do portu 443 (HTTPS) dla następujących adresów:
  - fcm.googleapis.com
  - Wszystkie adresy IP w ASN Google'a dla portu 15169

Jeśli ustawienia serwera proxy (**Zaawansowane** / **Konfiguracja dostępu do internetu**) zostały określone we właściwościach Serwera administracyjnego w Konsoli administracyjnej, będą używane do interakcji z FCM.

Konfigurowanie FCM: pobieranie ID nadawcy i pliku klucza prywatnego

W celu skonfigurowania FCM:

1. Zarejestruj się na portalu Google.
2. Przejdź do konsoli Firebase.
3. Wykonaj jedną z poniższych czynności:
   - Aby utworzyć nowy projekt, kliknij **Utwórz projekt** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
   - Otwórz istniejący projekt.
4. Kliknij ikonę koła zębatego i wybierz opcję **Ustawienia projektu**.

   Zostanie otwarte okno **Ustawienia projektu**.
5. Wybierz zakładkę **Cloud Messaging**.
6. Pobierz odpowiedni identyfikator nadawcy z pola **ID nadawcy** w sekcji **Firebase Cloud Messaging API (V1)**.

7. Wybierz zakładkę **Konta usług** i kliknij **Wygeneruj nowy klucz prywatny**.

8. W oknie, które zostanie otwarte, kliknij opcję **Generuj klucz**, aby wygenerować i pobrać plik klucza prywatnego.

Usługa Firebase Cloud Messaging jest teraz skonfigurowana.

Integracja z infrastrukturą kluczy publicznych

Integracja z infrastrukturą kluczy publicznych (zwana również PKI) jest przeznaczona głównie do uproszenia wystawiania certyfikatów użytkownika domeny przez Serwer administracyjny.

Administrator może przypisać certyfikat domeny dla użytkownika w Konsoli administracyjnej. Można to zrobić przy użyciu jednej z następujących metod:

- Przydziel użytkownikowi specjalny (niestandardowy) certyfikat z pliku w kreatorze instalacji certyfikatu.
- Przeprowadź integrację z PKI i wskaż PKI jako źródło certyfikatów dla określonego typu certyfikatów lub dla wszystkich typów certyfikatów.

Ustawienia integracji z PKI są dostępne w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** po kliknięciu odnośnika **Zintegruj z infrastrukturą klucza publicznego**.

Ogólne zasady integracji z PKI dla publikacji certyfikatów użytkownika domeny

W Konsoli administracyjnej, w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** kliknij odnośnik **Zintegruj z infrastrukturą klucza publicznego**, aby określić konto domeny, które będzie używane przez Serwer administracyjny do wystawiania certyfikatów użytkownika domeny poprzez urząd certyfikacji domeny (zwany również kontem, z poziomu którego wykonywana jest integracja z PKI).

Należy pamiętać, że:

- Ustawienia integracji z PKI oferują możliwość określenia domyślnego szablonu dla wszystkich typów certyfikatów. Nie wolno też zapominać, że reguły wydawania certyfikatów (dostępne w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** po kliknięciu przycisku **Konfiguruj reguły wydawania certyfikatów**) pozwalają na określenie indywidualnego szablonu dla każdego typu certyfikatu.
- Specjalny certyfikat Agenta rejestracji (EA) powinien zostać zainstalowany na urządzeniu z Serwerem administracyjnym, w repozytorium certyfikatów konta, z poziomu którego wykonywana jest integracja z PKI. Certyfikat Agenta rejestracji (EA) jest wystawiany przez administratora urzędu certyfikacji domeny (CA).

Konto, z poziomu którego wykonywana jest integracja z PKI, musi spełniać następujące kryteria.

- Jest to użytkownik domeny.
- Jest to lokalny administrator urządzenia z Serwerem administracyjnym, z poziomu którego została zainicjowana integracja z PKI.
- Posiada uprawnienie do *Zalogowania w trybie usługi*.
- Urządzenie z zainstalowanym Serwerem administracyjnym musiało być wcześniej uruchomione przynajmniej raz z poziomu tego konta w celu utworzenia trwałego profilu użytkownika.

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (zwany również serwerem sieciowym) jest składnikiem Kaspersky Security Center. Serwer sieciowy został zaprojektowany do publikowania autonomicznych pakietów instalacyjnych, autonomicznych pakietów instalacyjnych dla urządzeń mobilnych oraz plików z folderu współdzielonego.

Pakiety instalacyjne są automatycznie publikowane na serwerze sieciowym, a następnie są usuwane po pierwszym pobraniu. Administrator może wysłać użytkownikowi nowy odnośnik w dowolny sposób, na przykład za pośrednictwem poczty elektronicznej.

Klikając odnośnik, użytkownik może pobrać żądane informacje na urządzenie mobilne.

Ustawienia serwera sieciowego

Jeśli wymagane jest dostrojenie serwera WWW, jego właściwości umożliwiają zmiany portów dla HTTP (8060) i HTTPS (8061). Oprócz zmiany portów, możesz zastąpić certyfikat serwera dla HTTPS i zmienić FQDN serwera sieciowego dla HTTP.

Inne podstawowe prace

Ta sekcja zawiera zalecenia dotyczące codziennej pracy z Kaspersky Security Center.

Monitorowanie koloru wskaźnika i rejestrowanych zdarzeń w Konsoli administracyjnej

Konsola administracyjna umożliwia szybką ocenę bieżącego stanu Kaspersky Security Center i zarządzanych urządzeń poprzez sprawdzenie wskaźników przypominających sygnalizację świetlną. Kolory wskaźnika są pokazywane w obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Monitorowanie**. Zakładka udostępnia sześć paneli informacyjnych z kolorowymi wskaźnikami i zarejestrowanymi zdarzeniami. Wskaźnik to kolorowy, pionowy pasek po lewej stronie panelu. Każdy panel ze wskaźnikiem odpowiada określonym zakresom funkcjonalnym Kaspersky Security Center (patrz tabela poniżej).

Kolory ikony wskaźnika w Konsoli administracyjnej

Nazwa panelu	Zakres funkcji
Wdrażanie	Instalacja Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci organizacji
Schemat zarządzania	Struktura grup administracyjnych. Skanowanie sieci. Reguły przenoszenia urządzeń
Ustawienia ochrony	Funkcjonalność aplikacji zabezpieczającej: stan ochrony, skanowanie w poszukiwaniu złośliwego oprogramowania
Aktualizuj	Uaktualnienia i łaty
Monitorowanie	Stan ochrony
Serwer administracyjny	Funkcje Serwera administracyjnego i właściwości

Każdy wskaźnik może przyjąć jeden z pięciu kolorów (patrz tabela poniżej). Kolor wskaźnika zależy od aktualnego stanu Kaspersky Security Center i zdarzeń, które zostały zarejestrowane.

Kolory zestawów

Stan	Kolor wskaźnika	Znaczenie koloru wskaźnika
Informacja	Zielony	Nie jest wymagana interwencja administratora.
Ostrzeżenie	Żółty	Wymagana jest interwencja administratora.
Krytyczny	Czerwony	Wystąpiły poważne problemy. W celu rozwiązania tych problemów wymagana jest interwencja administratora.
Informacja	Niebieski	Wydarzenia, które zostały zarejestrowane, nie są związane z potencjalnymi lub rzeczywistymi zagrożeniami dla bezpieczeństwa zarządzanych urządzeń.
Informacja	Szary	Szczegóły zdarzeń są niedostępne lub nie zostały jeszcze pobrane.

Celem administratora jest zachowanie zielonych kolorów wskaźników na wszystkich panelach informacyjnych, na zakładce **Monitorowanie**.

Panele informacyjne pokazują również zarejestrowane zdarzenia, które mają wpływ na kolory wskaźnika i stan Kaspersky Security Center (patrz tabela poniżej).

Nazwa, opis i kolory wskaźnika zarejestrowanych zdarzeń

Kolor wskaźnika	Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Opis
Czerwony	**Licencja utraciła ważność na %1 urządzeniach**	IDS_AK_STATUS_LIC_EXPAIRED	Tego typu zdarzenia mają miejsce, gdy licencja komercyjna wygasła. Raz dziennie Kaspersky Security Center sprawdza, czy licencja na urządzeniach wygasła. Po wygaśnięciu licencji komercyjnej Kaspersky Security Center zapewnia tylko podstawową funkcjonalność. Aby kontynuować korzystanie z Kaspersky Security Center, musisz odnowić swoją licencję komercyjną.
Czerwony	**Aplikacja zabezpieczająca nie jest uruchomiona na %1 urządzeniach**	IDS_AK_STATUS_AV_NOT_RUNNING	Zdarzenia tego typu występują, gdy aplikacja zabezpieczająca zainstalowana na urządzeniu nie jest uruchomiona. Upewnij się, że Kaspersky Endpoint Security jest uruchomiony na urządzeniu.
Czerwony	**Ochrona jest wyłączona na %1 urządzeniach**	IDS_AK_STATUS_RTP_NOT_RUNNING	Zdarzenia tego typu występują, gdy aplikacja zabezpieczająca na urządzeniu jest wyłączona na dłużej niż określony przedział czasu. Sprawdź aktualny stan ochrony w czasie rzeczywistym na urządzeniu i upewnij się, że wszystkie potrzebne składniki ochrony są włączone.
Czerwony	**Na urządzeniach wykryto oprogramowanie zawierające luki**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Zdarzenia tego typu występują, gdy zadanie *Znajdź luki i wymagane aktualizacje* wykryje luki o priorytecie określonym w aplikacjach zainstalowanych na urządzeniu. Zobacz listę dostępnych aktualizacji w podfolderze **Aktualizacje oprogramowania** znajdującym się w folderze **Zarządzanie aplikacjami**. Ten folder zawiera listę aktualizacji pobranych przez Serwer administracyjny dla aplikacji Microsoft i innych producentów oprogramowania, które mogą być przesyłane na urządzenia. Po przejrzeniu informacji o dostępnych aktualizacjach, zainstaluj je na urządzeniu.
Czerwony	**Na Serwerze administracyjnym zostały zarejestrowane zdarzenia krytyczne**	IDS_AK_STATUS_EVENTS_OCCURED	Zdarzenia tego typu występują po wykryciu krytycznych zdarzeń Serwera administracyjnego. Sprawdź listę zdarzeń przechowywaną na Serwerze administracyjnym, a następnie napraw krytyczne zdarzenia jedno po drugim.

Kolor wskaźnika	Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Opis
Czerwony	**W zdarzeniach na Serwerze administracyjnym zostały zarejestrowane błędy**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Zdarzenia tego typu występują, gdy po stronie Serwera administracyjnego są rejestrowane nieoczekiwane błędy. Sprawdź listę zdarzeń przechowywaną na Serwerze administracyjnym, a następnie napraw błędy jeden po drugim.
Czerwony	**Utracono połączenie z %1 urządzeniami**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Zdarzenia tego typu występują w przypadku utraty połączenia między Serwerem administracyjnym a urządzeniem. Wyświetl listę rozłączonych urządzeń i spróbuj połączyć je ponownie.
Czerwony	**%1 urządzeń od dłuższego czasu nie nawiązało połączenia z Serwerem administracyjnym**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Zdarzenia tego typu występują, gdy urządzenie nie nawiązało połączenia z Serwerem administracyjnym w określonym przedziale czasu, ponieważ urządzenie było wyłączone. Upewnij się, że urządzenie jest włączone i że Agent sieciowy jest uruchomiony.
Czerwony	**Liczba urządzeń posiadających stan inny niż OK: %1**	IDS_AK_STATUS_HOST_NOT_OK	Zdarzenia tego typu występują, gdy stan *OK* urządzenia podłączonego do Serwera administracyjnego zmienia się na *Krytyczny* lub *Ostrzeżenie*. Możesz rozwiązać problem za pomocą narzędzia do zdalnej diagnostyki Kaspersky Security Center.
Czerwony	**Bazy danych są nieaktualne na: %1 urządzeniach**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Zdarzenia tego typu występują, gdy antywirusowe bazy danych nie zostały zaktualizowane na urządzeniu w określonym przedziale czasu. Postępuj zgodnie z instrukcjami, aby zaktualizować bazy danych Kaspersky.
Czerwony	**Urządzenia, na których wyszukiwanie aktualizacji systemu Windows nie było wykonywane od dłuższego czasu: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Zdarzenia tego typu występują, gdy zadanie *Wykonaj synchronizację usługi Windows Update* nie zostało uruchomione w określonym przedziale czasu. Postępuj zgodnie z instrukcjami, aby zsynchronizować aktualizacje z Windows Update z Serwerem administracyjnym.
Czerwony	**%1 – liczba wtyczek, które muszą zostać zainstalowane dla Kaspersky Security Center**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Zdarzenia tego typu występują, gdy zachodzi potrzeba zainstalowania dodatkowych wtyczek dla aplikacji Kaspersky. Pobierz i zainstaluj wymagane wtyczki administracyjne dla aplikacji Kaspersky ze strony Pomocy technicznej Kaspersky.

Zdalny dostęp do zarządzanych urządzeń

Ta sekcja zawiera informacje o zdalnym dostępie do zarządzanych urządzeń.

Zdalne połączenie z zarządzanymi urządzeniami nie jest obsługiwane podczas uzyskiwania dostępu do Kaspersky Security Center Web Console z urządzenia z systemem Microsoft Windows opartym na architekturze Arm.

Korzystanie z opcji „Nie odłączaj od Serwera administracyjnego” w celu zapewnienia ciągłej łączności między zarządzanym urządzeniem a Serwerem administracyjnym

Jeśli nie używasz serwerów push, Kaspersky Security Center nie zapewnia ciągłej łączności między zarządzanymi urządzeniami a Serwerem administracyjnym. Agenty sieciowe na zarządzanych urządzeniach okresowo nawiązują połączenie i synchronizują się z Serwerem administracyjnym. Przerwa między tymi synchronizacjami jest definiowana w zasadzie Agenta sieciowego. Jeśli wymagana jest wczesna synchronizacja, Serwer administracyjny (lub punkt dystrybucji, jeśli jest w użyciu) wysyła podpisany pakiet sieciowy poprzez sieć IPv4 lub IPv6 do portu UDP Agenta sieciowego. Domyślnym numerem portu jest 15000. Jeśli nie jest możliwe nawiązanie połączenia między Serwerem administracyjnym a zarządzanym urządzeniem przy użyciu UDP, synchronizacja zostanie uruchomiona przy następnym regularnym połączeniu Agenta sieciowego z Serwerem administracyjnym w trakcie okresu synchronizacji.

Niektórych operacji nie można wykonać bez wcześniejszego nawiązania połączenia między Agentem sieciowym a Serwerem administracyjnym, takich jak uruchamianie i zatrzymywanie zadań lokalnych, odbieranie statystyk dla zarządzanej aplikacji lub tworzenie tunelu. Aby rozwiązać ten problem, jeśli nie korzystasz z serwerów push, możesz użyć opcji **Nie odłączaj od Serwera administracyjnego**, aby upewnić się, że istnieje ciągła łączność między zarządzanym urządzeniem a serwerem administracyjnym.

W celu zapewnienia ciągłego połączenia między zarządzanym urządzeniem a Serwerem administracyjnym:

1. W drzewie konsoli wybierz folder **Zarządzane urządzenia**.
2. W obszarze roboczym folderu wybierz zarządzane urządzenie, z którym chcesz zapewnić ciągłą łączność.
3. Z otwartego menu kontekstowego urządzenia wybierz **Właściwości**.

   Zostanie otwarte okno właściwości wybranego urządzenia.
4. W sekcji **Ogólne** wyświetlanego okna wybierz opcję **Nie odłączaj od Serwera administracyjnego**.

Trwałe połączenie jest nawiązywane między zarządzanym urządzeniem a Serwerem administracyjnym.

Maksymalna całkowita liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego** to 300.

Informacje o sprawdzaniu czasu połączenia pomiędzy urządzeniem a Serwerem administracyjnym

Po wyłączeniu urządzenia, Agent sieciowy powiadamia Serwer administracyjny o tym zdarzeniu. W Konsoli administracyjnej to urządzenie jest wyświetlane jako wyłączone. Jednakże Agent sieciowy nie może powiadamiać Serwera administracyjnego o wszystkich tego typu zdarzeniach. Dlatego też Serwer administracyjny okresowo analizuje atrybut **Połączono z Serwerem administracyjnym** (wartość tego atrybutu jest wyświetlana w Konsoli administracyjnej, we właściwościach urządzenia, w sekcji **Ogólne**) dla każdego urządzenia i porównuje go z interwałem synchronizacji z aktualnych ustawień Agenta sieciowego. Jeśli urządzenie nie odpowiedziało w ponad trzech pomyślnych interwałach synchronizacji, to urządzenie zostanie oznaczone jako wyłączone.

Informacje o wymuszonej synchronizacji

Chociaż Kaspersky Security Center automatycznie synchronizuje stan, ustawienia, zadania i zasady dla zarządzanych urządzeń, to w niektórych przypadkach administrator musi dokładnie wiedzieć, czy dla określonego urządzenia w danym momencie została już przeprowadzona synchronizacja.

W menu kontekstowym zarządzanych urządzeń w Konsoli administracyjnej urządzenia element menu **Wszystkie zadania** zawiera polecenie **Wymuś synchronizację**. Jeśli Kaspersky Security Center 15.1 wykona to polecenie, Serwer administracyjny podejmie próbę nawiązania połączenia z urządzeniem. Jeśli ta próba zakończy się pomyślnie, zostanie wykonana wymuszona synchronizacja. W innym przypadku synchronizacja zostanie wymuszona dopiero po kolejnym zaplanowanym połączeniu nawiązanym pomiędzy Agentem sieciowym a Serwerem administracyjnym.

Informacje o tunelowaniu

Kaspersky Security Center umożliwia tunelowanie połączeń TCP z Konsoli administracyjnej poprzez Serwer administracyjny, a następnie poprzez Agenta sieciowego do określonego portu na zarządzanym urządzeniu. Tunelowanie połączeń jest przeznaczone dla połączenia aplikacji klienckiej na urządzeniu z zainstalowaną Konsolą administracyjną z portem TCP na zarządzanym urządzeniu—jeśli nie jest możliwe bezpośrednie połączenie między Konsolą administracyjną a urządzeniem docelowym.

Na przykład, tunelowanie jest wykorzystywane dla połączeń ze zdalnym pulpitem - zarówno do łączenia się z istniejącą sesją, jak i do tworzenia nowej zdalnej sesji.

Tunelowanie połączeń może zostać włączone także przy użyciu narzędzi zewnętrznych. Na przykład, administrator może uruchomić w ten sposób narzędzie putty, klienta VNC oraz inne narzędzia.

Poradnik dotyczący rozmiarów

Ta sekcja zawiera informacje na temat szacowania rozmiaru dla komponentów Kaspersky Security Center.

Informacje o podręczniku

Podręcznik szacowania rozmiaru dla Kaspersky Security Center 15.1 (zwany również Kaspersky Security Center) jest przeznaczony dla profesjonalistów, którzy instalują i zarządzają Kaspersky Security Center, a także dla tych, którzy zapewniają wsparcie techniczne organizacjom korzystającym z programu Kaspersky Security Center.

Wszystkie zalecenia i obliczenia zostały podane dla sieci, w których Kaspersky Security Center zarządza ochroną urządzeń z zainstalowanymi programami firmy Kaspersky, w tym urządzeniami mobilnymi. Jeśli urządzenia mobilne lub jakiekolwiek inne zarządzane urządzenia będą uwzględniane oddzielnie, zostanie to wyszczególnione.

Aby uzyskać i utrzymać optymalną wydajność w różnych warunkach pracy, należy wziąć pod uwagę liczbę urządzeń w sieci, topologię sieci oraz zestaw funkcji Kaspersky Security Center, jakich potrzebujesz.

Podręcznik zawiera następujące informacje:

- Ograniczenia Kaspersky Security Center
- Wyliczenia dla kluczowych węzłów Kaspersky Security Center (Serwerów administracyjnych i punktów dystrybucji):
  - Wymagania sprzętowe dla Serwerów administracyjnych i punktów dystrybucji
  - Obliczenie liczby i hierarchia Serwerów administracyjnych
  - Obliczenie liczby i konfiguracja punktów dystrybucji
- Konfiguracja rejestrowania zdarzeń w bazie danych w zależności od liczby urządzeń w sieci
- Popularne najlepsze praktyki optymalizacji wydajności
- Konfiguracja określonych zadań mających na celu zapewnienie optymalnego działania Kaspersky Security Center
- Ilość ruchu sieciowego (obciążenie sieci) pomiędzy Serwerem administracyjnym Kaspersky Security Center a chronionym urządzeniem

Korzystanie z tego podręcznika jest zalecane w następujących przypadkach:

- Podczas rozplanowywania zasobów przed instalacją Kaspersky Security Center
- Podczas rozplanowywania istotnych zmian w sieci, w której wdrożony jest Kaspersky Security Center
- Jeśli przełączasz z używania Kaspersky Security Center w obrębie ograniczonego segmentu sieci (środowisko testowe) do wdrożenia Kaspersky Security Center na pełną skalę w sieci korporacyjnej
- Podczas wprowadzania zmian do zestawu używanych funkcji Kaspersky Security Center

Informacje o ograniczeniach Kaspersky Security Center

Poniższa tabela wyświetla ograniczenia bieżącej wersji Kaspersky Security Center.

Ograniczenia Kaspersky Security Center

Rodzaj ograniczenia	Wartość
Maksymalna liczba zarządzanych urządzeń na Serwer administracyjny	100 000
Maksymalna liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego**	300
Maksymalna liczba grup administracyjnych	10 000
Maksymalna liczba przechowywanych zdarzeń	45 000 000
Maksymalna liczba zasad	2000
Maksymalna liczba zadań	2000
Maksymalna całkowita liczba obiektów Active Directory (jednostek organizacyjnych i kont użytkowników, urządzeń oraz grup bezpieczeństwa)	1 000 000
Maksymalna liczba profili w zasadzie	100
Maksymalna liczba podrzędnych Serwerów administracyjnych w jednym głownym Serwerze administracyjnym	500
Maksymalna liczba wirtualnych Serwerów administracyjnych	500
Maksymalna liczba urządzeń, jaką obejmuje pojedynczy punkt dystrybucji (punkty dystrybucji mogą obejmować tylko urządzenia niemobilne)	10 000
Maksymalna liczba urządzeń, które mogą używać pojedynczej bramy połączenia	10 000, w tym urządzenia mobilne
Maksymalna liczba urządzeń mobilnych na Serwer administracyjny	100 000 minus liczba stacjonarnych zarządzanych urządzeń

Wyliczenia dla Serwerów administracyjnych

Ta sekcja zawiera wymagania programowe i sprzętowe dla urządzeń używanych jako Serwery administracyjne. Można tu znaleźć także zalecenia odnośnie wyliczania liczby i hierarchii Serwerów administracyjnych w zależności od konfiguracji sieci organizacji.

Obliczanie zasobów sprzętowych dla Serwera administracyjnego

Ta sekcja zawiera obliczenia pomagające w rozplanowaniu zasobów sprzętowych dla Serwera administracyjnego. Zalecenia dotyczące obliczenia przestrzeni dyskowej podczas korzystania z funkcji Zarządzanie lukami i poprawkami są dostępne oddzielnie.

Wymagania sprzętowe dla systemu zarządzania bazą danych i Serwera administracyjnego

W poniższej tabeli zostały uwzględnione zalecane minimalne wymagania sprzętowe dla DBMS i Serwera administracyjnego uzyskane w trakcie testów. Pełna lista obsługiwanych systemów operacyjnych i systemów DBMS znajduje się na liście wymagań sprzętowych i programowych.

Serwer administracyjny i DBMS znajdują się na różnych urządzeniach, sieć zawiera 50 000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym

Sprzęt	Wartość
Procesor	4 rdzenie, 2500 MHz
Pamięć RAM	8 GB
Dysk twardy	300 GB, zalecany RAID
Karta sieciowa	1 Gbit

Konfiguracja urządzenia z zainstalowanym DBMS

Sprzęt	Wartość
Procesor	4 rdzenie, 2500 MHz
Pamięć RAM	16 GB
Dysk twardy	200 GB, SATA RAID
Karta sieciowa	1 Gbit

Serwer administracyjny i DBMS znajdują się na tym samym urządzeniu, sieć zawiera 50 000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym i DBMS

Sprzęt	Wartość
Procesor	8 rdzeni, 2500 MHz
Pamięć RAM	16 GB
Dysk twardy	500 GB, SATA RAID
Karta sieciowa	1 Gbit

Serwer administracyjny i DBMS znajdują się na różnych urządzeniach, sieć zawiera 100 000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym

Sprzęt	Wartość
Procesor	8 rdzenie, 2,13 GHz
Pamięć RAM	8 GB

Sprzęt	Wartość
Dysk twardy	1 TB, RAID
Karta sieciowa	1 Gbit

Konfiguracja urządzenia z zainstalowanym serwerem DBMS

Sprzęt	Wartość
Procesor	8 rdzenie, 2,53 GHz
Pamięć RAM	26 GB
Dysk twardy	500 GB, SATA RAID
Karta sieciowa	1 Gbit

Testy zostały przeprowadzone z użyciem następujących ustawień:

- Automatyczne przydzielanie punktów dystrybucji jest włączone na Serwerze administracyjnym lub punkty dystrybucji są przydzielane ręcznie według zalecanej tabeli.
- Zadanie tworzenia kopii zapasowej zapisuje kopie zapasowe w zasobie plików znajdującym się na dedykowanym serwerze.
- Interwał synchronizacji dla Agentów sieciowych jest ustawiony w taki sposób, w jaki opisano to w poniższej tabeli.

  Interwał synchronizacji dla Agentów sieciowych

Okres synchronizacji (minuty)	Liczba zarządzanych urządzeń
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
150	100 000

Obliczanie pojemności bazy danych

Przybliżoną ilość miejsca, jaką powinna zajmować baza danych, można obliczyć, korzystając z następującego wzoru:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

gdzie:

- C to liczba urządzeń.

  > Jeśli wśród zarządzanych urządzeń znajdują się dynamiczne maszyny wirtualne, C jest sumą liczby niedynamicznych zarządzanych urządzeń oraz liczby dynamicznych maszyn wirtualnych, dla których Agent sieciowy został utworzony między dwoma kolejnymi uruchomieniami zadania **Konserwacja Serwera administracyjnego**.

- E to liczba przechowywanych zdarzeń.

- A to całkowita liczba obiektów Active Directory:
  - Konta urządzeń
  - Konta użytkowników
  - Konta grup bezpieczeństwa
  - Jednostki organizacyjne Active Directory

  Jeśli skanowanie Active Directory jest wyłączone, zmienna A będzie równa zero.
- N to średnia liczba zinwentaryzowanych plików wykonywalnych na urządzeniu końcowym.
- F to liczba urządzeń końcowych, na których zinwentaryzowano pliki wykonywalne.

Jeśli planujesz włączyć w ustawieniach zasady Kaspersky Endpoint Security powiadamianie Serwera administracyjnego o aplikacjach, które uruchamiasz, będziesz potrzebował dodatkowej ilości (0,03 * C) gigabajtów do przechowywania w bazie danych informacji o aplikacjach, które uruchamiasz.

Jeśli Serwer administracyjny rozsyła aktualizacje systemu Windows (zachowując się przy tym jak serwer Windows Server Update Services), baza danych będzie wymagała dodatkowych 2,5 GB na dysku.

Podczas działania, w bazie danych zawsze znajduje się część *nieprzydzielonego obszaru*. Dlatego też, rzeczywisty rozmiar pliku bazy danych (domyślnie jest to plik KAV.MDF, jeśli jako DBMS używasz serwera SQL) okazuje się być około dwukrotnie większy niż ilość miejsca zajmowanego przez bazę danych.

Nie jest zalecane wyraźne ograniczenie rozmiaru dziennika transakcji (domyślnie, plik KAV_log.LDF, jeśli używasz serwera SQL jako systemu DBMS). Zalecane jest pozostawienie domyślnej wartości parametru MAXSIZE. Jednakże, jeśli musisz ograniczyć rozmiar tego pliku, weź pod uwagę fakt, że typowa niezbędna wartość parametru MAXSIZE dla KAV_log.LDF to 20 480 MB.

Obliczanie przestrzeni dyskowej (z użyciem oraz bez użycia funkcji Zarządzanie lukami i poprawkami)

Obliczanie przestrzeni dyskowej bez użycia funkcji Zarządzanie lukami i poprawkami

Przestrzeń dyskowa na Serwerze administracyjnym, wymagana dla folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit, może zostać oszacowana w przybliżeniu przy użyciu wzoru:

(724 * C + 0,15 * E + 0,17 * A), KB

gdzie:

- C to liczba urządzeń.

  Jeśli zarządzane urządzenia obejmują dynamiczne maszyny wirtualne, C jest sumą liczby niedynamicznych zarządzanych urządzeń oraz liczby dynamicznych maszyn wirtualnych z Agentem sieciowym utworzonych między dwoma kolejnymi uruchomieniami zadania **Konserwacja Serwera administracyjnego**.

- E to liczba przechowywanych zdarzeń.
- A to całkowita liczba obiektów Active Directory:
  - Konta urządzeń
  - Konta użytkowników
  - Konta grup bezpieczeństwa
  - Jednostki organizacyjne Active Directory

Jeśli skanowanie Active Directory jest wyłączone, zmienna A będzie równa zero.

Obliczanie dodatkowej przestrzeni dyskowej z użyciem funkcji Zarządzanie lukami i poprawkami

- Uaktualnienia. Folder współdzielony dodatkowo potrzebuje przynajmniej 4 GB do przechowywania uaktualnień.
- Pakiety instalacyjne. Jeśli niektóre pakiety instalacyjne są przechowywane na Serwerze administracyjnym, folder współdzielony będzie wymagał dodatkowej ilości miejsca na dysku, równej całkowitemu rozmiarowi wszystkich dostępnych pakietów instalacyjnych przeznaczonych do zainstalowania.
- Zadania zdalnej instalacji. Jeśli zadania zdalnej instalacji znajdują się na Serwerze administracyjnym, wymagana będzie dodatkowa wolna przestrzeń na dysku (w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit) równa całkowitemu rozmiarowi wszystkich pakietów instalacyjnych przeznaczonych do zainstalowania.
- Poprawki. Jeśli Serwer administracyjny jest zaangażowany w instalację łat, niezbędna jest dodatkowa ilość wolnego miejsca na dysku:
  - Folder z poprawkami powinien posiadać ilość miejsca na dysku równą całkowitemu rozmiarowi wszystkich pobranych łat. Domyślnie poprawki są przechowywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles.

    Możesz użyć narzędzia klsrvswch, aby określić inny folder do przechowywania poprawek. Narzędzie klsrvswch znajduje się w folderze, w którym zainstalowany jest serwer administracyjny. Domyślna ścieżka instalacji: <Disk>:\Program Files (x86)\ Kaspersky Lab\ Kaspersky Security Center.

    Jeśli Serwer administracyjny jest używany jako serwer WSUS, zalecane jest przydzielenie temu folderowi przynajmniej 100 GB.
  - Folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit musi posiadać ilość miejsca na dysku równą całkowitemu rozmiarowi tych łat, do których odwołują się istniejące zadania instalacji aktualizacji (łat) i eliminacji luk.

Obliczanie liczby i konfigurowanie Serwerów administracyjnych

Aby zmniejszyć obciążenie na głównym Serwerze administracyjnym, do każdej grupy administracyjnej możesz przypisać oddzielny Serwer administracyjny. Liczba podrzędnych Serwerów administracyjnych nie może przekraczać 500 dla jednego głównego Serwera administracyjnego.

Zalecane jest utworzenie konfiguracji Serwerów administracyjnych w odniesieniu do konfiguracji sieci organizacji.

Zalecenia dotyczące łączenia dynamicznych maszyn wirtualnych z Kaspersky Security Center

Dynamiczne maszyny wirtualne (nazywane również dynamicznymi maszynami wirtualnymi) zużywają więcej zasobów niż statyczne maszyny wirtualne.

Aby uzyskać więcej informacji na temat dynamicznych maszyn wirtualnych, zobacz Obsługa dynamicznych maszyn wirtualnych.

Po podłączeniu nowej dynamicznej maszyny wirtualnej, Kaspersky Security Center tworzy ikonę dla tej dynamicznej maszyny wirtualnej w Konsoli administracyjnej i przenosi dynamiczną maszynę wirtualną do grupy administracyjnej. Następnie dynamiczna maszyna wirtualna jest dodawana do bazy danych Serwera administracyjnego. Serwer administracyjny jest w pełni zsynchronizowany z Agentem sieciowym zainstalowanym na tej dynamicznej maszynie wirtualnej.

W sieci organizacji Agent sieciowy tworzy następujące listy sieci dla każdej dynamicznej maszyny wirtualnej:

- Sprzęt
- Zainstalowane oprogramowanie
- Wykryte luki w zabezpieczeniach
- Zdarzenia i listy plików wykonywalnych komponentu Kontrola aplikacji

Agent sieciowy przesyła te listy sieciowe do Serwera administracyjnego. Rozmiar list sieciowych zależy od komponentów zainstalowanych na dynamicznej maszynie wirtualnej i może wpływać na wydajność Kaspersky Security Center i systemu zarządzania bazami danych (DBMS). Należy zauważyć, że obciążenie może rosnąć nieliniowo.

Po zakończeniu pracy z dynamiczną maszyną wirtualną przez użytkownika i wyłączeniu jej, maszyna ta jest następnie usuwana z infrastruktury wirtualnej, a wpisy dotyczące tej maszyny są usuwane z bazy danych Serwera administracyjnego.

Wszystkie te działania zużywają dużo zasobów bazy danych Kaspersky Security Center i Serwera administracyjnego i mogą zmniejszyć wydajność Kaspersky Security Center i DBMS. Zalecamy podłączenie maksymalnie 20 000 dynamicznych maszyn wirtualnych do Kaspersky Security Center.

Możesz podłączyć ponad 20 000 dynamicznych maszyn wirtualnych do Kaspersky Security Center, jeśli połączone dynamiczne maszyny wirtualne wykonują standardowe operacje (na przykład aktualizacje baz danych) i zużywają nie więcej niż 80 procent pamięci i 75–80 procent dostępnych rdzeni.

Zmiana ustawień zasad, oprogramowania lub systemu operacyjnego na dynamicznej maszynie wirtualnej może zmniejszyć lub zwiększyć zużycie zasobów. Za optymalne uważa się zużycie 80–95 procent zasobów.

Wyliczenia dla punktów dystrybucji i bram połączenia

Ta sekcja zawiera wymagania sprzętowe dla urządzeń używanych jako punkty dystrybucji wraz z zaleceniami dotyczącymi obliczenia liczby punktów dystrybucji i bram połączenia w zależności od konfiguracji sieci firmowej.

Wymagania wobec punktu dystrybucji

W celu zarządzania maksymalnie 10 000 urządzeń klienckich, punkt dystrybucji musi spełniać przynajmniej następujące wymagania (dostępna jest konfiguracja dla środowiska test stand):

- Procesor: Intel® Core™ i7-7700 CPU, 3.60 GHz 4 rdzenie.
- Pamięć RAM: 8 GB.
- Wolne miejsce na dysku: 120 GB.

> Nie zaleca się wyznaczania Serwera administracyjnego jako punktu dystrybucji, ponieważ zwiększy to obciążenie Serwera administracyjnego.

Jeśli jakiekolwiek zadanie zdalnej instalacji jest oczekujące na Serwerze administracyjnym, urządzenie z zainstalowanym punktem dystrybucji będzie także wymagało wolnej przestrzeni na dysku równej całkowitemu rozmiarowi pakietów instalacyjnych przeznaczonych do zainstalowania.

Jeśli na Serwerze administracyjnym jest oczekujące jedno lub kilka zadań instalacji aktualizacji (poprawek) i naprawy luk, urządzenie z zainstalowanym punktem dystrybucji będzie także wymagało dodatkowej wolnej przestrzeni na dysku równej podwojonej wartości całkowitego rozmiaru wszystkich poprawek przeznaczonych do zainstalowania.

Jeśli używasz schematu, gdy punkty dystrybucji otrzymują aktualizacje baz danych i modułów aplikacji bezpośrednio z serwerów aktualizacji Kaspersky, punkty dystrybucji muszą być podłączone do Internetu.

Obliczanie liczby i konfigurowanie punktów dystrybucji

Im więcej urządzeń klienckich zawiera sieć, tym więcej punktów dystrybucji wymaga. Nie jest zalecane wyłączanie automatycznego przypisywania punktów dystrybucji. Jeśli automatyczne przypisywanie punktów dystrybucji jest włączone, Serwer administracyjny przypisuje punkty dystrybucji, gdy liczba urządzeń klienckich jest dosyć duża, oraz definiuje ich konfigurację.

Używanie specjalnie przypisanych punktów dystrybucji

Jeśli planujesz używać określonych urządzeń jako punktów dystrybucji (na przykład, specjalnie wybranych serwerów), możesz zrezygnować z automatycznego przypisywania punktów dystrybucji. W tym przypadku upewnij się, że na urządzeniach, które mają pełnić rolę punktów dystrybucji, jest wystarczająca ilość wolnego miejsca, nie są regularnie wyłączane, a tryb uśpienia jest na nich wyłączony.

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)
10–100	1
Więcej niż 100	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Korzystanie ze standardowych urządzeń klienckich (stacji roboczych) jako punktów dystrybucji

Jeśli planujesz używać standardowych urządzeń klienckich (czyli stacji roboczych) jako punktów dystrybucji, zalecane jest przypisanie punktów dystrybucji w sposób pokazany w tabelach poniżej, aby uniknąć nadmiernego obciążenia kanałów komunikacji i Serwera administracyjnego:

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)
10–30	1
31–300	2
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Jeśli punkt dystrybucji jest wyłączony (lub z jakiegoś powodu niedostępny), zarządzane urządzenia w tym obszarze mogą uzyskać dostęp do Serwera administracyjnego w celu pobrania uaktualnień.

Obliczanie liczby bram połączenia

Jeśli planujesz używać bramy połączenia, zalecane jest wskazanie specjalnego urządzenia do pełnienia tej funkcji.

Brama połączenia może obejmować maksymalnie 10 000 zarządzanych urządzeń, w tym urządzeń mobilnych.

Zapisywanie informacji o zdarzeniach dla zadań i zasad

Ta sekcja zawiera wyliczenia związane z przechowywaniem zdarzeń w bazie danych Serwera administracyjnego i oferuje zalecenia dotyczące zminimalizowania liczby zdarzeń, co pozwala zmniejszyć obciążenie na Serwerze administracyjnym.

Domyślnie, właściwości każdego zadania i zasady zapewniają przechowywanie wszystkich zdarzeń związanych z wykonywaniem zadań i wymuszeniem zasady.

Jednakże, jeśli zadanie jest uruchamiane dość często (na przykład, więcej niż raz w tygodniu) i na całkiem dużej liczbie urządzeń (na przykład, więcej niż 10 000), liczba zdarzeń może okazać się zbyt duża i zdarzenia mogą wypełnić bazę danych. W tym przypadku zalecane jest wybranie jednej z dwóch opcji w ustawieniach zadania:

- **Zapisz zdarzenia dotyczące postępu zadania**. W tym przypadku baza danych pobiera tylko informacje o uruchomieniu zadania, postępie i zakończeniu (pomyślnie, z ostrzeżeniem lub błędem) z każdego urządzenia, na którym zadanie jest uruchomione.

- **Zapisz jedynie wyniki wykonywania zadania**. W tym przypadku baza danych pobiera tylko informacje o zakończeniu zadania (pomyślnie, z ostrzeżeniem lub błędem) z każdego urządzenia, na którym zadanie jest uruchomione.

Jeśli zasada została zdefiniowana dla całkiem dużej liczby urządzeń (na przykład, więcej niż 10 000), liczba zdarzeń może okazać się zbyt duża i zdarzenia mogą wypełnić bazę danych. W tym przypadku zalecane jest wybranie tylko najbardziej krytycznych zdarzeń w ustawieniach zasady i włączenie ich zapisywania. Zalecane jest wyłączenie zapisywania wszystkich pozostałych zdarzeń.

Postępując w ten sposób, zmniejszysz liczbę zdarzeń w bazie danych, zwiększysz prędkość wykonywania scenariuszy skojarzonych z analizą tabeli zdarzeń w bazie danych, a także zmniejszysz ryzyko nadpisania krytycznych zdarzeń przez dużą liczbę zdarzeń.

Możesz także skrócić okres przechowywania zdarzeń skojarzonych z zadaniem lub zasadą. Domyślny okres wynosi 7 dni dla zdarzeń związanych z zadaniem oraz 30 dni dla zdarzeń związanych z zasadą. Podczas zmiany okresu przechowywania zdarzeń należy uwzględnić procedury obowiązujące w organizacji oraz czas, jaki administrator systemu może poświęcić na przeanalizowanie każdego zdarzenia.

Zmodyfikowanie ustawień przechowywania zdarzeń jest zalecane w następujących przypadkach:

- Zdarzenia dotyczące zmian w stanach pośrednich zadań grupowych oraz zdarzenia dotyczące stosowania zasad zajmują dużą część wszystkich zdarzeń w bazie danych Kaspersky Security Center.

- Dziennik zdarzeń aplikacji Kaspersky zaczyna wyświetlać wpisy o automatycznym usuwaniu zdarzeń, gdy przekroczony zostanie ustawiony limit całkowitej liczby zdarzeń przechowywanych w bazie danych.

Wybierz opcje zapisywania zdarzeń w oparciu o założenie, że optymalna liczba zdarzeń pochodzących z jednego urządzenia w ciągu dnia nie może przekraczać 20. Jeśli to konieczne, możesz delikatnie zwiększyć ten limit, ale tylko wtedy, gdy liczba urządzeń w sieci jest relatywnie mała (mniej niż 10 000).

Szczególne względy i optymalne ustawienia określonych zadań

Niektóre zadania podlegają szczególnym zasadom dotyczącym liczby urządzeń w sieci. Ta sekcja oferuje zalecenia odnośnie optymalnej konfiguracji ustawień takich zadań.

Wyszukiwanie urządzeń, zadanie tworzenia kopii zapasowej danych, zadanie konserwacji Serwera administracyjnego oraz grupowe zadania aktualizacji Kaspersky Endpoint Security są częścią podstawowej funkcjonalności Kaspersky Security Center.

Częstotliwość wykrywania urządzeń

Nie jest zalecane zwiększanie domyślnej częstotliwości wyszukiwania urządzeń, gdyż może to spowodować znaczne obciążenie kontrolerów domeny. Natomiast zalecane jest skonfigurowanie terminarza przeszukiwania z minimalną możliwą częstotliwością dozwoloną przez potrzeby organizacji. Zalecenia dotyczące obliczenia optymalnego terminarza znajdują się w tabeli poniżej.

Terminarz wyszukiwania urządzeń

Liczba urządzeń w sieci	Zalecana częstotliwość wyszukiwania urządzeń
Mniej niż 10 000	Domyślna częstotliwość lub mniejsza
10 000 lub większa	Raz dziennie lub rzadziej

Zadanie tworzenia kopii zapasowej danych Serwera administracyjnego i zadanie konserwacji Serwera administracyjnego

Serwer administracyjny przestaje działać podczas wykonywania następujących zadań:

- Tworzenie kopii zapasowych danych Serwera administracyjnego
- Konserwacja Serwera administracyjnego

Podczas wykonywania tych zadań baza danych nie może pobierać żadnych danych.

Konieczna może okazać się zmiana terminarza uruchamiania tych zadań, aby nie były uruchamiane w tym samym czasie co inne zadania Serwera administracyjnego.

Grupowe zadania aktualizacji Kaspersky Endpoint Security

Jeśli Serwer administracyjny pełni rolę źródła uaktualnień, zalecana opcja terminarza dla grupowych zadań aktualizacji Kaspersky Endpoint Security 10 i nowszych wersji to **Po pobraniu nowych uaktualnień do repozytorium** z zaznaczonym polem wyboru **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Jeśli lokalne zadanie pobierania uaktualnień z serwerów Kaspersky do repozytorium jest tworzone na każdym punkcie dystrybucji, okresowe planowanie jest zalecane dla grupowego zadania aktualizacji Kaspersky Endpoint Security. W tym przypadku okres randomizacji musi wynosić jedną godzinę.

Zadanie inwentaryzacji

Możesz zmniejszyć obciążenie bazy danych, jednocześnie uzyskując informacje o plikach wykonywalnych. W tym celu zalecamy uruchomienie zadania inwentaryzacji dla Kaspersky Endpoint Security na odpowiednich urządzeniach, na których jest zainstalowany standardowy zestaw oprogramowania.

Liczba plików wykonywalnych pobranych przez Serwer administracyjny z jednego urządzenia nie może przekraczać 150 000. Jeśli Kaspersky Security Center osiągnie ten limit, nie będzie mógł otrzymywać nowych plików.

Zazwyczaj liczba plików na standardowym urządzeniu klienckim nie przekracza 60 000. Liczba plików wykonywalnych na serwerze plików może być większa, a nawet przekraczać wartość progową wynoszącą 150 000.

Pomiary testowe wykazały, że zadanie inwentaryzacji zwraca następujące wyniki na urządzeniach działających pod kontrolą systemu operacyjnego Windows 7 z zainstalowanym programem Kaspersky Endpoint Security 11 i bez aplikacji innych producentów:

- Przy odznaczonych polach **Inwentaryzacja modułów DLL** i **Inwentaryzacja plików skryptu**: około 3 000 plików.
- Przy zaznaczonych polach **Inwentaryzacja modułów DLL** i **Inwentaryzacja plików skryptu**: od 10 000 do 20 000 plików w zależności od liczby zainstalowanych dodatków service pack dla systemu operacyjnego.
- Przy zaznaczonym polu **Inwentaryzacja plików skryptu**: około 10 000 plików.

Szczegóły dotyczące obciążenia sieci pomiędzy Serwerem administracyjnym a chronionymi urządzeniami

Ta sekcja zawiera wyniki pomiarów testowych ruchu sieciowego wraz z opisem warunków, w jakich te pomiary były robione. Możesz użyć tych informacji podczas planowania infrastruktury sieci i przepustowości sieci w organizacji (lub pomiędzy Serwerem administracyjnym a inną organizacją z urządzeniami, które mają być chronione). Znając przepustowość sieci, możesz w przybliżeniu oszacować czas potrzebny na przesłanie różnych danych.

Zużycie ruchu sieciowego w różnych scenariuszach

Poniższa tabela przedstawia wyniki testów pomiarowych ruchu sieciowego pomiędzy Serwerem administracyjnym a zarządzanym urządzeniem w różnych scenariuszach.

Domyślnie, urządzenia są synchronizowane z Serwerem administracyjnym co 15 minut lub w dłuższych odstępach czasu. Jednakże, jeśli zmodyfikujesz ustawienia zasady lub zadania na Serwerze administracyjnym, wczesna synchronizacja będzie miała miejsce na urządzeniach, do których zasada (lub zadanie) ma zastosowanie, aby nowe ustawienia zostały przesłane na te urządzenia.

Ilość ruchu sieciowego między Serwerem administracyjnym a zarządzanym urządzeniem

Scenariusz	Ruch sieciowy z Serwera administracyjnego do każdego zarządzanego urządzenia	Ruch sieciowy z każdego zarządzanego urządzenia do Serwera administracyjnego
Instalowanie Kaspersky Endpoint Security 11.7 for Windows z zaktualizowanymi bazami danych	390 MB	3.3 MB
Instalacja Agenta sieciowego	75 MB	397 KB
Równoległa instalacja Agenta sieciowego i Kaspersky Endpoint Security 11.7 for Windows	459 MB	3.6 MB
Wstępna aktualizacja antywirusowych baz danych bez aktualizowania baz danych w pakiecie (jeśli uczestnictwo w Kaspersky Security Network zostało wyłączone)	113 MB	1,8 MB
Codzienna aktualizacja antywirusowych baz danych (jeśli uczestnictwo w Kaspersky Security Network zostało włączone)	22 MB	373 MB

Scenariusz	Ruch sieciowy z Serwera administracyjnego do każdego zarządzanego urządzenia	Ruch sieciowy z każdego zarządzanego urządzenia do Serwera administracyjnego
Wstępna synchronizacja przed zaktualizowaniem baz danych na urządzeniu (przesłanie zasad i zadań)	382 KB	446 KB
Wstępna synchronizacja po aktualizacji baz danych na urządzeniu	20 KB	157 KB
Synchronizacja bez zmian na Serwerze administracyjnym (zgodnie z terminarzem)	18 KB	23 KB
Synchronizacja po zmianie jednego ustawienia w zasadzie grupy (natychmiast po zmianie ustawienia)	19 KB	20 KB
Synchronizacja po zmianie jednego ustawienia w zadaniu grupowym (natychmiast po zmianie ustawienia)	14 KB	11 KB
Wymuszona synchronizacja	110 KB	109 KB
Zdarzenie **Wykryto wirusa** (1 wirus)	44 KB	50 KB
Zdarzenie **Wykryto wirusa** (10 wirusów)	58 KB	77 KB
Jednorazowy ruch po włączeniu listy Rejestr aplikacji	do 10 KB	do 12 KB
Codzienny ruch, gdy lista Rejestr aplikacji jest włączona	do 840 KB	do 1 MB

Przeciętne zużycie ruchu sieciowego w ciągu 24 godzin

Średnie 24-godzinne zużycie ruchu sieciowego między Serwerem administracyjnym a zarządzanym urządzeniem jest następujące:

- Ruch sieciowy z Serwera administracyjnego na zarządzane urządzenie wynosi 840 KB.
- Ruch sieciowy z zarządzanego urządzenia do Serwera administracyjnego wynosi 1 MB.

Ruch sieciowy mierzono w następujących warunkach:

- Na zarządzanym urządzeniu zainstalowano Agenta sieciowego i Kaspersky Endpoint Security 11.6 for Windows.
- Urządzenie nie zostało wskazane jako punkt dystrybucji.
- Funkcja Zarządzanie lukami i poprawkami nie została włączona.
- Częstotliwość synchronizacji z Serwerem administracyjnym wynosiło 15 minut.

Kontakt z działem pomocy technicznej

Ta sekcja opisuje sposób uzyskania pomocy technicznej oraz warunki, na jakich jest ona dostępna.

Jak uzyskać pomoc techniczną

Jeśli nie znajdziesz rozwiązania swojego problemu w dokumentacji do Kaspersky Security Center lub w jednym z dodatkowych źródeł informacji o Kaspersky Security Center, skontaktuj się z działem pomocy technicznej Kaspersky. Specjaliści z działu pomocy technicznej odpowiedzą na wszystkie pytania związane z instalacją i użytkowaniem Kaspersky Security Center.

Kaspersky zapewnia wsparcie dla Kaspersky Security Center w trakcie jej cyklu życia (zobacz stronę zawierającą czas trwania wsparcia technicznego aplikacji). Przed skontaktowaniem się z działem pomocy technicznej przeczytaj zasady korzystania z pomocy technicznej.

Możesz skontaktować się z działem pomocy technicznej na jeden z następujących sposobów:

- Odwiedzając witrynę pomocy technicznej
- Wysyłając zgłoszenie do pomocy technicznej poprzez portal Kaspersky CompanyAccount

Pomoc techniczna poprzez Kaspersky CompanyAccount

Kaspersky CompanyAccount jest to portal dla firm korzystających z aplikacji firmy Kaspersky. Portal Kaspersky CompanyAccount został zaprojektowany w celu ułatwienia interakcji między użytkownikami a specjalistami z Kaspersky poprzez zgłoszenia online. Możesz używać Kaspersky CompanyAccount do śledzenia stanu zgłoszeń online, a także przechowywać ich historię.

Możliwe jest zarejestrowanie wszystkich pracowników firmy pod jednym kontem w serwisie Kaspersky CompanyAccount. Jedno konto umożliwia scentralizowane zarządzanie zgłoszeniami elektronicznymi zarejestrowanych pracowników oraz zarządzanie uprawnieniami tych pracowników poprzez Kaspersky CompanyAccount.

Portal Kaspersky CompanyAccount jest dostępny w następujących językach:

- angielskim
- hiszpańskim
- włoskim
- niemieckim
- polskim
- portugalskim

- rosyjskim
- francuskim
- japońskim

Więcej informacji o Kaspersky CompanyAccount można znaleźć na stronie pomocy technicznej.

Uzyskiwanie plików zrzutu Serwera administracyjnego

Pliki zrzutów Serwera administracyjnego zawierają wszystkie informacje o procesach Serwera administracyjnego w danym momencie. Pliki zrzutów Serwera administracyjnego są przechowywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps. Pliki zrzutów są przechowywane tak długo, jak używany jest Kaspersky Security Center, i w przypadku usunięcia są usuwane trwale. Pliki zrzutu nie są automatycznie wysyłane do Kaspersky.

Jeśli Serwer administracyjny ulegnie awarii, możesz skontaktować się z pomocą techniczną Kaspersky. Specjalista pomocy technicznej może poprosić Cię o przesłanie plików zrzutu Serwera administracyjnego do dalszej analizy w Kaspersky.

Pliki zrzutów mogą zawierać dane osobowe. Zalecamy, aby przed wysłaniem informacji do Kaspersky zabezpieczyć je przed nieautoryzowanym dostępem.

Źródła informacji o aplikacji

Strona Kaspersky Security Center na witrynie Kaspersky

Na stronie internetowej programu Kaspersky Security Center, dostępnej w witrynie Kaspersky znajdziesz ogólne informacje o aplikacji, jej funkcjach i właściwościach.

Strona Kaspersky Security Center w Bazie wiedzy

Baza wiedzy to sekcja na stronie działu pomocy technicznej Kaspersky.

Na stronie Kaspersky Security Center w Bazie wiedzy możesz przeczytać artykuły zawierające przydatne informacje, zalecenia i odpowiedzi na najczęściej zadawane pytania dotyczące zakupu, instalacji i korzystania z aplikacji.

Artykuły w Bazie wiedzy mogą zawierać odpowiedzi na pytania dotyczące Kaspersky Security Center, a także innych aplikacji firmy Kaspersky. Artykuły w Bazie wiedzy mogą zawierać także nowości z działu pomocy technicznej.

Społeczność użytkowników produktów firmy Kaspersky

Jeżeli zapytanie nie wymaga natychmiastowej odpowiedzi, możesz przedyskutować je ze specjalistami z firmy Kaspersky lub z innymi użytkownikami na naszym Forum.

Na Forum możesz przeglądać istniejące tematy, pozostawiać swoje komentarze i tworzyć nowe tematy.

> Do przeglądania zasobów internetowych wymagane jest połączenie z internetem.

Jeśli nie możesz znaleźć rozwiązania swojego problemu, skontaktuj się z działem pomocy technicznej.

Słownik

Administrator dostawcy usługi

Pracownik u dostawcy usługi ochrony antywirusowej. Administrator wdraża i obsługuje systemy ochrony antywirusowej oparte na produktach antywirusowych firmy Kaspersky oraz zapewnia klientom pomoc techniczną.

Administrator Kaspersky Security Center

Osoba zarządzająca działaniami aplikacji poprzez system scentralizowanej zdalnej administracji Kaspersky Security Center.

Administrator klienta

Pracownik firmy klienta, który jest odpowiedzialny za stan ochrony antywirusowej i monitorowanie.

Agent autoryzacji

Interfejs umożliwiający przeprowadzenie procesu autoryzacji w celu uzyskania dostępu do zaszyfrowanych dysków twardych i załadowania systemu operacyjnego po zaszyfrowaniu dysku twardego.

Agent sieciowy

Składnik Kaspersky Security Center umożliwiający interakcję Serwera administracyjnego z aplikacjami firmy Kaspersky zainstalowanymi na określonym węźle sieciowym (stacji roboczej lub serwerze). Ten moduł jest wspólny dla wszystkich produktów Kaspersky dla Microsoft® Windows®. Oddzielne wersje Agenta sieciowego dostępne są dla aplikacji Kaspersky przeznaczonych dla systemów Unix i macOS.

Aktualizacja

Procedura zastępowania lub dodawania nowych plików (baz danych lub modułów aplikacji) pobieranych z serwerów aktualizacji firmy Kaspersky.

Aktualizacja Kaspersky Security Center

Procedura instalacji nowszej wersji Kaspersky Security Center na urządzeniu, na którym jest zainstalowana wcześniejsza wersja tych aplikacji.

Aktywny klucz

Klucz, który jest aktualnie używany przez aplikację.

Amazon Machine Image (AMI)

Szablon zawierający konfigurację oprogramowania niezbędną do uruchomienia maszyny wirtualnej. W oparciu o jeden obraz AMI można utworzyć kilka instancji.

Antywirusowe bazy danych

Bazy danych zawierają opisy zagrożeń ochrony komputera znane specjalistom z Kaspersky w momencie opublikowania antywirusowych baz danych. Wpisy w antywirusowych bazach danych pozwalają na wykrywanie szkodliwego kodu w skanowanych obiektach. Antywirusowe bazy danych są tworzone przez specjalistów z Kaspersky i aktualizowane co godzinę.

Atak MITM

Człowiek pośrodku. Atak na infrastrukturę IT organizacji, w którym haker przejmuje połączenie komunikacyjne między dwoma punktami dostępowymi, przekazuje je iw razie potrzeby modyfikuje połączenie między tymi punktami dostępowymi.

Atak wirusa

Seria celowych prób zainfekowania urządzenia wirusem.

AWS API (Application Program Interface)

Interfejs programistyczny aplikacji platformy AWS, który jest używany przez Kaspersky Security Center. Narzędzia AWS API są przede wszystkim używane do przeszukiwania segmentu chmury i instalowania Agenta sieciowego na instancjach.

Bezpośrednie zarządzanie aplikacjami

Zarządzanie aplikacją poprzez interfejs lokalny.

Brama połączenia

Brama połączenia to Agent sieciowy działający w trybie specjalnym. Brama połączenia akceptuje połączenia z innych Agentów sieciowych i tuneluje je przez Serwer administracyjny poprzez własne połączenie z serwerem. W przeciwieństwie do zwykłego Agenta sieciowego brama połączenia oczekuje na połączenia z Serwerem administracyjnym bardziej niż nawiązuje te połączenia z Serwerem administracyjnym.

Certyfikat współdzielony

Certyfikat, który jest przeznaczony do identyfikacji urządzenia mobilnego użytkownika.

Certyfikatu Serwera administracyjnego

Certyfikat używany przez Serwer administracyjny do następujących celów:

- Uwierzytelnianie Serwera administracyjnego podczas nawiązywania połączenia z Konsolą administracyjną opartą na MMC lub Konsolą Kaspersky Security Center Web Console
- Bezpieczna interakcja pomiędzy Serwerem administracyjnym a Agentami sieciowymi na zarządzanych urządzeniach
- Uwierzytelnianie Serwerów administracyjnych podczas łączenia głównego Serwera administracyjnego z podrzędnym Serwerem administracyjnym

Certyfikat jest tworzony automatycznie podczas instalacji Serwera administracyjnego, a następnie jest przechowywany na Serwerze administracyjnym.

Cloud Discovery

Cloud Discovery zarządza dostępem użytkowników do usług w chmurze. Do usług w chmurze zalicza się np. Microsoft Teams, Salesforce, Microsoft Office 365. Usługi w chmurze są pogrupowane w kategorie, na przykład *Udostępnianie plików*, *Komunikatory*, *Poczta e-mail*.

Dodatkowy (lub rezerwowy) klucz licencyjny

Klucz, który daje prawo do korzystania z aplikacji, chociaż nie jest on aktualnie w użyciu.

Domena rozgłoszeniowa

Logiczny obszar sieci, w której wszystkie węzły mogą wymieniać dane przy użyciu kanału informacyjnego na poziomie modelu OSI (Open Systems Interconnection Basic Reference Model).

Dostawca usługi ochrony antywirusowej

Firma, która oferuje organizacji klienta usługę ochrony antywirusowej opartą na rozwiązaniach firmy Kaspersky.

Dostępne aktualizacje

Zestaw uaktualnień dla modułów aplikacji firmy Kaspersky, w tym krytycznych aktualizacji zebranych przez pewien okres czasu oraz zmiany w architekturze aplikacji.

FileTransferBridge

Wewnętrzny komponent Kaspersky Security Center, który zapewnia lokalne dostarczanie aktualizacji aplikacji firmy Kaspersky. FileTransferBridge jest zintegrowany z Agentem sieciowym (klnagent) i działa lokalnie na każdym zarządzanym urządzeniu.

Gdy aplikacje firmy Kaspersky otrzymują aktualizacje z Kaspersky Security Center, Agent sieciowy pobiera pliki aktualizacji z Serwera administracyjnego lub punktu dystrybucji. FileTransferBridge przesyła następnie pliki lokalnie do zainstalowanych aplikacji firmy Kaspersky, zapewniając niezawodne dostarczanie aktualizacji baz danych i poprawek oprogramowania.

FileTransferBridge używa portów TCP 30522 i 30523. Porty nasłuchują tylko na interfejsie localhost (127.0.0.1) i nie akceptują połączeń przychodzących z sieci zewnętrznych.

Folder Kopia zapasowa

Specjalny folder do przechowywania kopii danych Serwera administracyjnego utworzonych przy użyciu narzędzia kopii zapasowej.

Funkcja rozpoznawania lokalizacji w sieci (NLA)

Usługa systemu Windows, która pomaga systemowi operacyjnemu zidentyfikować bieżącą sieć. NLA wykrywa zmiany w sieci i dostosowuje konfigurację zabezpieczeń urządzenia.

Grupa administracyjna

Zestaw urządzeń pogrupowanych według funkcji i zainstalowanych aplikacji firmy Kaspersky. Urządzenia są pogrupowane dla ułatwienia zarządzania nimi jako pojedynczą jednostką. Grupa może zawierać w sobie inne grupy. Zasady grupy i zadania grupy mogą być tworzone dla każdej zainstalowanej aplikacji w grupie.

Grupa licencjonowanych aplikacji

Grupa aplikacji utworzona w oparciu o kryterium ustalone przez administratora (na przykład, przez dostawcę), dla których zbierane są statystyki instalacji na urządzeniach klienckich.

HTTPS

Bezpieczny protokół używający szyfrowania do przesyłania danych między przeglądarką internetową a serwerem sieciowym. HTTPS jest używany w celu uzyskania dostępu do poufnych informacji, takich jak dane firmowe i finansowe.

Identity and Access Management (IAM)

Usługa AWS, która umożliwia zarządzanie dostępem użytkownika do innych zasobów i usług AWS.

Instalacja lokalna

Instalacja aplikacji zabezpieczającej na urządzeniu w sieci firmowej, która zakłada ręczne uruchomienie procesu instalacji z pakietu dystrybucyjnego aplikacji antywirusowej lub ręczne uruchomienie opublikowanego pakietu instalacyjnego, który wcześniej został pobrany na urządzenie.

Instalacja ręczna

Instalacja aplikacji zabezpieczającej na urządzeniu w sieci firmowej z pakietu dystrybucyjnego. Ręczna instalacja musi odbywać się z udziałem administratora lub innego specjalisty ds. IT. Zazwyczaj ręczna instalacja jest wykonywana wtedy, gdy zdalna instalacja zakończyła się błędem.

Instalacja wymuszona

Metoda zdalnej instalacji aplikacji Kaspersky, która umożliwia zainstalowanie oprogramowania na określonych urządzeniach klienckich. Aby instalacja wymuszona mogła być poprawnie przeprowadzona, konto używane dla tego zadania musi posiadać odpowiednie uprawnienia do zdalnego uruchamiania aplikacji na urządzeniach klienckich. Ta metoda jest zalecana do zainstalowania aplikacji na urządzeniach, które działają pod kontrolą systemów operacyjnych Microsoft Windows i obsługują tę funkcjonalność.

Instalacja zdalna

Instalacja aplikacji firmy Kaspersky przy użyciu usług oferowanych przez Kaspersky Security Center.

Instancja Amazon EC2

Maszyna wirtualna utworzona w oparciu o obraz AMI przy użyciu Amazon Web Services.

Istotność poprawki

Atrybut poprawki. Dla poprawek firmy Microsoft i poprawek firm trzecich istnieje pięć poziomów istotności:

- Krytyczny
- Wysoki
- Średni
- Niski
- Nieznany

Istotność poprawki firmy trzeciej lub firmy Microsoft jest determinowana przez najmniej preferowane priorytety wśród luk, które poprawka powinna wyeliminować.

JavaScript

Język programowania rozszerzający działanie stron internetowych. Strony internetowe utworzone przy użyciu JavaScript mogą wykonywać funkcje (na przykład zmieniać widok elementów interfejsu lub otwierać dodatkowe okna) bez konieczności odświeżania strony internetowej z nowymi danymi z serwera sieciowego. Aby przeglądać strony utworzone przy użyciu JavaScript, włącz obsługę JavaScript w ustawieniach swojej przeglądarki internetowej.

Kaspersky Private Security Network (KPSN)

Sieć Kaspersky Private Security Network to rozwiązanie, które daje użytkownikom urządzeń z zainstalowanymi aplikacjami firmy Kaspersky możliwość dostępu do baz danych reputacji Kaspersky Security Network i innych danych statystycznych bez wysyłania danych z ich urządzeń do Kaspersky Security Network. Sieć Kaspersky Private Security Network została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z jednego z następujących powodów:

- Urządzenia nie są podłączone do Internetu.
- Przesyłanie jakichkolwiek danych poza kraj lub firmową sieć LAN jest zabronione przez prawo lub politykę bezpieczeństwa firmy.

Kaspersky Security Center System Health Validator (SHV)

Składnik aplikacji Kaspersky Security Center, zaprojektowany do sprawdzania działania systemu operacyjnego w przypadku równoczesnego działania Kaspersky Security Center i Microsoft NAP.

Kaspersky Security Center Web Server

Komponent Kaspersky Security Center, który jest instalowany wraz z Serwerem administracyjnym. Serwer WWW został zaprojektowany do przesyłania za pośrednictwem sieci autonomicznych pakietów instalacyjnych, profili iOS MDM oraz plików z folderu współdzielonego.

Kaspersky Security Network (KSN)

Usługa chmury oferująca dostęp do bazy danych firmy Kaspersky, zawierającej ciągle aktualizowane informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji Kaspersky po wykryciu zagrożenia, ulepszenie działania niektórych składników ochrony oraz zmniejszenie ryzyka wystąpienia fałszywych alarmów.

Klient Serwera administracyjnego (urządzenie klienckie)

Urządzenie, serwer lub stacja robocza, na której zainstalowany jest Agent sieciowy i zarządzane aplikacje Kaspersky.

Klucz dostępu AWS IAM

Jest to kombinacja identyfikatora klucza (który wygląda jak "AKIAIOSFODNN7EXAMPLE") i klucza tajnego (który wygląda jak "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Ta para należy do użytkownika IAM i jest używana do uzyskania dostępu do usług AWS.

Konsola administracyjna

Składnik Kaspersky Security Center oparty na systemie Windows (zwany również Konsolą administracyjną opartą na MMC). Ten składnik zapewnia interfejs użytkownika dla usług administracyjnych Serwera administracyjnego i Agenta sieciowego.

Konsola zarządzania AWS

Interfejs sieciowy do przeglądania i zarządzania zasobami AWS. Konsola zarządzania AWS jest dostępna na stronie https://aws.amazon.com/console/.

Kopia zapasowa danych Serwera administracyjnego

Kopiowanie przy użyciu narzędzia kopii zapasowej danych Serwera administracyjnego do miejsca przechowywania oraz ich późniejsze przywracanie. Narzędzie to umożliwia zapisanie:

- Bazy danych Serwera administracyjnego (zasady, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym)
- Informacji o konfiguracji struktury grup administracyjnych i urządzeń klienckich
- Miejsc przechowywania plików instalacyjnych przeznaczonych do zdalnej instalacji aplikacji (zawartość folderów: Pakiety, Dezinstalacja uaktualnień)
- Certyfikatu Serwera administracyjnego

Lightweight Nagent (LWNGT)

Protokół interakcji z Kaspersky Endpoint Security na urządzeniach mobilnych. Protokół LWNGT (zwany również protokołem mobilnym) funkcjonuje jako Agent sieciowy bez konieczności faktycznej instalacji Agenta sieciowego na urządzeniach mobilnych.

Luka

Jest to słaby punkt systemu operacyjnego lub aplikacji, który może zostać wykorzystany przez twórców szkodliwego oprogramowania w celu przeniknięcia do systemu operacyjnego lub aplikacji i naruszenia jego/jej integralności. Duża liczba luk w systemie operacyjnym świadczy o jego zawodności, gdyż wirusy, które przeniknęły do systemu, mogą powodować błędy w działaniu systemu i zainstalowanych aplikacjach.

Macierzysty Serwer administracyjny

Macierzysty Serwer administracyjny jest to Serwer administracyjny, który został określony podczas instalacji Agenta sieciowego. Macierzysty Serwer administracyjny może zostać użyty w ustawieniach profili połączenia Agenta sieciowego.

Niekompatybilna aplikacja

Aplikacja antywirusowa innego producenta lub aplikacja firmy Kaspersky, która nie obsługuje opcji zarządzania poprzez Kaspersky Security Center.

Ochrona antywirusowa sieci

Zestaw działań technicznych i firmowych, które zmniejszają prawdopodobieństwo przeniknięcia wirusów i spamu do sieci organizacji, a także blokują ataki sieciowe, phishing i inne zagrożenia. Ochrona sieci wzrasta, gdy używasz usług i aplikacji zabezpieczających i gdy stosujesz zasady ochrony danych firmowych.

Okres licencji

Przedział czasu, w którym masz dostęp do funkcji aplikacji i posiadasz uprawnienia do korzystania z dodatkowych usług. Zakres usług zależy od typu licencji.

Operator Kaspersky Security Center

Użytkownik monitorujący stan i działanie systemu ochrony zarządzanego poprzez Kaspersky Security Center.

Pakiet instalacyjny

Zestaw plików utworzonych dla zdalnej instalacji aplikacji Kaspersky przy pomocy systemu zdalnego zarządzania Kaspersky Security Center. Pakiet instalacyjny zawiera zakres ustawień potrzebnych do zainstalowania aplikacji i uruchomienia jej natychmiast po zainstalowaniu. Ustawienia odpowiadają domyślnym ustawieniom aplikacji. Pakiet instalacyjny jest tworzony przy użyciu plików z rozszerzeniami .kpd i .kud zawartych w pakiecie dystrybucyjnym aplikacji.

Plik klucza

Plik w formacie xxxxxxxx.key pozwala na korzystanie z aplikacji firmy Kaspersky na warunkach licencji testowej lub komercyjnej.

Priorytet zdarzenia

Cecha zdarzenia, które wystąpiło podczas działania aplikacji firmy Kaspersky. Dostępne są następujące priorytety:

- Zdarzenie krytyczne
- Błąd funkcjonalny
- Ostrzeżenie
- Informacja

Zdarzenia tego samego typu mogą posiadać różne poziomy priorytetu, w zależności od sytuacji, w której wystąpiły.

Profil informacyjny

Zbiór ustawień dotyczących działania aplikacji na urządzeniach mobilnych iOS. Profil informacyjny zawiera informacje o licencji; jest związany z określoną aplikacją.

Profil iOS MDM

Zbiór ustawień dotyczących łączenia urządzeń mobilnych iOS z Serwerem administracyjnym. Użytkownik instaluje profil iOS MDM na urządzeniu mobilnym, po czym to urządzenie mobilne łączy się z Serwerem administracyjnym.

Profil konfiguracyjny

Zasada zawierająca zbiór ustawień i ograniczeń dla urządzenia mobilnego iOS MDM.

Próg aktywności wirusa

Największa dozwolona liczba zdarzeń określonego typu w pewnym przedziale czasowym; przekroczenie tej wartości jest interpretowane jako wzrost aktywności wirusa i zagrożenie epidemią wirusa. Funkcja ta jest bardzo przydatna podczas okresów epidemii wirusów, gdyż daje administratorom możliwość reagowania w odpowiedniej chwili na zagrożenia ataku wirusów.

Przewodnik po zwiększaniu odporności

Opisuje zalecenia i funkcje konfigurowania Kaspersky Security Center i jego komponentów, mające na celu zmniejszenie ryzyka związanego z włamaniem się do niego.

Przywracanie

Przeniesienie oryginalnego obiektu z kwarantanny lub folderu kopii zapasowej do folderu, w którym się znajdował przed umieszczeniem go w kwarantannie, wyleczeniem czy usunięciem, lub do folderu wskazanego przez użytkownika.

Przywrócenie danych Serwera administracyjnego

Przywrócenie danych Serwera administracyjnego z informacji zapisanej w kopii zapasowej przy pomocy narzędzia kopii zapasowej. Narzędzie to umożliwia przywrócenie:

- Bazy danych Serwera administracyjnego (zasady, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym)
- Informacji o konfiguracji struktury grup administracyjnych i urządzeń klienckich
- Miejsc przechowywania plików instalacyjnych przeznaczonych do zdalnej instalacji aplikacji (zawartość folderów: Pakiety, Dezinstalacja uaktualnień)
- Certyfikatu Serwera administracyjnego

Punkt dystrybucji

Komputer, na którym został zainstalowany Agent sieciowy i który jest używany do rozsyłania uaktualnień, zdalnej instalacji aplikacji, uzyskiwania informacji o komputerach w grupie administracyjnej i/lub domenie rozgłoszeniowej. Punkty dystrybucji zostały utworzone w celu zmniejszenia obciążenia na Serwerze administracyjnym podczas dystrybucji aktualizacji i zoptymalizowania ruchu sieciowego. Punkty dystrybucji mogą być wskazywane automatycznie, przez Serwer administracyjny, lub ręcznie, przez administratora. Punkt dystrybucji był wcześniej znany jako agent aktualizacji.

Repozytorium zdarzeń

Część bazy danych Serwera administracyjnego przeznaczonej do przechowywania informacji o zdarzeniach, które występują w Kaspersky Security Center.

Rola IAM

Zestaw uprawnień do wykonywania żądań do usług opartych na AWS. Role IAM nie są skojarzone z określonym użytkownikiem lub grupą; zapewniają uprawnienia dostępu bez kluczy dostępu AWS IAM. Możesz przypisać rolę IAM do użytkowników IAM, instancji EC2 oraz usług i aplikacji opartych na AWS.

Scentralizowane zarządzanie aplikacjami

Zdalne zarządzanie aplikacją przy pomocy usług administracyjnych zawartych w Kaspersky Security Center.

Serwer administracyjny

Moduł aplikacji Kaspersky Security Center realizujący funkcje scentralizowanego przechowywania informacji na temat wszystkich aplikacji firmy Kaspersky zainstalowanych w sieci korporacyjnej. Może być używany do zarządzania tymi aplikacjami.

Serwer iOS MDM

Składnik Kaspersky Security Center zainstalowany na urządzeniu klienckim pozwalający na połączenie urządzeń mobilnych iOS z Serwerem administracyjnym za pośrednictwem usługi Apple Push Notifications (APN).

Serwer urządzeń mobilnych

Składnik Kaspersky Security Center umożliwiający dostęp do urządzeń mobilnych i zarządzanie nimi za pośrednictwem Konsoli administracyjnej.

Serwery aktualizacji Kaspersky

Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji.

Sklep aplikacji

Komponent Kaspersky Security Center. Sklep aplikacji jest używany do zainstalowania aplikacji na urządzeniach z systemem Android, należących do użytkownika. Sklep aplikacji umożliwia opublikowanie plików APK aplikacji oraz odnośników do aplikacji w Google Play.

Środowisko chmury

Maszyny wirtualne i inne zasoby wirtualne, które są oparte na platformie chmury i są połączone w sieci.

SSL

Protokół szyfrowania danych używany w internecie i sieciach lokalnych. Protokół Secure Sockets Layer (SSL) jest używany w aplikacjach internetowych do tworzenia bezpiecznego połączenia między klientem a serwerem.

Stacja robocza administratora

Urządzenie, na którym zainstalowana jest Konsola administracyjna lub którego używasz do otwierania Kaspersky Security Center Web Console. Ten komponent oferuje interfejs zarządzania Kaspersky Security Center.

Stacja robocza administratora służy do konfigurowania i zarządzania częścią serwerową Kaspersky Security Center. Korzystając ze stacji roboczej administratora, administrator tworzy i zarządza scentralizowanym systemem ochrony antywirusowej dla korporacyjnych sieci LAN opartych o aplikacje Kaspersky.

Stan ochrony

Bieżący stan ochrony, który odzwierciedla poziom ochrony komputera.

Stan ochrony sieci

Bieżący stan ochrony, który definiuje bezpieczeństwo urządzeń w sieci firmowej. Stan ochrony sieci uwzględnia takie czynniki, jak zainstalowane aplikacje zabezpieczające, użycie kluczy licencyjnych oraz liczba i typy wykrytych zagrożeń.

Strefa zdemilitaryzowana (DMZ)

Strefa zdemilitaryzowana jest segmentem sieci lokalnej zawierającej serwery, które odpowiadają na zapytania z sieci globalnej. Aby zapewnić bezpieczeństwo firmowej sieci lokalnej, dostęp do sieci LAN z poziomu strefy zdemilitaryzowanej jest chroniony przez zaporę sieciową.

Uprawnienia administracyjne

Poziom uprawnień użytkownika wymaganych do zarządzania obiektami Exchange w obrębie organizacji Exchange.

Urządzenie chronione UEFI

Urządzenie z programem lub aplikacją Kaspersky dla UEFI zintegrowanym na poziomie BIOS-u. Zintegrowana ochrona zapewnia bezpieczeństwo urządzenia od momentu uruchomienia systemu, natomiast ochrona na urządzeniach bez zintegrowanego oprogramowania zaczyna działać dopiero po uruchomieniu aplikacji zabezpieczającej.

Urządzenie iOS MDM

Urządzenie mobilne, które jest podłączone do serwera iOS MDM poprzez protokół iOS MDM. Urządzenia działające pod kontrolą systemu operacyjnego iOS mogą być podłączane i zarządzane poprzez protokół iOS MDM.

Urządzenie KES

Urządzenie mobilne, które jest podłączone do Serwera administracyjnego Kaspersky Security Center i zarządzane poprzez aplikację Kaspersky Endpoint Security for Android.

Ustawienia programu

Ustawienia aplikacji, które są wspólne dla wszystkich typów zadań i zarządzają ogólnym działaniem aplikacji, na przykład, ustawienia działania aplikacji, ustawienia raportowania i ustawienia tworzenia kopii zapasowej.

Ustawienia zadania

Ustawienia aplikacji, które są specyficzne dla każdego typu zadania.

Użytkownicy wewnętrzni

Konta użytkowników wewnętrznych są używane do pracy z wirtualnymi Serwerami administracyjnymi. Kaspersky Security Center nadaje wewnętrznym użytkownikom aplikacji uprawnienia rzeczywistych użytkowników.

Konta wewnętrznych użytkowników są tworzone i używane tylko w obrębie Kaspersky Security Center. Do systemu operacyjnego nie są przesyłane żadne dane dotyczące wewnętrznych użytkowników. Kaspersky Security Center autoryzuje wewnętrznych użytkowników.

Użytkownik IAM

Użytkownik usług AWS. Użytkownik IAM może mieć uprawnienia do wykonywania przeszukiwania segmentu chmury.

Windows Server Update Services (WSUS)

Aplikacja wykorzystywana do rozpowszechniania aktualizacji dla aplikacji firmy Microsoft na komputerach użytkowników w sieci firmowej.

Wirtualny Serwer administracyjny

Składnik Kaspersky Security Center zaprojektowany do zarządzania systemem ochrony sieci organizacji klienta.

Wirtualny Serwer administracyjny jest szczególnym przypadkiem podrzędnego Serwera administracyjnego i ma następujące ograniczenia w porównaniu z fizycznym Serwerem administracyjnym:

- Wirtualny Serwer administracyjny można utworzyć tylko na głównym Serwerze administracyjnym.
- Podczas działania wirtualny Serwer administracyjny używa bazy danych głównego Serwera administracyjnego. Zadania tworzenia kopii zapasowych i przywracania danych, a także zadania pobierania i skanowania aktualizacji nie są obsługiwane na wirtualnym Serwerze administracyjnym.
- Serwer wirtualny nie obsługuje tworzenia podrzędnych Serwerów administracyjnych (łącznie z Serwerami wirtualnymi).

Właściciel urządzenia

Właściciel urządzenia to użytkownik, z którym administrator może skontaktować się, gdy zajdzie potrzeba wykonania określonych działań na urządzeniu.

Wtyczka administracyjna

Specjalny moduł, który zawiera interfejs zarządzania aplikacją poprzez Konsolę administracyjną. Każda aplikacja posiada własną wtyczkę. Znajduje się ona we wszystkich aplikacjach firmy Kaspersky, które mogą być zarządzane przy użyciu Kaspersky Security Center.

Zadanie

Funkcje wykonywane przez aplikacje Kaspersky są zaimplementowane w postaci zadań, na przykład: Ochrona plików w czasie rzeczywistym, Pełne skanowanie komputera, Aktualizacja baz danych.

Zadanie dla określonych urządzeń

Zadanie przypisane do zbioru urządzeń klienckich z dowolnej grupy administracyjnej, wykonywane na tych urządzeniach.

Zadanie grupowe

Zadanie zdefiniowane dla grupy administracyjnej i wykonywane na wszystkich urządzeniach klienckich należących do tej grupy administracyjnej.

Zadanie lokalne

Zadanie utworzone i uruchomione na pojedynczym komputerze klienckim.

Zarządzane urządzenia

Urządzenia z sieci firmowej, które znajdują się w grupie administracyjnej.

Zasada

Zasada określa ustawienia aplikacji i zarządza możliwością konfigurowania tą aplikacją na komputerach w grupie administracyjnej. Dla każdej aplikacji należy utworzyć jedną zasadę. Możliwe jest utworzenie kilku zasad dla aplikacji zainstalowanych na komputerach w każdej grupie administracyjnej, ale tylko jedna zasada może być stosowana do każdej aplikacji w obrębie grupy administracyjnej w danym czasie.

Informacje o kodzie firm trzecich

Informacje o kodzie firm trzecich znajdują się w pliku legal_notices.txt, znajdującym się w folderze instalacyjnym aplikacji.

Informacje o znakach towarowych

Zastrzeżone znaki towarowe i usługowe stanowią odpowiednio własność ich właścicieli.

Adobe, Acrobat, Flash, Shockwave i PostScript są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Adobe w Stanach Zjednoczonych i/lub innych krajach.

AMD, AMD64 są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace są znakami towarowymi firmy Amazon.com, Inc. lub jej podmiotów stowarzyszonych.

Apache jest zastrzeżonym znakiem towarowym lub znakiem towarowym firmy Apache Software Foundation w Stanach Zjednoczonych i/lub innych krajach.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime i Touch ID są zastrzeżonymi znakami towarowymi firmy Apple Inc.

Arm jest zastrzeżonym znakiem towarowym firmy Arm Limited (lub jej spółek zależnych) w Stanach Zjednoczonych i/lub innych krajach.

Logo, marka i słowo Bluetooth należą do firmy Bluetooth SIG, Inc.

Ubuntu, LTS są zastrzeżonymi znakami towarowymi firmy Canonical Ltd.

Cisco Systems, Cisco, Cisco Jabber, IOS są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Cisco Systems, Inc. i/lub jej podmiotów w Stanach Zjednoczonych i innych krajach.

Citrix, XenServer są zarejestrowanymi znakami towarowymi lub znakami towarowymi firmy Cloud Software Group, Inc. i/lub jej spółek zależnych w Stanach Zjednoczonych i/lub innych krajach.

Corel jest zastrzeżonym znakiem towarowym bądź znakiem towarowym firmy Corel Corporation i/lub jej oddziałów w Kanadzie, Stanach Zjednoczonych i/lub innych krajach.

Cloudflare, logo Cloudflare i Cloudflare Workers są znakami towarowymi i/lub zastrzeżonymi znakami towarowymi firmy Cloudflare, Inc. w Stanach Zjednoczonych i innych jurysdykcjach.

Dropbox jest zastrzeżonym znakiem towarowym firmy Dropbox, Inc.

Radmin jest zastrzeżonym znakiem towarowym firmy Famatech.

Firebird jest zastrzeżonym znakiem towarowym firmy Firebird Foundation.

Foxit jest zastrzeżonym znakiem towarowym firmy Foxit Corporation.

FreeBSD jest zastrzeżonym znakiem towarowym firmy The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts, Google Public DNS i YouTube są zastrzeżonymi znakami towarowymi firmy Google, Inc.

EulerOS, FusionCompute, FusionSphere są znakami towarowymi firmy Huawei Technologies Co., Ltd.

Intel, Core, Xeon są znakami towarowymi firmy Intel Corporation lub jej spółek zależnych.

IBM, QRadar są znakami towarowymi firmy International Business Machines Corporation, zarejestrowanymi w wielu jurysdykcjach na świecie.

Node.js jest zastrzeżonym znakiem towarowym firmy Joyent, Inc.

Linux jest zastrzeżonym znakiem towarowym Linus Torvalds w Stanach Zjednoczonych i innych krajach.

Logitech jest zastrzeżonym znakiem towarowym lub znakiem towarowym firmy Logitech w Stanach Zjednoczonych i/lub innych krajach.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, Office 365, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Mobile, Windows Server, Windows Phone, Windows Vista, oraz Windows Azure są znakami towarowymi grupy firm Microsoft.

CVE jest zastrzeżonym znakiem towarowym The MITRE Corporation.

Mozilla, Firefox, Thunderbird są znakami towarowymi Fundacji Mozilla w Stanach Zjednoczonych i innych krajach.

Novell jest zastrzeżonym znakiem towarowym firmy Novell Enterprises Inc. w Stanach Zjednoczonych i innych krajach.

NetWare jest zastrzeżonym znakiem towarowym firmy Novell, Inc. w Stanach Zjednoczonych i innych krajach.

OpenVPN jest zarejestrowanym znakiem towarowym OpenVPN, Inc.

OpenSSL jest znakiem towarowym będącym własnością OpenSSL Software Foundation.

Oracle, Java, JavaScript i TouchDown są zastrzeżonymi znakami towarowymi firmy Oracle i/lub jej oddziałów.

Parallels, logo Parallels i Coherence są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Parallels International GmbH.

Chef jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Progress Software Corporation i/lub jednym z jej oddziałów lub podmiotów, zarejestrowanym w Stanach Zjednoczonych i/lub innych krajach.

Puppet jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Puppet, Inc.

Python jest znakiem towarowym lub zastrzeżonym znakiem towarowym Python Software Foundation.

Red Hat, Fedora i Red Hat Enterprise Linux są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Red Hat, Inc. lub jej oddziałów, zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

Ansible jest zastrzeżonym znakiem towarowym firmy Red Hat, Inc. w Stanach Zjednoczonych i innych krajach.

CentOS jest znakiem towarowym lub zarejestrowanym znakiem towarowym firmy Red Hat, Inc. lub jej spółek zależnych w Stanach Zjednoczonych i innych krajach.

BlackBerry jest zastrzeżonym znakiem towarowym firmy Research In Motion Limited zarejestrowanym na terenie Stanów Zjednoczonych i jest w trakcie rejestrowania lub już jest zarejestrowany na terenie innych krajów.

Rocky Linux jest znakiem towarowym The Rocky Enterprise Software Foundation.

SAMSUNG jest znakiem towarowym firmy SAMSUNG w Stanach Zjednoczonych i innych krajach.

Debian jest zastrzeżonym znakiem towarowym firmy Software in the Public Interest, Inc.

Splunk, SPL są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Splunk Inc., zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

SUSE jest zastrzeżonym znakiem towarowym firmy SUSE LLC, zarejestrowanym w Stanach Zjednoczonych i innych krajach.

Symbian jest znakiem towarowym firmy Symbian Foundation Ltd.

OpenAPI to znak towarowy firmy The Linux Foundation.

UNIX jest zastrzeżonym znakiem towarowym w Stanach Zjednoczonych i innych krajach, używanym na wyłącznej licencji firmy X/Open Company Limited.

Zabbix jest zastrzeżonym znakiem towarowym firmy Zabbix SIA.

Znane problemy

Kaspersky Security Center Web Console ma szereg ograniczeń, które nie są krytyczne dla działania aplikacji:

- 9838414: Instalacja Agenta sieciowego dla systemu Microsoft Windows opartego na architekturze Arm przy użyciu autonomicznego pakietu instalacyjnego może zatrzymać się na etapie **Sprawdzanie połączenia z Serwerem administracyjnym**, mimo że urządzenie zostało pomyślnie połączone z Serwerem administracyjnym, a instalacja została ukończona. Jeśli instalacja zatrzyma się na tym etapie, możesz zamknąć okno instalacji. Agent sieciowy dla systemu Microsoft Windows on Arm jest już zainstalowany.

- 9978211: Opcja **Użyj Agenta sieciowego jako bramy połączenia w DMZ** nie jest obsługiwana w systemie Microsoft Windows opartym na architekturze ARM.

- Zmiany wprowadzone w harmonogramie zadań nie są propagowane do zarządzanych urządzeń, jeśli harmonogram korzysta z ustawienia „ **Według dni tygodnia** . Jeśli chcesz zmienić harmonogram, usuń istniejące zadanie i utwórz nowe ze zaktualizowanymi ustawieniami.

- Informacje o komponentach zarządzanych aplikacji nie są dostępne, jeśli Agent sieciowy jest zainstalowany w systemie Microsoft Windows XP.

- Konsola wyświetla podsekcję **Alerty** w sekcji **Monitorowanie i raportowanie** menu głównego tylko wtedy, gdy dodałeś klucz licencyjny dla EDR Optimum do repozytorium Serwera administracyjnego poprzez wprowadzenie kodu aktywacyjnego.

- Aby zagwarantować siłę szyfrowania, certyfikat Serwera administracyjnego musi być podpisany za pomocą algorytmu SHA-2 i mieć klucz o minimalnej długości 2048. Jeśli musisz ponownie wystawić certyfikat, zapoznaj się z bazą wiedzy Kaspersky Security Center.

- Jeśli utworzysz zadanie z ustawieniami harmonogramu **Co N dni** i **Według dni tygodnia** w Kaspersky Security Center 15.1 Web Console, a następnie otworzysz zadanie w starszych wersjach Kaspersky Security Center Web Console lub Konsoli administracyjnej Kaspersky Security Center (na przykład, gdy zadanie jest również stosowane na pomocniczych serwerach administracyjnych, które mogą być zarówno oparte na systemie Linux, jak i Windows), ustawienia harmonogramu mogą być wyświetlane nieprawidłowo lub może wystąpić błąd.

- Podczas konfigurowania eksportu do systemów SIEM w Kaspersky Security Center Web Console i wybierania protokołu UDP po kliknięciu przycisku **Sprawdź połączenie** zwracany jest błąd, ponieważ protokół UDP nie nawiązuje połączenia i nie można zagwarantować dostarczenia danych.

- Po uruchomieniu zadania mającego na celu usunięcie Agenta sieciowego z urządzenia opartego na architekturze Arm i działającego pod kontrolą systemu Astra Linux Special Edition RUSB.10015-01 (aktualizacja operacyjna 1.7), Agent sieciowy zostanie pomyślnie usunięty, ale stan zadania dla bieżącego postępu na liście zadań zostanie zamrożony.

- Okno właściwości zasad Kaspersky Device Management for iOS nadal zawiera sekcję **Ustawienia urządzeń EAS**, mimo że protokół Exchange ActiveSync nie jest już obsługiwany.

- Połączenie z KSN za pośrednictwem protokołu HTTPS nie powiedzie się, jeśli Kaspersky Security Center jest zainstalowany na urządzeniu, którego nazwa zawiera symbole cyrylicy, a na Serwerze administracyjnym włączony jest KSN Proxy.

- Gdy próbujesz zmienić właściwości konta użytkownika, dla którego włączono opcję **Żądaj uwierzytelnienia w celu sprawdzenia uprawnień do modyfikacji kont użytkowników**, a następnie klikasz **Anuluj** w oknie **Ochrona konta**, występuje nieoczekiwany błąd.

- Jeśli zmienisz czas lub strefę czasową na swoim urządzeniu, musisz ponownie uruchomić usługę Kaspersky Security Center Web Console.

- Jeśli na urządzeniu używany jest serwer proxy i ustawione są zmienne środowiskowe serwera proxy, instalator Kaspersky Security Center Web Console może się zawiesić.

- W przypadku importowania zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* lub zadania *Weryfikacja uaktualnień*, włączona jest opcja **Wybierz urządzenia, do których zadanie zostanie przypisane**. Zadań tych nie można przypisać do wyboru urządzenia ani do określonych urządzeń. W przypadku przypisania zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* lub zadania *Weryfikacja aktualizacji* do określonych urządzeń, zadanie zostanie zaimportowane niepoprawnie.

- Jeśli przeprowadzasz odpytywanie usługi Active Directory przy użyciu punktu dystrybucji systemu Linux z zainstalowanym Agentem sieciowym w wersji 15, możesz odpytywać tylko domeny usługi Active Directory, dla których określisz adres i poświadczenia użytkownika. Sondowanie bieżącej domeny Active Directory i lasu domeny Active Directory nie jest dostępne.

- Urządzenia klienckie mogą nie zostać znalezione po uruchomieniu sondowania sieci systemu Windows.

- Jeśli w **Kreatorze dodawania podrzędnego Serwera administracyjnego** określisz konto z włączoną weryfikacją dwuetapową do uwierzytelniania na przyszłym Serwerze podrzędnym, kreator zakończy działanie z błędem. Aby rozwiązać ten problem, określ konto, dla którego weryfikacja dwuetapowa jest wyłączona, lub utwórz hierarchię z przyszłego serwera pomocniczego.

- Jeśli podczas logowania do Kaspersky Security Center Web Console, używasz uwierzytelniania domeny i określisz wirtualny Serwer administracyjny, z którym chcesz się połączyć, wylogujesz się, a następnie spróbujesz zalogować do głównego Serwera administracyjnego, Kaspersky Security Center Web Console połączy się do wirtualnego Serwera administracyjnego. Aby połączyć się z głównym Serwerem administracyjnym, ponownie otwórz przeglądarkę.

- Szybkie/Pełne przeszukiwanie sieci Windows zwraca pusty wynik.

- Jeśli zainstalujesz Kaspersky Security Center Web Console z Identity and Access Manager, a następnie zmienisz Serwer administracyjny na Kaspersky Security Center Web Console, Identity and Access Manager nie otrzyma informacji o nowym Serwerze administracyjnym.

- Zarządzane urządzenie, które ma więcej niż jedną kartę sieciową, wysyła do Serwera administracyjnego informacje o adresie MAC karty sieciowej, która nie jest używana do łączenia się z Serwerem administracyjnym.

- Połączenie testowe z SIEM kończy się niepowodzeniem po wybraniu formatu danych CEF.

- Uwierzytelnianie NTLM nie działa dla kont użytkowników należących do grupy Chronieni użytkownicy.