kaspersky

Kaspersky Endpoint Security 14.1 for Windows

© 2026 AO Kaspersky Lab

Spis treści

Pomoc dla Kaspersky Endpoint Security for Windows
- Nowości
- Naprawione problemy
- Najczęściej zadawane pytania

Kaspersky Endpoint Security for Windows
- Tryby aplikacji: Standardowy, EDR Agent, Light Agent
- Pakiet dystrybucyjny
- Wymagania sprzętowe i programowe
- Porównanie dostępnych funkcji aplikacji w zależności od typu systemu operacyjnego
- Porównanie funkcji aplikacji w zależności od narzędzi do zarządzania
- Kompatybilność z innymi aplikacjami

Instalowanie i dezinstalowanie aplikacji
- Wdrożenie za pośrednictwem Kaspersky Security Center
  - Standardowa instalacja aplikacji
  - Tworzenie pakietu instalacyjnego
  - Aktualizowanie baz danych w pakiecie instalacyjnym
  - Tworzenie zadania zdalnej instalacji
- Instalowanie aplikacji lokalnie przy użyciu kreatora
- Zdalne instalowanie aplikacji przy użyciu System Center Configuration Manager
- Opis ustawień instalacji pliku setup.ini
- Zmiana składników aplikacji
- Aktualizowanie poprzedniej wersji aplikacji
  - Aktualizacja aplikacji bez ponownego uruchomienia
  - Aktualizacja SMU aplikacji
- Dezinstalacja aplikacji

Licencjonowanie aplikacji
- Informacje o Umowie licencyjnej
- Informacje o licencji
- Informacje o certyfikacie licencji
- Informacje o subskrypcji
- Informacje o kluczu licencyjnym
- Informacje o kodzie aktywacyjnym
- Informacje o pliku klucza
- Porównanie funkcjonalności aplikacji w zależności od typu licencji dla stacji roboczych
- Porównanie funkcjonalności aplikacji w zależności od typu licencji dla serwerów
- Aktywowanie aplikacji
- Usuwanie klucza licencyjnego
- Przeglądanie informacji o licencji
- Kupowanie licencji
- Odnawianie subskrypcji

Rozpoczęcie pracy
- Informacje o wtyczce zarządzającej Kaspersky Endpoint Security for Windows
- Kwestie specjalne dotyczące pracy z różnymi wersjami wtyczek zarządzających

- Kwestie specjalne podczas używania zaszyfrowanych protokołów do interakcji z zewnętrznymi usługami
- Interfejs aplikacji
  - Ikona aplikacji w obszarze powiadomień paska zadań
  - Uproszczony interfejs aplikacji
  - Konfigurowanie wyświetlania interfejsu aplikacji
- Przygotowanie aplikacji do użytku
- Zarządzanie profilami
  - Tworzenie profilu
  - Eksportowanie i importowanie zasad
  - Wskaźnik poziomu ochrony
- Zarządzanie zadaniami
- Konfigurowanie lokalnych ustawień aplikacji
- Uruchamianie i zatrzymywanie Kaspersky Endpoint Security
- Wstrzymywanie i wznawianie kontroli i ochrony komputera
- Tworzenie i korzystanie z pliku konfiguracyjnego
- Przywracanie ustawień domyślnych aplikacji
- Działanie Kaspersky Endpoint Security i kompatybilność z innymi aplikacjami
  - Włączanie i wyłączanie trybu oszczędzania energii
  - Włączanie i wyłączanie udostępniania zasobów innym aplikacjom
  - Praktyczne zastosowanie aplikacji do optymalizowania wydajności Kaspersky Endpoint Security

Skanowanie w poszukiwaniu złośliwego oprogramowania
- Skanowanie komputera
- Skanowanie napędów wymiennych po ich podłączeniu do komputera
- Skanowanie w tle
- Skanowanie z menu kontekstowego
- Sprawdzanie integralności aplikacji
- Modyfikowanie obszaru skanowania
- Uruchamianie zaplanowanego skanowania
- Uruchamianie skanowania jako inny użytkownik
- Optymalizacja skanowania

Aktualizowanie baz danych i modułów aplikacji
- Scenariusze aktualizacji baz danych i modułów aplikacji
  - Aktualizowanie z repozytorium serwera
  - Aktualizowanie z folderu współdzielonego
  - Aktualizowanie przy użyciu narzędzia Kaspersky Update Utility
  - Aktualizowanie w trybie mobilnym
- Uruchamianie i zatrzymywanie zadania aktualizacji
- Uruchamianie zadania aktualizacji z poziomu konta innego użytkownika
- Wybieranie trybu uruchamiania zadania aktualizacji
- Dodawanie źródła uaktualnień
- Aktualizowanie modułów aplikacji
- Używanie serwera proxy do aktualizacji
- Wycofanie ostatniej aktualizacji

Używanie technologii zaawansowanego leczenia
- Leczenie aktywnych zagrożeń na stacjach roboczych
- Leczenie aktywnych zagrożeń na serwerach

Eliminowanie nieprzetworzonych zagrożeń

Ochrona komputera
Ochrona plików
Włączanie i wyłączanie modułu Ochrona plików
Automatyczne wstrzymywanie Ochrony plików
Zmienianie akcji wykonywanej na zainfekowanych plikach przez moduł Ochrona plików
Tworzenie obszaru ochrony modułu Ochrona plików
Używanie metod skanowania
Używanie technologii skanowania w działaniu modułu Ochrona plików
Optymalizowanie skanowania plików
Skanowanie plików złożonych
Zmienianie trybu skanowania
Skanowanie kontenerów
Ochrona przed włamaniami
Włączanie i wyłączanie modułu Ochrona przed włamaniami
Zarządzanie grupami zaufania aplikacji
Zmiana grupy zaufania aplikacji
Konfigurowanie uprawnień grupy zaufania
Wybieranie grupy zaufania dla aplikacji uruchamianych przed Kaspersky Endpoint Security
Wybieranie grupy zaufania dla nieznanych aplikacji
Wybieranie grupy zaufania dla cyfrowo podpisanych aplikacji
Zarządzanie uprawnieniami aplikacji
Ochrona zasobów systemu operacyjnego i danych osobowych
Usuwanie informacji o nieużywanych aplikacjach
Monitorowanie Ochrony przed włamaniami
Ochrona dostępu do audio i wideo
Ochrona przed atakami BadUSB
Włączanie i wyłączanie Ochrony przed atakami BadUSB
Korzystanie z Klawiatury ekranowej do autoryzacji urządzeń USB
Autoryzacja czytnika kodów kreskowych
Ochrona AMSI
Włączanie i wyłączanie Ochrony AMSI
Optymalizacja skanowania plików przez Ochronę AMSI
Ochrona WWW
Włączanie i wyłączanie modułu Ochrona WWW
Konfigurowanie metod wykrywania szkodliwych adresów internetowych
Anti-Phishing
Tworzenie listy zaufanych adresów internetowych
Eksportowanie i importowanie listy zaufanych adresów internetowych
Ochrona poczty
Włączanie i wyłączanie modułu Ochrona poczty
Zmienianie akcji podejmowanej na zainfekowanych wiadomościach e-mail
Tworzenie obszaru ochrony modułu Ochrona poczty
Skanowanie plików złożonych załączonych do wiadomości e-mail
Filtrowanie załączników wiadomości e-mail
Eksportowanie i importowanie rozszerzeń dla filtrowania załączników
Skanowanie poczty elektronicznej w programie Microsoft Office Outlook
Skanowanie wiadomości e-mail w Thunderbird, MyOffice, R7-Office

Ochrona sieci
- Włączanie i wyłączanie modułu Ochrona sieci
- Blokowanie atakującego komputera
- Konfigurowanie wykluczania adresów z blokowania
- Eksportowanie i importowanie listy wykluczeń z blokowania
- Konfigurowanie Ochrony sieci według typu

Zapora sieciowa
- Włączanie i wyłączanie modułu Zapora sieciowa
- Zmiana typu połączenia sieciowego
- Zarządzanie regułami dla pakietów sieciowych
  - Tworzenie reguły dla pakietu sieciowego.
  - Włączanie i wyłączanie reguły dla pakietu sieciowego
  - Zmienianie akcji Zapory sieciowej dla reguły dla pakietu sieciowego
  - Zmienianie priorytetu reguły dla pakietu sieciowego
  - Eksportowanie i importowanie reguł dla pakietów sieciowych
  - Definiowanie reguł pakietów sieciowych w pliku XML
- Zarządzanie regułami sieciowymi dla aplikacji
  - Tworzenie reguły sieciowej dla aplikacji
  - Włączanie i wyłączanie reguły sieciowej dla aplikacji
  - Zmienianie akcji Zapory sieciowej dla reguły sieciowej dla aplikacji
  - Zmienianie priorytetu reguły sieciowej dla aplikacji
- Monitor sieci

Ochrona przed exploitami
- Włączanie i wyłączanie modułu Ochrona przed exploitami
- Ochrona pamięci procesów systemowych

Wykrywanie zachowań

Anti-Cryptor
- Włączanie i wyłączanie ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym
- Konfigurowanie okresu blokowania niezaufanego komputera
- Modyfikowanie zakresu ochrony
- Dodawanie zaufanych komputerów na potrzeby zewnętrznego szyfrowania danych
- Eksportowanie i importowanie listy wykluczeń z ochrony folderów współdzielonych przed zewnętrznym szyfrowaniem

Silnik korygujący

Kaspersky Security Network
- Włączanie i wyłączanie korzystania z Kaspersky Security Network
- Ograniczenia Kaspersky Private Security Network
- Włączanie i wyłączanie dla składników ochrony trybu chmury
- Ustawienia proxy KSN
- Sprawdzanie reputacji pliku w Kaspersky Security Network

Skanowanie połączeń szyfrowanych
- Włączanie skanowania połączeń szyfrowanych
- Instalowanie zaufanych certyfikatów głównych
- Skanowanie połączeń szyfrowanych z użyciem niezaufanego certyfikatu
- Dodawanie certyfikatu Kaspersky do własnego magazynu certyfikatów
- Wyłączanie połączeń szyfrowanych ze skanowania

Wyczyść dane

Kontrola komputera
Kontrola sieci
Dodawanie reguły dostępu do zasobu sieciowego
Filtrowanie według adresów zasobów sieciowych
Filtrowanie według zawartości zasobów sieciowych
Testowanie reguł dostępu do zasobów sieciowych
Eksportowanie i importowanie reguł kontroli sieci
Eksportowanie i importowanie adresów zasobu sieciowego z reguły Kontroli sieci
Monitorowanie aktywności użytkownika w internecie
Modyfikowanie szablonów wiadomości Kontroli sieci
Modyfikowanie masek adresów zasobów sieciowych
Kontrola sieci dla maszyn wirtualnych
Zmienne w szablonach komunikatów komponentu Kontrola sieci
Kontrola urządzeń
Informacje o regułach dostępu
Zarządzanie dostępem do urządzeń według typu
Zarządzanie dostępem do urządzeń za pomocą magistrali połączeniowej
Różnicowanie praw dostępu użytkowników do urządzeń
Zarządzanie dostępem do urządzeń mobilnych
Zarządzanie dostępem do urządzeń Bluetooth.
Kontrola wydruku
Kontrola połączeń Wi-Fi
Monitorowanie korzystania z nośników wymiennych
Zmiana czasu trwania buforowania
Działania podejmowane na zaufanych urządzeniach
Dodawanie urządzenia do listy Zaufane z poziomu interfejsu aplikacji
Dodawanie urządzenia do listy Zaufane z poziomu Kaspersky Security Center
Eksportowanie i importowanie listy zaufanych urządzeń
Uzyskiwanie dostępu do zablokowanego urządzenia
Tryb online dla zezwalania na dostęp
Tryb offline dla zezwalania na dostęp
Modyfikowanie szablonów wiadomości Kontroli urządzeń
Anti-Bridging
Włączanie modułu Anti-Bridging
Zmiana stanu reguły połączenia
Zmiana priorytetu reguły połączenia
Adaptacyjna kontrola anomalii
Uczenie modułu Adaptacyjna kontrola anomalii
Włączanie i wyłączanie reguły Adaptacyjnej kontroli anomalii
Modyfikowanie akcji podejmowanej w momencie wyzwolenia reguły Adaptacyjnej kontroli anomalii
Tworzenie wykluczeń dla reguły Adaptacyjnej kontroli anomalii
Eksportowanie i importowanie wykluczeń dla reguł Adaptacyjnej kontroli anomalii
Stosowanie aktualizacji dla reguł Adaptacyjnej kontroli anomalii
Modyfikowanie szablonów wiadomości Adaptacyjnej kontroli anomalii
Monitorowanie działania Adaptacyjnej kontroli anomalii

- Kontrola aplikacji
  - Ograniczenia funkcjonalności Kontroli aplikacji
  - Otrzymywanie informacji o aplikacjach zainstalowanych na komputerach użytkowników
  - Jak włączyć tryb zablokowanych aplikacji?
  - Kontrola aplikacji na podstawie komputera bazowego
  - Zarządzanie regułami Kontroli aplikacji
    - Dodawanie warunku wyzwalającego dla reguły Kontroli aplikacji
    - Dodawanie plików wykonywalnych z folderu Pliki wykonywalne do kategorii aplikacji
    - Dodawanie plików wykonywalnych związanych ze zdarzeniami do kategorii aplikacji
    - Dodawanie reguły Kontroli aplikacji
    - Zmienianie stanu reguły Kontroli aplikacji przy użyciu Kaspersky Security Center
    - Eksportowanie i importowanie reguł Kontroli aplikacji
    - Przeglądanie zdarzeń z działania modułu Kontrola aplikacji
    - Przeglądanie raportu dotyczącego zablokowanych aplikacji
  - Testowanie działania reguł Kontroli aplikacji
    - Włączanie i wyłączanie testowania reguł modułu Kontrola Aplikacji
    - Przeglądanie raportu dotyczącego zablokowanych aplikacji w trybie testowym
    - Przeglądanie zdarzeń z działania testowego komponentu Kontrola aplikacji
  - Monitor aktywności aplikacji
  - Reguły tworzenia masek nazw dla plików i folderów
  - Modyfikowanie szablonów wiadomości Kontroli aplikacji
  - Zmienne w szablonach wiadomości komponentu Kontrola aplikacji
  - Praktyczne zastosowanie aplikacji w celu zaimplementowania listy dozwolonych aplikacji
    - Konfigurowanie trybu listy zezwolonych aplikacji
    - Testowanie trybu listy zezwolonych
    - Obsługa listy zezwolonych aplikacji
- Monitorowanie portów sieciowych
  - Włączanie monitorowania wszystkich portów sieciowych
  - Tworzenie listy monitorowanych portów sieciowych
  - Tworzenie listy aplikacji, dla których monitorowane są wszystkie porty sieciowe
  - Eksportowanie i importowanie list monitorowanych portów
- Kontrola dziennika
  - Konfiguracja wstępnie zdefiniowanych reguł
  - Dodawanie reguł niestandardowych
- Monitor integralności systemu
  - Informacje o regułach monitorowania integralności systemu
  - Monitorowanie integralności systemu w czasie rzeczywistym
  - Sprawdzanie integralności systemu na żądanie
  - Eksportowanie i importowanie reguł Monitorowania integralności systemu
  - Podgląd raportów Monitorowania integralności systemu
  - Reset statusu integralności systemu
- Cloud Discovery

Strefa zaufana

- Tworzenie wykluczenia ze skanowania
- Tworzenie wykluczenia według typu wykrytych obiektów
- Modyfikowanie listy zaufanych aplikacji
- Tworzenie lokalnej strefy zaufanej

- Eksportowanie i importowanie zaufanych stref
- Obsługa aplikacji z zaufanym podpisem cyfrowym
- Dodatek. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje
  - Serwer SQL
  - Serwer Microsoft Exchange
  - System Center Configuration Manager
  - Citrix
  - VMware
- Zarządzanie Kopią zapasową
  - Konfigurowanie maksymalnego okresu przechowywania plików w Kopii zapasowej
  - Konfigurowanie maksymalnego rozmiaru Kopii zapasowej
  - Przywracanie plików z Kopii zapasowej
  - Usuwanie kopii zapasowych plików z Kopii zapasowej
- Usługa powiadomień
  - Konfigurowanie ustawień dziennika zdarzeń
  - Konfigurowanie wyświetlania i dostarczania powiadomień
  - Konfigurowanie wyświetlania komunikatów o stanie aplikacji w obszarze powiadomień
  - Przesyłanie wiadomości między użytkownikami a administratorem
- Zarządzanie raportami
  - Wyświetlanie raportów
  - Konfigurowanie maksymalnego czasu przechowywania raportu
  - Konfigurowanie maksymalnego rozmiaru pliku raportu
  - Zapisywanie raportu do pliku
  - Czyszczenie raportów
- Autoochrona Kaspersky Endpoint Security
  - Włączanie i wyłączanie Autoochrony
  - Włączanie i wyłączanie obsługi AM-PPL
  - Ochrona usług aplikacji przed zewnętrznym zarządzaniem
  - Obsługiwanie aplikacji do zdalnej administracji
  - Ochrona hasłem
    - Włączanie ochrony hasłem
    - Nadawanie uprawnień pojedynczym użytkownikom lub grupom
    - Używanie hasła tymczasowego do nadawania uprawnień
    - Unieważnienie tymczasowego hasła
    - Specjalne kwestie dotyczące uprawnień Ochrony hasłem
    - Resetowanie hasła KLAdmin
  - Ochrona połączenia z Serwerem administracyjnym
- Szyfrowanie danych
  - Ograniczenia funkcji szyfrowania
  - Zmiana długości klucza szyfrowania (AES56 / AES256)
  - Kaspersky Disk Encryption
    - Specjalne funkcje szyfrowania dysku SSD
    - Uruchamianie Kaspersky Disk Encryption
    - Tworzenie listy dysków twardych wykluczonych z szyfrowania
    - Eksportowanie i importowanie listy dysków twardych wykluczonych z szyfrowania
    - Włączanie technologii Single Sign-On (SSO)
    - Zarządzanie kontami Agenta autoryzacji

- Używanie tokenów i kart inteligentnych z Agentem autoryzacji
- Deszyfrowanie dysków twardych
- Przywracanie dostępu do dysku chronionego przez technologię Kaspersky Disk Encryption
- Logowanie z użyciem konta usługi Agenta autoryzacji
- Aktualizowanie systemu operacyjnego
- Eliminowanie błędów aktualizacji funkcjonalności szyfrowania
- Śledzenie Agenta autoryzacji
- Modyfikowanie komunikatów pomocy Agenta Autoryzacji
- Usuwanie obiektów i danych pozostałych po testowym działaniu Agenta autoryzacji
- Zarządzanie BitLocker
  - Uruchamianie Szyfrowania dysków funkcją BitLocker
  - Deszyfrowanie dysku twardego chronionego przez funkcję BitLocker
  - Przywracanie dostępu do dysku chronionego funkcją BitLocker
  - Wstrzymywanie ochrony funkcją BitLocker w celu zaktualizowania oprogramowania
- Szyfrowanie na poziomie plików na lokalnych dyskach komputera
  - Szyfrowanie plików na lokalnych dyskach komputera
  - Tworzenie reguł dostępu do zaszyfrowanego pliku dla aplikacji
  - Szyfrowanie plików utworzonych lub zmodyfikowanych przez określone aplikacje
  - Generowanie reguły deszyfrowania
  - Deszyfrowanie plików na lokalnych dyskach komputera
  - Tworzenie zaszyfrowanych pakietów
  - Przywracanie dostępu do zaszyfrowanych plików
  - Przywracanie dostępu do zaszyfrowanych danych po awarii systemu operacyjnego
  - Modyfikowanie szablonów wiadomości dostępu do zaszyfrowanego pliku
- Szyfrowanie nośników wymiennych
  - Uruchamianie szyfrowania nośników wymiennych
  - Dodawanie reguły szyfrowania dla nośników wymiennych
  - Eksportowanie i importowanie listy reguł szyfrowania dla nośników wymiennych
  - Tryb przenośny dla uzyskiwania dostępu do zaszyfrowanych plików na dyskach wymiennych
  - Deszyfrowanie nośników wymiennych
- Przeglądanie informacji szczegółowych dotyczących szyfrowania danych
  - Sprawdzanie stanu szyfrowania
  - Przeglądanie statystyk szyfrowania dotyczących pulpitów nawigacyjnych Kaspersky Security Center
  - Przeglądanie błędów szyfrowania plików na lokalnych dyskach komputera
  - Przeglądanie raportu z szyfrowania danych
- Praca z zaszyfrowanymi urządzeniami, gdy nie ma dostępu do nich
  - Odzyskiwanie danych za pomocą narzędzia przywracania FDERT
  - Tworzenie dysku ratunkowego systemu operacyjnego
- Rozwiązania Detection and Response
  - Licencje MDR i EDR Optimum
  - Kompatybilność z rozwiązaniami EDR innych firm
  - Kaspersky Endpoint Agent
    - Migracja konfiguracji [KES+KEA] do konfiguracji [KES+wbudowany agent]
    - Migracja zasad i zadań dla Kaspersky Endpoint Agent
  - Endpoint Detection and Response Agent (EDR Agent)
    - Instalowanie EDR Agent
    - Integracja EDR Agent z MDR

- Integracja EDR Agent z EDR (KATA)
- Integracja EDR Agent z NDR (KATA)
- Integracja agenta EDR z EDR Expert (on-premises)
- Kompatybilność z aplikacjami EPP innych firm

Managed Detection and Response
- Integracja wbudowanego agenta z MDR
- Przewodnik migracji z KEA do KES dla MDR

Endpoint Detection and Response
- Integracja wbudowanego agenta z EDR Optimum / EDR Expert
- Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa (zadanie standardowe)
- Rozszerzona telemetria dla Skanowania IOC
- Przenieś plik do Kwarantanny
- Uzyskaj plik
- Usuń plik
- Rozpoczęcie procesu
- Kończenie działania procesu
- Zapobieganie wykonywaniu
- Izolacja sieci komputerowej
- Cloud Sandbox
- Przewodnik migracji z KEA do KES dla EDR Optimum

Kaspersky Sandbox
- Integracja wbudowanego agenta z ze środowiskiem testowym "Kaspersky Sandbox"
- Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa (zadanie autonomiczne)
- Przewodnik migracji z KEA do KES dla Kaspersky Sandbox

Kaspersky Anti Targeted Attack Platform
- Integracja wbudowanego agenta z EDR / NDR (KATA)
- Konfiguracja telemetrii EDR (KATA)
- Wykluczenia telemetryczne EDR (KATA)
  - Przykład 1. Wykluczone procesy
  - Przykład 2. Wykluczona komunikacja sieciowa
  - Przykład 3. Wykluczone operacje na plikach
  - Przykład 4. Wykluczone modyfikacje rejestru
- KATA Sandbox
  - Integracja wbudowanego agenta z ze środowiskiem testowym "KATA Sandbox"
  - Konfigurowanie akcji Threat Response
- Przewodnik migracji z KEA do KES dla EDR (KATA)

Endpoint Detection and Response Expert (on-premises)
- Integracja wbudowanego agenta z EDR Expert (on-premises)
- Konfigurowanie ustawień telemetrii EDR Expert (on-premises)
- Wykluczenia telemetrii EDR Expert (on-premises)
- Eksportowanie i importowanie filtrów zdarzeń EDR Expert (on-premises)
- Szczególne uwagi dotyczące używania profili zasad do konfigurowania integracji z EDR Expert (on-premises) i EDR (KATA)

Endpoint Detection and Response Expert (cloud)
- Integracja wbudowanego agenta z EDR Expert (cloud)
- Konfigurowanie ustawień telemetrii EDR Expert (cloud)
- Wykluczenia telemetrii EDR Expert (cloud)
- Eksportowanie i importowanie filtrów zdarzeń EDR Expert (cloud)

- Zarządzanie Kwarantanną
  - Konfigurowanie maksymalnego rozmiaru Kwarantanny
  - Wysyłanie danych o plikach poddanych kwarantannie do Kaspersky Security Center
  - Przywracanie plików z Kwarantanny
- Monitorowanie działań EDR

Kaspersky Unified Monitoring and Analysis Platform (KUMA)
- Integracja Kaspersky Endpoint Security z KUMA
- Filtrowanie zdarzeń, które mają zostać wysłane do KUMA
- Eksportowanie i importowanie filtrów zdarzeń KUMA

Przewodnik migracji z KSWS do KES
- Zgodność komponentów KSWS i KES
- Zgodność ustawień KSWS i KES
- Migracja komponentów KSWS
- Migracja zadań i zasad KSWS
- Migracja strefy zaufanej KSWS
- Migracja reguł zadania Kontrola uruchamiania aplikacji KSWS
- Instalowanie KES zamiast KSWS
- Migracja konfiguracji [KSWS+KEA] do konfiguracji [KES+wbudowany agent]
- Upewnianie się, że pomyślnie usunięto Kaspersky Security for Windows Server
- Aktywowanie KES przy użyciu klucza dla KSWS
- Specjalne kwestie dotyczące migracji serwerów o dużym obciążeniu
- Zarządzanie aplikacją na serwerze w trybie Server Core
- Migracja konfiguracji [KSWS+KEA] do konfiguracji [KES+built-in agent]

Tryb Light Agent do ochrony maszyn wirtualnych
- Specjalne uwagi dotyczące trybu Light Agent
- Wstępna konfiguracja maszyny wirtualnej
  - Zgodność z technologią Citrix App Layering
  - Zgodność z technologią Citrix Provisioning (Citrix Provisioning Services)
  - Zgodność z technologią Omnissa App Volumes
- Instalowanie klienta Light Agent
- Łączenie klienta Light Agent z maszyną SVM
  - Wykrywanie maszyn SVM
  - Konfigurowanie algorytmu wyboru SVM na potrzeby klienta Light Agent
  - Dystrybucja połączeń klientów Light Agent z maszynami SVM (znaczniki)
  - Ochrona połączenia między klientem Light Agent a maszyną SVM
- Aktywacja klienta Light Agent
- Przewodnik migracji z KSVLA Light Agent do KES Light Agent
  - Instalowanie KES Light Agent zamiast KSVLA Light Agent
  - Zgodność komponentów KSVLA Light Agent i KES Light Agent
  - Migracja zadań i zasad KSVLA Light Agent
  - Migracja konfiguracji [KSVLA Light Agent+KEA] do konfiguracji [KES Light Agent+wbudowany agent]

Zarządzanie aplikacją z poziomu wiersza poleceń
- Setup. Instalowanie aplikacji
- Setup /x. Dezinstalacja aplikacji
- msiexec /i. Odzyskiwanie aplikacji

Polecenia AVP
- SCAN. Skanowanie w poszukiwaniu złośliwego oprogramowania
- UPDATE. Aktualizowanie baz danych i modułów aplikacji
- ROLLBACK. Wycofanie ostatniej aktualizacji
- TRACES. Śledzenie
- START. Uruchamianie profilu
- STOP. Zatrzymywanie profilu
- STAN. Stan profilu
- STATISTICS. Statystyki działania profilu
- RESTORE. Przywracanie plików z Kopii zapasowej
- EXPORT. Eksportowanie ustawień aplikacji
- IMPORT. Importowanie ustawień aplikacji
- ADDKEY. Zastosowanie pliku klucza
- LICENSE. Licencjonowanie
- RENEW. Kupowanie licencji
- PBATESTRESET. Resetowanie wyników sprawdzania dysku przed zaszyfrowaniem dysku
- EXIT. Zakończenie działania aplikacji
- EXITPOLICY. Wyłączanie profilu
- STARTPOLICY. Włączanie profilu
- DISABLE. Wyłączanie ochrony
- SPYWARE. Wykrywanie oprogramowania szpiegującego
- KSN. Przełączanie między KSN / KPSN
- SERVERBINDINGDISABLE. Wyłączanie ochrony połączenia z serwerem

Polecenia KESCLI
- Scan. Skanowanie w poszukiwaniu złośliwego oprogramowania
- GetScanState. Stan zakończenia skanowania
- GetLastScanTime. Określanie czasu zakończenia skanowania
- GetThreats. Uzyskiwanie danych dotyczących wykrytych zagrożeń
- UpdateDefinitions. Aktualizowanie baz danych i modułów aplikacji
- GetDefinitionState. Określenie daty i godziny ostatniej aktualizacji baz danych
- EnableRTP. Włączanie ochrony
- GetRealTimeProtectionState. Stan Ochrony plików
- GetEncryptionState. Stan szyfrowania dysku
- Version. Identyfikowanie wersji aplikacji

Polecenia zarządzania Detection and Response
- SANDBOX. Zarządzanie Sandbox
- PREVENTION. Zarządzanie zapobieganiem wykonaniu
- ISOLATION. Zarządzanie Izolacją sieci
- RESTORE. Przywracanie plików z Kwarantanny
- IOCSCAN. Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa (IOC)
- MDRLICENSE. Aktywacja MDR
- EDRKATA. Integracja z EDR (KATA)
- KUMA. Integracja z KUMA
- YARA. Uruchamianie skanowania YARA
- TELEMETRYFILTERS. Filtrowanie zdarzeń, które mają zostać wysłane do KUMA

Polecenia do zarządzania klientem Light Agent
KSVLAINFO. Określanie trybu klienta Light Agent
VIISINFO. Stan połączeniu klienta Light Agent z serwerem integracyjnym
SVMINFO. Stan połączeniu klienta Light Agent z serwerem ochrony
Kody błędów
Dodatek. Profile aplikacji
Zarządzanie aplikacją za pośrednictwem interfejsu API REST
Instalowanie aplikacji za pośrednictwem interfejsu API REST
Praca z interfejsem API
Źródła informacji o aplikacji
Kontakt z działem pomocy technicznej
Zawartość i przechowywanie plików śledzenia
Śledzenie działania aplikacji
Śledzenie wydajności aplikacji
Zapisywanie zrzutu pamięci
Ochrona plików zrzutu i plików śledzenia
Uzyskiwanie danych systemu operacyjnego (Kaspersky Get System Info)
Ograniczenia i uwagi
Słownik
Agent autoryzacji
Agent sieciowy
Aktywny klucz
Antywirusowe bazy danych
Archiwum
Baza adresów phishingowych
Baza danych szkodliwych adresów internetowych
Certyfikat licencji
Cloud Discovery
Fałszywy alarm
Grupa administracyjna
IOC
Leczenie
Light Agent
Maska
Obiekt OLE
Obszar ochrony
Obszar skanowania
OpenIOC
Plik infekowalny
Plik IOC
Przenośny menedżer plików
Serwer integracyjny
SVM
Trusted Platform Module (moduł TPM)
Uwierzytelnianie Kerberos
Wystawca certyfikatu
Zadanie

Zainfekowany plik
Znormalizowana postać adresu zasobu sieciowego
Dodatki
Dodatek 1. Ustawienia aplikacji
Ochrona plików
Ochrona WWW
Ochrona poczty
Ochrona sieci
Zapora sieciowa
Ochrona przed atakami BadUSB
Ochrona AMSI
Ochrona przed exploitami
Wykrywanie zachowań
Ochrona przed włamaniami
Silnik korygujący
Kaspersky Security Network
Kontrola dziennika
Anti-Cryptor
Kontrola sieci
Kontrola urządzeń
Kontrola aplikacji
Adaptacyjna kontrola anomalii
Monitor integralności systemu
Endpoint Sensor
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert (on-premises)
Network Detection and Response (KATA)
Integracja z KUMA
Szyfrowanie całego dysku
Szyfrowanie plików
Szyfrowanie nośników wymiennych
Szablony (szyfrowanie danych)
Wykluczenia
Ustawienia aplikacji
Raporty i Kopia zapasowa
Ustawienia sieci
Interfejs
Zarządzaj ustawieniami
Aktualizowanie baz danych i modułów aplikacji
Dodatek 2. Grupy zaufania aplikacji
Dodatek 3. Rozszerzenia plików do szybkiego skanowania dysków wymiennych
Dodatek 4. Typy plików dla filtra załączników modułu Ochrona poczty
Dodatek 5. Ustawienia sieci do interakcji z usługami zewnętrznymi

Dodatek 6. Zdarzenia aplikacji
Krytyczny
Błąd funkcjonalny
Ostrzeżenie
Wiadomość informacyjna
Dodatek 7. Obsługiwane rozszerzenia plików dla Zapobiegania wykonywaniu
Dodatek 8. Obsługiwane interpretery skryptów do usługi Zapobiegania wykonywaniu
Dodatek 9. Obszar skanowania IOC w rejestrze (RegistryItem)
Dodatek 10. Wymagania pliku IOC
Dodatek 11. Interfejs API dla usługi reagowania na zagrożenia EDR
Dodatek 12. Konta użytkowników w regułach składników aplikacji
Informacje prawne
Przekazywanie danych
Przekazywanie danych zgodnie z Umową licencyjną
Przekazywanie danych podczas korzystania z Kaspersky Security Network
Przekazywanie danych podczas korzystania z rozwiązań Detection and Response
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
Integracja z Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Zgodność z prawem Unii Europejskiej (RODO)
Informacje o znakach towarowych
Informacje o kodzie firm trzecich

Pomoc dla Kaspersky Endpoint Security for Windows

Nowości

Aktualizacja 14.1

W programie Kaspersky Endpoint Security 14.1 for Windows wprowadzono następujące funkcje i ulepszenia:

1. Dodano obsługę systemu operacyjnego Windows Server 2025.

2. Zwiększono limit liczby reguł filtrowania zdarzeń telemetrycznych dla Endpoint Detection and Response Expert (on-premises) i Kaspersky Endpoint Detection and Response Expert (cloud). Kaspersky Endpoint Security obsługuje teraz łącznie do 10 000 reguł filtrowania (współdzielonych i wyłącznych).

3. Można teraz skonfigurować zadania w celu uruchamiania ich tylko w określone dni tygodnia i w określonych tygodniowych przedziałach. Ten harmonogram jest dostępny w programie Kaspersky Security Center w wersji 16.1 lub nowszej.

4. Można teraz określić przedział czasu, w którym zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* będzie wstrzymane, na przykład w celu zminimalizowania wpływu na wydajność komputera w okresach zwiększonego obciążenia.

5. Wydajność podsystemu dysku twardego w chronionym komputerze została zoptymalizowana poprzez zmniejszenie liczby operacji wejścia/wyjścia.

6. Podczas opracowywania tej wersji Kaspersky Endpoint Security uwzględniliśmy zmiany zawarte w następujących prywatnych poprawkach: PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF14071, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF25013, PF25016, PF25019.

Aktualizacja 14.0

W programie Kaspersky Endpoint Security 14.0 for Windows wprowadzono następujące funkcje i ulepszenia:

1. Komputery oparte na architekturze ARM są teraz obsługiwane. Aplikację możesz zainstalować w trybie standardowym lub w trybie agenta EDR. Aplikacja ma jednak pewne ograniczenia (na przykład spośród technologii szyfrowania danych obsługiwana jest tylko technologia BitLocker).

2. Rozszerzona kontrola zasad jest obsługiwana w Kaspersky Security Center Web Console w wersji 15.0 lub nowszej. Teraz możesz przeglądać zmiany zasad i zapisywać je w pliku. *Korekta* jest zbiorem zmodyfikowanych parametrów zapisanych przez użytkownika. Korekty umożliwiają porównywanie i cofanie zmian w parametrach zasad.

3. Użytkownicy Kaspersky Endpoint Detection and Response mają już dostęp do nowych zdarzeń telemetrycznych. Te nowe zdarzenia poszerzają możliwości wykrywania zagrożeń przez rozwiązania Kaspersky EDR.

4. Podczas opracowywania tej wersji Kaspersky Endpoint Security for Windows uwzględniliśmy zmiany zawarte w następujących prywatnych poprawkach: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Aktualizacja 12.12

W programie Kaspersky Endpoint Security 12.12 for Windows wprowadzono następujące funkcje i ulepszenia:

1. Ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym, które wcześniej było częścią komponentu Wykrywanie zachowań, jest teraz osobnym komponentem, Anti-Cryptor.

2. Dodano obsługę protokołu Kerberos w celu uwierzytelniania aplikacji za pomocą serwera proxy do dostępu do internetu.

3. Teraz można określić skrót pliku dla zaufanej aplikacji, a nie tylko pełnej ścieżki.

4. Więcej funkcji *Zadania skanowania IOC* jest dostępne dla użytkowników rozwiązań Endpoint Detection and Response (EDR). Funkcjonalność Retrospektywne skanowanie IOC jest już dostępna. *Retrospektywne skanowanie IOC* jest trybem zadania *Skanowanie IOC*, w ramach którego Kaspersky Endpoint Security skanuje dane w poszukiwaniu oznak naruszenia bezpieczeństwa przez określony czas. Tryb ten jest przeznaczony do wykrywania oznak naruszenia bezpieczeństwa danych aktywności sieciowej komputera. Kaspersky Endpoint Security analizuje dane w dziennikach systemu operacyjnego i dziennikach przeglądarki na komputerze.

5. Użytkownicy rozwiązania Kaspersky Endpoint Detection and Response (EDR) mogą usunąć limit wielkości kwarantanny. Może to być konieczne w przypadku skanowania YARA, ponieważ aplikacja może zapisać duży plik zrzutu pamięci. Teraz można wykorzystać całą wolną przestrzeń dyskową na potrzeby kwarantanny.

6. Kompresja HTTPS jest teraz obsługiwana w celu optymalizacji eksportu zdarzeń do Kaspersky Unified Monitoring and Analysis Platform (KUMA). Pomaga to ograniczyć ruch wychodzący.

7. Podczas opracowywania tej wersji Kaspersky Endpoint Security for Windows uwzględniliśmy zmiany zawarte w następujących prywatnych poprawkach: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Aktualizacja 12.11

Program Kaspersky Endpoint Security 12.11 for Windows oferuje następujące funkcje i ulepszenia:

1. Aplikacja sprawdza konfigurację komponentów sterujących przed zapisaniem ustawień. Dodano sprawdzanie dla komponentów Kontrola aplikacji, Kontrola urządzeń, Monitor integralności systemu. Aplikacja wyświetla teraz ostrzeżenie, jeśli bieżące ustawienia komponentu sterującego mogą zwiększyć obciążenie komputera lub spowodować awarie systemu. Na przykład w przypadku Kontroli aplikacji, jeśli wybierzesz tryb blokowania wszystkich aplikacji poza dozwolonymi i nie dodasz żadnej reguły zezwalającej, aplikacja wyświetli ostrzeżenie, ponieważ taka konfiguracja może spowodować awarie systemu.

2. Dodano obsługę automatycznego przesyłania plików do KATA Sandbox w celu przeglądu. *KATA Sandbox* jest składnikiem platformy Kaspersky Anti Targeted Attack Platform, który uruchamia pliki na wirtualnych obrazach systemów operacyjnych. Sandbox analizuje zachowanie obiektów w celu wykrywania szkodliwej aktywności oraz aktywności charakterystycznej dla ataków docelowych ukierunkowanych na infrastrukturę IT organizacji. Sandbox analizuje i skanuje obiekty na specjalnych serwerach z wdrożonymi obrazami wirtualnymi systemów operacyjnych Microsoft Windows (serwery Sandbox). Aby KATA Sandbox działał w trybie automatycznym, konieczne jest wdrożenie Kaspersky Anti Targeted Attack Platform w wersji 8.0 lub nowszej.

3. Zoptymalizowano wysyłanie danych telemetrycznych EDR. Teraz możesz określić maksymalną długość pakietu.

4. Udoskonalono diagnostykę połączenia z Kaspersky Security Network. Rozszerzono szczegóły błędów połączenia dla Kaspersky Security Network w celu rozwiązania potencjalnych problemów.

5. Dodano obsługę konfigurowania list zdarzeń, które mają być wysyłane do Kaspersky Unified Monitoring and Analysis Platform (KUMA). Teraz, oprócz predefiniowanych list zdarzeń w KUMA, możesz ręcznie dodawać zdarzenia do telemetrii lub wykluczać zdarzenia według ich identyfikatora w dzienniku zdarzeń systemu Windows.

6. Zaktualizowano interfejs zasad w Web Console. Zmieniono układ sekcji zasad, aby umożliwić szybszy dostęp do najważniejszych funkcji.

7. Obsługę systemu Windows 11 25H2.

8. Podczas opracowywania tej wersji Kaspersky Endpoint Security for Windows uwzględniliśmy zmiany zawarte w następujących prywatnych poprawkach: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

Aktualizacja 12.10

Program Kaspersky Endpoint Security 12.10 for Windows oferuje następujące funkcje i ulepszenia:

1. W komponencie Ochrona przed atakami BadUSB dodano opcję autoryzacji czytników kodów kreskowych poprzez odczyt kodu kreskowego z ekranu. Teraz nie musisz już wpisywać kodu za pomocą klawiatury ekranowej, aby autoryzować czytniki kodów kreskowych.

2. Następujące funkcje i udoskonalenia są dostępne dla użytkowników rozwiązań Endpoint Detection and Response (EDR) firmy Kaspersky:

   - Teraz można zarządzać izolacją komputera od sieci w szczegółach alertu. Dodatkowo w szczegółach alertu można określić okres izolacji komputera od sieci i dodawać wykluczenia.

   - Uzupełniono szczegóły alertu o nowe dane. Teraz szczegóły alertu zawierają więcej informacji o zagrożeniu, w tym o zachowaniu aplikacji przy reagowaniu na zagrożenia wykryte przez EDR.

   - Ulepszono przetwarzanie plików IOC. Teraz możesz przeglądać i edytować zawartość plików IOC w interfejsie Web Console w Kaspersky Security Center. Po załadowaniu pliku IOC aplikacja wyświetla raport dotyczący stosowania warunków IOC.

   - Ulepszona reakcja na wykryte wskaźniki IOC. Teraz możesz poddać kwarantannie pliki wykryte przez zadanie *Skanowanie IOC* bezpośrednio w wynikach wykrywania IOC we właściwościach zadania. Możesz również odizolować komputery od sieci we właściwościach zadania.

   - Teraz można tworzyć pliki IOC bezpośrednio we właściwościach zadania *Skanowania IOC*, na podstawie skrótów plików, adresów IP lub nazw DNS generowanych w pliku TXT.

   - Rozszerzony zakres skanowania dla zadania *Skanowanie IOC*. Teraz możesz zdefiniować zakres skanowania IOC rejestru (**Rejestr systemu Windows – RegistryItem**). We wcześniejszych wersjach aplikacji można było używać wyłącznie predefiniowanego zakresu skanowania IOC w rejestrze.

3. Dodano nowe uprawnienie ochrony hasłem, *Ustawienia eksportu*. Domyślnie tylko użytkownik KLAdmin może utworzyć plik konfiguracyjny z ustawieniami Kaspersky Endpoint Security w interfejsie aplikacji. Aby przyznać dostęp innym użytkownikom, musisz przyznać im odpowiednie uprawnienia.

4. Podczas opracowywania tej wersji Kaspersky Endpoint Security for Windows uwzględniliśmy zmiany zawarte w następujących prywatnych poprawkach: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

Aktualizacja 12.9

Program Kaspersky Endpoint Security 12.9 for Windows oferuje następujące funkcje i ulepszenia:

1. Nowa funkcjonalność dla *zarządzania hasłami tymczasowymi* została dodana. Hasło tymczasowe umożliwia dostęp do Kaspersky Endpoint Security z włączoną ochroną hasłem na innym komputerze. Zarządzanie hasłami tymczasowymi umożliwia zapisywanie historii haseł (do 30 dni), monitorowanie statusu haseł tymczasowych (*Aktywny*, *Utraciła ważność*, *Odwołany*) i unieważnienie haseł tymczasowych.

2. Dodano opcję umożliwiającą natychmiastowe zakończenie połączenia z zasobami internetowymi zabronionymi przez reguły Kontroli sieci po zastosowaniu zasad. W poprzednich wersjach aplikacji Kontrola sieci ograniczała jedynie nowe połączenia do zabronionych zasobów internetowych.

3. Użytkownicy Kaspersky Anti Targeted Attack Platform otrzymali możliwość uruchomienia lokalnego sprawdzania YARA na komputerze. Aby to zrobić, musisz pobrać plik z regułami YARA i wykonać polecenie w wierszu poleceń CMD.

4. Naprawiono zachowanie aplikacji, gdy funkcja BitLocker jest włączona na komputerach, na których dyski są już chronione przez funkcję BitLocker za pomocą narzędzi innych firm. Kaspersky Endpoint Security rozpocznie procedurę odzyskiwania w celu wysłania klucza odzyskiwania do Kaspersky Security Center. Zarządzanie funkcją BitLocker zostaje zatem przeniesione do konsoli Kaspersky Security Center.

5. Nowa sekcja, **Historia odpowiedzi**, jest dostępna dla użytkowników rozwiązań Detection and Response firmy Kaspersky. W tej sekcji znajdują się informacje o działaniach podejmowanych na komputerze w odpowiedzi na zagrożenia. Do takich działań zalicza się na przykład uruchomienie zadania *Zakończ proces* lub odizolowanie komputera od sieci. Historia odpowiedzi dostępna jest wyłącznie dla użytkowników następujących rozwiązań Kaspersky: MDR, EDR, KATA.

6. Dla użytkowników Kaspersky Unified Monitoring and Analysis Platform obsługa działań reagowania na zagrożenia EDR jest już dostępna. Reagując na zagrożenia, KUMA uruchamia skrypty, które tworzą odpowiednie zadania EDR. Aby wykonać zadania EDR, należy utworzyć regułę odpowiedzi dla niestandardowego skryptu w konsoli KUMA i wybrać zdarzenia.

7. Podczas opracowywania tej wersji Kaspersky Endpoint Security for Windows uwzględniliśmy zmiany zawarte w następujących prywatnych poprawkach: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

Aktualizacja 12.8

Program Kaspersky Endpoint Security 12.8 for Windows oferuje następujące funkcje i ulepszenia:

1. Aplikacja obsługuje teraz tryb Light Agent do ochrony środowisk wirtualnych. Teraz możesz wdrożyć aplikację w trybie Light Agent w ramach rozwiązania Kaspersky Security for Virtualization Light Agent 6.2.

2. Obecnie obsługiwane jest przechwytywanie operacji na plikach w kontenerach Docker na serwerach. *Kontener* jest odizolowanym środowiskiem, w którym aplikacja może działać bez bezpośredniej interakcji z systemem operacyjnym. Kaspersky Endpoint Security skanuje pliki znajdujące się w kontenerach, do których użytkownik uzyskuje dostęp. Gdy zostanie wykryta szkodliwa aktywność, aplikacja zablokuje ją i podejmie próbę wyleczenia pliku wewnątrz kontenera. Jeżeli pliku nie można wyleczyć, aplikacja zatrzymuje kontener.

3. Teraz możesz zdefiniować zakres ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym (komponent Wykrywanie zachowań). Teraz możesz określić foldery współdzielone, które aplikacja ma monitorować pod kątem aktywności plików. Można również wykluczyć pliki z zakresu ochrony. W poprzednich wersjach aplikacji komponent Wykrywanie zachowań monitorował wszystkie foldery współdzielone pod kątem aktywności plików.

4. Teraz w pakiecie instalacyjnym można skonfigurować różne zestawy komponentów dla różnych typów systemów operacyjnych. Oznacza to, że możesz wdrażać aplikację na stacjach roboczych i serwerach, korzystając z tego samego pakietu instalacyjnego. Komponenty niedostępne dla danego typu systemu operacyjnego są automatycznie wykluczane we właściwościach pakietu instalacyjnego.

5. Została dodana możliwość wyboru predefiniowanych wykluczeń ze skanowania i zaufanych aplikacji. Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje umożliwiają szybką konfigurację strefy zaufanej dla aplikacji w środowisku wirtualnym (Citrix, VMware). Do takich wykluczeń zaliczają się, na przykład, pliki maszyn wirtualnych VHD i VHDX. Wykluczenia można dodać podczas tworzenia pakietu instalacyjnego aplikacji lub zasady albo podczas instalacji Kaspersky Endpoint Security.

6. Telemetria EDR obejmuje teraz zdarzenia dotyczące operacji wykonywanych na urządzeniach podłączonych przez USB. Te zdarzenia można również dodać do wykluczeń z telemetrii EDR.

7. Dodano opcję blokowania połączeń sieciowych przez przestarzały protokół TLS 1.0. Poziom bezpieczeństwa protokołu TLS 1.0 jest niski, dlatego zaleca się jego wyłączenie i korzystanie z nowszych wersji TLS 1.2 lub TLS 1.3. Domyślnie Kaspersky Endpoint Security blokuje połączenia TLS 1.0. Po zaktualizowaniu wersji aplikacji może wystąpić problem z działaniem usług innych firm korzystających z protokołu TLS 1.0. Aby uniknąć problemów w działaniu usług innych firm, możesz zezwolić na używanie protokołu TLS 1.0 w zasadach grupy przed aktualizacją wersji aplikacji.

8. Podczas opracowywania tej wersji Kaspersky Endpoint Security for Windows uwzględniliśmy zmiany zawarte w następujących prywatnych poprawkach: PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

Aktualizacja 12.7

Program Kaspersky Endpoint Security 12.7 for Windows oferuje następujące funkcje i ulepszenia:

1. Teraz możesz ograniczyć użycie zasobów procesora dla zadań *skanowania w poszukiwaniu złośliwego oprogramowania*. Aby to zrobić, w ustawieniach aplikacji określ maksymalny procent obciążenia procesora dla wszystkich rdzeni, który może być wykorzystany podczas skanowania komputera.

2. Teraz możesz ręcznie wysyłać pliki do skanowania w KATA Sandbox. *KATA Sandbox* jest składnikiem platformy Kaspersky Anti Targeted Attack Platform, który uruchamia pliki na wirtualnych obrazach systemów operacyjnych. Sandbox analizuje zachowanie obiektów w celu wykrywania szkodliwej aktywności oraz aktywności charakterystycznej dla ataków docelowych ukierunkowanych na infrastrukturę IT organizacji. Sandbox analizuje i skanuje obiekty na specjalnych serwerach z wdrożonymi obrazami wirtualnymi systemów operacyjnych Microsoft Windows (serwery Sandbox). Aby wysłać plik do skanowania przez KATA Sandbox, wybierz odpowiednie polecenie w menu kontekstowym pliku.

3. Obecnie możesz skonfigurować integrację z rozwiązaniem, które chroni firmową sieć LAN, *Kaspersky Network Detection and Response*. Rozwiązanie Kaspersky Network Detection and Response (NDR) jest częścią Kaspersky Anti Targeted Attack Platform. Interakcję z NDR można skonfigurować zarówno w trybie standardowym, jak i w trybie EDR Agent.

4. Do rozszerzenia Ochrony poczty dodano obsługę klienta poczty Microsoft Office Outlook w wersji 2021. Rozszerzenie umożliwia skanowanie wiadomości na poziomie klienta pocztowego zamiast na poziomie protokołu. Oprócz wiadomości rozszerzenie umożliwia skanowanie obiektów otrzymanych przez interfejs MAPI z repozytoriów Microsoft Exchange (na przykład obiektów w Kalendarzu). To skanowanie odbywa się w kliencie pocztowym.

5. Podczas opracowywania tej wersji Kaspersky Endpoint Security for Windows uwzględniliśmy zmiany zawarte w następujących prywatnych poprawkach: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Aktualizacja 12.6

Program Kaspersky Endpoint Security 12.6 for Windows oferuje następujące funkcje i ulepszenia:

1. Dodano funkcjonalność integracji z rozwiązaniem Kaspersky SIEM (*Kaspersky Unified Monitoring and Analysis Platform; KUMA*). Możliwe jest teraz wysyłanie zdarzeń z dzienników zdarzeń Windows do poborcy KUMA. Dzięki temu KUMA może odbierać zdarzenia systemu Windows (obsługiwany jest ograniczony zestaw identyfikatorów EventID) ze wszystkich komputerów, na których zainstalowany jest Kaspersky Endpoint Security, bez konieczności instalowania agentów KUMA na tych komputerach.

2. Komponent *Monitor integralności systemu* został dodany w celu zastąpienia komponentu Monitor integralności plików. Komponent Monitorowanie integralności systemu zawiera całą funkcjonalność Monitora integralności plików oraz dodatkowo pozwala na monitorowanie zmian w rejestrze i podłączania urządzeń zewnętrznych. Monitorowanie integralności systemu monitoruje zmiany w systemie operacyjnym, które mogą wskazywać na naruszenia bezpieczeństwa komputera. Po wykryciu takich zmian Kaspersky Endpoint Security generuje odpowiednie zdarzenia i powiadamia administratora. Monitor integralności plików nie jest już częścią aplikacji. Ustawienia Monitora integralności plików są automatycznie przenoszone do Monitorowania integralności systemu po aktualizacji aplikacji. Aby zapewnić prawidłowe działanie Monitora integralności systemu, zarówno aplikacja Kaspersky Endpoint Security, jak i wtyczka zarządzająca powinny zostać zaktualizowane do wersji 12.6.

3. Stan zainstalowanego wbudowanego agenta EDR Agent (KATA) został dodany do właściwości komputera w konsoli Kaspersky Security Center. Teraz, jeżeli dysponujesz zainstalowanym wbudowanym agentem EDR Agent (KATA), kolumna **statusu Endpoint Sensor** wyświetla aktualny status komponentu (np. *Uruchomienie*, *Zatrzymanie*, *Nieobsługiwany przez licencję* itp.).

4. Została dodana możliwość wyboru predefiniowanych wykluczeń ze skanowania i zaufanych aplikacji. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować strefę zaufaną podczas korzystania z aplikacji na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Do takich wykluczeń zaliczają się, na przykład, pliki baz danych MDF i LDF. Wykluczenia można dodać podczas tworzenia nowej zasady, modyfikowania istniejącej zasady lub podczas instalacji Kaspersky Endpoint Security.

5. Wyświetlanie szczegółów alertów dla Kaspersky Endpoint Detection and Response Optimum zostało przeniesione z wtyczki zarządzającej Kaspersky Endpoint Security do osobnej wtyczki zarządzającej Kaspersky Endpoint Detection and Response. Wtyczka zarządzająca EDR to pojedyncza wtyczka do pracy z agentami w systemach operacyjnych Windows, Mac i Linux. Teraz, pracując z EDR Optimum, będziesz potrzebować wtyczki zarządzającej Kaspersky Endpoint Security do tworzenia zadań Threat Response oraz wtyczki zarządzającej EDR do przeglądania szczegółów alertów.

6. Obsługę systemu Windows 11 24H2.

7. Tworząc tę wersję Kaspersky Endpoint Security for Windows, uwzględniliśmy zmiany zawarte w następujących prywatnych poprawkach: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

Aktualizacja 12.5

Program Kaspersky Endpoint Security 12.5 for Windows oferuje następujące funkcje i ulepszenia:

1. Dodano opcję konfigurowania wykluczeń telemetrii. *Telemetria* to lista zdarzeń, które wystąpiły na chronionym komputerze. Dane telemetryczne są używane przez Kaspersky Anti Targeted Attack Platform (EDR) do monitorowania i ochrony infrastruktury IT organizacji. Konfigurowanie wykluczeń telemetrii pomaga poprawić wydajność komputera i zoptymalizować transmisję danych do serwera gromadzenia danych telemetrycznych.

2. Udoskonalono interfejs strefy zaufanej aplikacji. Kaspersky Endpoint Security ukrywa teraz przed użytkownikiem obiekty strefy zaufanej, jeśli administrator zabronił użytkownikowi dodawania własnych (lokalnych) wykluczeń ze skanowania i zaufanych aplikacji. Zapobiega to nieautoryzowanemu dostępowi przestępcy do strefy zaufanej, zwiększając poziom bezpieczeństwa komputera.

3. Dodano opcję skanowania ruchu sieciowego dla klientów pocztowych MyOffice Mail i R7-Office Organizer. Składnik ochrony poczty skanuje teraz nie tylko załączniki wiadomości podczas pobierania, ale także wiadomości wysyłane i odbierane.

4. Dodano nową kategorię zasobów sieciowych *Narzędzia generatywnej sztucznej inteligencji*. Można skonfigurować dostęp do stron internetowych z nowej kategorii za pomocą Kontroli sieci.

5. Teraz można wybrać lokalizację reguły pakietów sieciowych na liście Zapora sieciowa. Lokalizacja reguły pakietu sieciowego na liście określa jego priorytet. W poprzednich wersjach aplikacji nową regułę można było dodać jedynie na końcu listy, po czym trzeba było ręcznie przenosić regułę na liście, aby nadać jej priorytet. Teraz podczas dodawania reguły możesz wybrać, czy reguła ma zostać umieszczona na początku, na końcu listy, czy obok wybranej reguły.

6. W regułach składników Kaspersky Endpoint Security można teraz wybierać użytkowników nie tylko z Active Directory, ale także z listy użytkowników w Kaspersky Security Center. Możesz także ręcznie wprowadzić dane lokalnego konta użytkownika. Możliwość ta została dodana dla reguł następujących składników: Kontrola aplikacji, Kontrola urządzeń, Kontrola sieci, Adaptacyjna kontrola anomalii i Kontrola dziennika.

7. Raport o wykryciu ataku sieciowego zawiera teraz kolumnę z adresem MAC atakującego komputera (składnik ochrony sieci). Teraz oprócz adresu IP w raporcie możesz zobaczyć adres MAC atakującego komputera. Jest to pomocne przy badaniu incydentu. Raporty zawierające adres MAC atakującego komputera będą również dostępne w konsoli Kaspersky Security Center Linux w wersji 15.1 lub nowszej.

8. Zwiększono poziom wymagań dotyczących ochrony komputerów. Wysoki poziom ochrony wymaga teraz włączenia Ochrony usług aplikacji przed zewnętrznym zarządzaniem. Sprawdź wskaźnik poziomu ochrony w górnej części okna z zasadami. Jeśli masz średni lub niski poziom bezpieczeństwa, możesz włączyć Ochronę usług aplikacji przed zewnętrznym zarządzaniem w oknie zaleceń wskaźnika poziomu ochrony.

9. Dodano obsługę nowych zdarzeń wykrywania obiektów, gdy aplikacja jest uruchomiona w konfiguracji Endpoint Detection and Response Agent (EDR Agent). Zdarzenia te były już obsługiwane w konfiguracji [KES+wbudowany agent].

10. Tworząc tę wersję Kaspersky Endpoint Security for Windows, uwzględniliśmy zmiany zawarte w następujących prywatnych poprawkach: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

Aktualizacja 12.4

Program Kaspersky Endpoint Security 12.4 for Windows oferuje następujące funkcje i ulepszenia:

1. Dodano nową funkcję ochrony połączenia komputera z Kaspersky Security Center. Nowe zadanie *Ochrona połączenia z Serwerem administracyjnym* umożliwia ustawienie hasła do połączenia z serwerem zaufanym. Oznacza to, że nie można ponownie połączyć komputera i wykonywać poleceń z innego serwera bez tego hasła.

2. W składniku Ochrona hasłem dodano możliwość wyboru użytkowników ręcznie i innych niż użytkownicy z usługi Active Directory. Oznacza to, że możesz ręcznie wybrać nazwę użytkownika i hasło oraz przydzielić prawa dostępu do oprogramowania Kaspersky Endpoint Security dla tego konta. W ten sposób nie musisz udostępniać hasła KLAdmin innym użytkownikom ani tworzyć nowych kont Active Directory, aby kontrolować dostęp do aplikacji.

3. Obsługę systemu Windows 11 23H2.

Aktualizacja 12.3

Program Kaspersky Endpoint Security 12.3 for Windows oferuje następujące funkcje i ulepszenia:

1. Teraz możesz zainstalować aplikację w konfiguracji Endpoint Detection and Response Agent. Ta konfiguracja umożliwia zainstalowanie aplikacji z zestawem komponentów wymaganych przez rozwiązania Detection and Response firmy Kaspersky: Kaspersky Managed Detection and Response oraz Kaspersky Anti Targeted Attack Platform (EDR). Możesz zainstalować aplikację w tej konfiguracji wraz z rozwiązaniami innych firm (na przykład Dr.Web, Dallas Lock, ESET). Dzięki temu możesz korzystać z zabezpieczeń infrastruktury innych firm wraz z funkcją Detection and Response firmy Kaspersky.

2. Ulepszono działanie Kaspersky Endpoint Security z urządzeniami Bluetooth. Teraz możesz skonfigurować wykluczenia i ograniczyć dostęp do wszystkich urządzeń Bluetooth z wyjątkiem urządzeń wejściowych (klawiatury bezprzewodowe, myszy itp.).

3. Zoptymalizowano działanie komponentu Kontrola aplikacji z bazą danych plików wykonywalnych. Kaspersky Endpoint Security może teraz automatycznie usunąć informacje o pliku z bazy danych, jeśli ten plik zostanie usunięty z komputera. Umożliwia to aktualizowanie bazy danych i oszczędzanie zasobów Kaspersky Security Center.

4. Zwiększono poziom wymagań dotyczących ochrony komputerów. Wysoki poziom ochrony wymaga włączenia ochrony hasłem. Sprawdź wskaźnik poziomu ochrony w górnej części okna z zasadami. Jeśli masz średni lub niski poziom bezpieczeństwa, możesz włączyć ochronę hasłem w oknie zaleceń wskaźnika poziomu ochrony.

5. Dodano obsługę protokołu HTTPS, aby umożliwić aplikacji współpracę z Kaspersky Security Network. Włącz użycie HTTPS we właściwościach Serwera administracyjnego w pliku Ustawienia serwera proxy KSN.

Aktualizacja 12.2

Program Kaspersky Endpoint Security 12.2 for Windows oferuje następujące funkcje i ulepszenia:

1. Dodano obsługę protokołu WPA3 w celu kontrolowania połączeń z sieciami Wi-Fi (Kontrola urządzeń). Teraz możesz wybrać protokół WPA3 w ustawieniach zaufanej sieci Wi-Fi i nie zezwolić na połączenia z siecią przy użyciu mniej bezpiecznego protokołu.

2. Teraz możesz wybrać protokół i porty dla wykluczeń Ochrony sieci. Teraz oprócz określania adresów IP zaufanych urządzeń możesz także wybrać port i protokół. Pozwala to wykluczyć poszczególne strumienie danych i zapobiec atakom sieciowym z zaufanych adresów IP.

3. Inna kolejność źródeł aktualizacji dla lokalnego pliku *zadania Aktualizacja baz danych i modułów aplikacji*, jeśli zasada jest zastosowana do komputera. Serwer Kaspersky Security Center jest teraz domyślnie używany jako pierwsze źródło aktualizacji zamiast serwerów Kaspersky. Pomaga to zaoszczędzić ruch, gdy użytkownik uruchamia lokalne zadanie *Aktualizacja baz danych i modułów aplikacji*.

Aktualizacja 12.1

Program Kaspersky Endpoint Security 12.1 for Windows oferuje następujące funkcje i ulepszenia:

1. Dodano wbudowanego agenta do rozwiązania Kaspersky Anti Targeted Attack Platform. Aby korzystać z EDR (KATA), niepotrzebny jest już Kaspersky Endpoint Agent. Wszystkie funkcje Kaspersky Endpoint Agent będą wykonywane przez Kaspersky Endpoint Security. Aby migrować zasady Kaspersky Endpoint Agent, użyj Kreatora migracji. Po aktualizacji aplikacji Kaspersky Endpoint Security przełącza się na używanie wbudowanego agenta i usuwa Kaspersky Endpoint Agent. Rozwiązanie Kaspersky Endpoint Agent zostało dodane do listy niezgodnego oprogramowania. Kaspersky Endpoint Security wyposażono we wbudowanych agentów do wszystkich rozwiązań Detection and Response, dlatego instalowanie Kaspersky Endpoint Agent w celu integracji z tymi rozwiązaniami nie jest już konieczne.

2. Tryb zgodności platformy Azure WVD jest teraz obsługiwany. Ta funkcja zapewnia prawidłowe wyświetlanie stanu maszyny wirtualnej Azure w konsoli Kaspersky Anti Targeted Attack Platform. Tryb zgodności Azure WVD umożliwia przypisanie do tych maszyn wirtualnych trwałego unikatowego identyfikatora czujnika.

3. Teraz możesz skonfigurować dostęp użytkowników do urządzeń mobilnych w iTunes lub podobnych aplikacjach. Oznacza to, że możesz na przykład zezwolić na używanie urządzenia mobilnego tylko w iTunes i zablokować używanie urządzenia mobilnego jako dysku wymiennego. Aplikacja obsługuje również te reguły w przypadku aplikacji Android Debug Bridge (ADB).

4. Kaspersky Security Center w wersji 11 nie jest już obsługiwany. Zaktualizuj Kaspersky Security Center do najnowszej wersji.

Naprawione problemy

Poniższa tabela zawiera listę wszystkich problemów wykrytych w poprzednich wersjach Kaspersky Endpoint Security i naprawionych w bieżącej wersji.

Lista problemów naprawionych w wersji 14.1

Identyfikator problemu	Opis problemu
10140523	Włączenie natywnej obsługi NVMe w systemie Windows 11 może spowodować niestabilne działanie aplikacji.
9340076	Na urządzeniu z zainstalowaną aplikacją i włączonym komponentem Szyfrowanie plików Eksplorator Windows nie odświeża automatycznie zawartości folderu sieciowego po jej zmodyfikowaniu z innego urządzenia.
9722863	Raport Kontroli urządzeń nie zawiera zdarzenia odłączenia tokena USB.
10006481	Po zastosowaniu reguły blokującej ruch przychodzący aktywne połączenia TCP z usługami zewnętrznymi mogą zostać przedwcześnie zakończone z powodu nieprawidłowego obliczania limitu czasu.
10140912	Aplikacja nie wykrywa urządzenia PDA BHT1100B.

Identyfikator problemu	Opis problemu
10157563	Folder Redirection może nie działać po ponownym uruchomieniu na stacjach roboczych VDI.
10158494	Kontrola urządzeń rejestruje wiele zdarzeń podłączenia i odłączenia urządzenia wymiennego bez jego fizycznego ponownego podłączenia.

Najczęściej zadawane pytania

OGÓLNE

Na jakich komputerach może działać Kaspersky Endpoint Security?

Co się zmieniło od ostatniej wersji?

Z jakimi innymi aplikacjami Kaspersky może działać Kaspersky Endpoint Security?

Jak można oszczędzić zasoby komputera podczas działania Kaspersky Endpoint Security?

WDRAŻANIE

Jak zainstalować Kaspersky Endpoint Security na wszystkich komputerach w organizacji?

Które ustawienia instalacji mogą zostać skonfigurowane z poziomu wiersza poleceń?

Jak zdalnie odinstalować Kaspersky Endpoint Security?

AKTUALIZACJA

Jakie metody są dostępne do aktualizowania baz danych?

Co należy zrobić, jeśli po aktualizacji wystąpią problemy?

W jaki sposób można zaktualizować bazy danych poza siecią korporacyjną?

Czy możliwe jest używanie serwera proxy dla aktualizacji?

BEZPIECZEŃSTWO

W jaki sposób Kaspersky Endpoint Security skanuje wiadomości e-mail?

Jak można wykluczyć zaufany plik ze skanowania?

Jak można chronić komputer przed wirusami z dysków flash?

Jak uruchamiać skanowanie w poszukiwaniu złośliwego oprogramowania ukryte przed użytkownikiem?

W jaki sposób tymczasowo wstrzymać ochronę Kaspersky Endpoint Security?

Jak przywrócić plik, który został pomyłkowo usunięty przez Kaspersky Endpoint Security?

Jak chronić Kaspersky Endpoint Security przed odinstalowaniem przez użytkownika?

INTERNET

Czy Kaspersky Endpoint Security skanuje połączenia szyfrowane (HTTPS)?

Jak zezwolić użytkownikom na nawiązywanie połączenia tylko z zaufanymi sieciami Wi-Fi?

Jak zablokować sieci społecznościowe?

APLIKACJE

Jak można się dowiedzieć, które aplikacje są zainstalowane na komputerze użytkownika (inwentarz)?

Jak uniemożliwić uruchamianie gier komputerowych?

Jak mogę sprawdzić, czy Kontrola aplikacji została poprawnie skonfigurowana?

Jak dodać aplikację do listy zaufanych?

URZĄDZENIA

Jak można zablokować korzystanie z dysków flash?

Jak dodać urządzenie do listy zaufanych?

Czy możliwe jest uzyskanie dostępu do zablokowanego urządzenia?

SZYFROWANIE

W jakich warunkach szyfrowanie jest niemożliwe?

Jak można używać hasła do ograniczenia dostępu do archiwum?

Czy możliwe jest używanie kart inteligentnych i tokenów z szyfrowaniem?

Czy możliwe jest uzyskanie dostępu do zaszyfrowanych danych, jeśli nie ma połączenia z Kaspersky Security Center?

Co należy zrobić, jeśli wystąpi błąd systemu operacyjnego komputera, a dane pozostaną zaszyfrowane?

POMOC TECHNICZNA

Gdzie jest przechowywany plik raportu?

Jak można utworzyć plik śledzenia?

Jak można włączyć zapisywanie zrzutu pamięci?

Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows (zwany dalej Kaspersky Endpoint Security) zapewnia odpowiednią ochronę komputera przed różnymi typami zagrożeń, atakami sieciowymi i phishingowymi.

Aplikacja nie jest przeznaczona do stosowania w procesach technologicznych wymagających zautomatyzowanych systemów sterowania. Aby chronić urządzenia w takich systemach, zaleca się korzystanie z aplikacji Kaspersky Industrial CyberSecurity for Nodes.

Technologie wykrywania zagrożeń



Uczenie maszynowe

Kaspersky Endpoint Security używa modeli opartych o uczenie maszynowe. Model został opracowany przez ekspertów z firmy Kaspersky. Model jest cały czas uzupełnianymi danymi zagrożeń z KSN (uczenie modelu).



Analiza w chmurze

Kaspersky Endpoint Security pobiera dane zagrożeń z Kaspersky Security Network. *Kaspersky Security Network (KSN)* jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobów sieciowych oraz oprogramowania.



Analiza ekspercka

Kaspersky Endpoint Security wykorzystuje dane zagrożeń pobrane przez analityków wirusów Kaspersky. Analitycy wirusów oceniają, czy reputacja obiektów nie może zostać określona automatycznie.



Analiza zachowań

Kaspersky Endpoint Security analizuje aktywność obiektu w czasie rzeczywistym.



Analiza automatyczna

Kaspersky Endpoint Security pobiera dane z systemu automatycznej analizy obiektów. System przetwarza wszystkie obiekty, które są wysyłane do Kaspersky. Następnie system określa reputację obiektu i dodaje dane do antywirusowych baz danych. Jeśli system nie może określić reputacji obiektu, system pyta analityków wirusów z Kaspersky.



Sandbox

Kaspersky Endpoint Security przetwarza obiekt na maszynie wirtualnej. Kaspersky Sandbox analizuje zachowanie obiektu i podejmuje decyzję odnośnie jego reputacji. Ta technologia jest dostępna tylko wtedy, gdy używasz rozwiązania Kaspersky Sandbox.



Cloud Sandbox

Kaspersky Endpoint Security skanuje obiekty w izolowanym środowisku zapewnionym przez firmę Kaspersky. Technologia Cloud Sandbox jest stale włączona i jest dostępna dla wszystkich użytkowników Kaspersky Security Network, niezależnie od typu licencji, z której korzystają. Jeżeli wdrożono już Endpoint Detection and Response Optimum, możesz włączyć osobny licznik dla zagrożeń wykrytych przez Cloud Sandbox.

Drzewo wyboru

Każdy typ zagrożenia jest przetwarzany przez dedykowany moduł. Moduły mogą być włączane lub wyłączane niezależnie od siebie.

Sekcja	Składnik
Podstawowa ochrona przed zagrożeniami 	**Ochrona plików** Komponent Ochrona plików pozwala zapobiegać infekcjom systemu plików komputera. Domyślnie komponent Ochrona plików znajduje się na stałe w pamięci RAM komputera i na bieżąco skanuje wszystkie otwierane, zapisywane i uruchamiane pliki. Ten komponent skanuje pliki na wszystkich dyskach komputera, także na dyskach podłączonych. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej. **Ochrona WWW** Komponent Ochrona WWW zapobiega pobieraniu szkodliwych plików z internetu, a także blokuje szkodliwe i phishingowe strony internetowe. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej. **Ochrona poczty** Ochrona poczty skanuje załączniki odbieranych i wysyłanych wiadomości e-mail w poszukiwaniu wirusów i innych zagrożeń. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej. Ochrona poczty może skanować zarówno wiadomości odbierane, jak i wysyłane. Aplikacja obsługuje protokoły POP3, SMTP, IMAP i NNTP w następujących klientach pocztowych: • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer Aby skanować ruch w klientach pocztowych Mozilla Thunderbird, MyOffice Mail i R7-Office Organizer, musisz dodać certyfikat Kaspersky do magazynu certyfikatów oraz wybrać własny magazyn certyfikatów. Ochrona poczty nie obsługuje innych protokołów i klientów pocztowych. Ochrona poczty może nie zawsze być w stanie zyskać dostęp do wiadomości na *poziomie protokołu* (na przykład podczas korzystania z rozwiązania Microsoft Exchange). Z tego powodu Ochrona poczty obejmuje rozszerzenie dla programu Microsoft Office Outlook. Rozszerzenie umożliwia skanowanie wiadomości na *poziomie klienta pocztowego*. Rozszerzenie Ochrony poczty obsługuje 32- i 64-bitowe wersje programów Outlook 2010, 2013, 2016, 2019, 2021, 2024 i 365. Na komputerach opartych na architekturze Arm rozszerzenie Ochrony poczty obsługuje 32- i 64-bitowe wersje programów Outlook 2016, Outlook 2021, Outlook 2024 i Outlook 365 dla architektury Arm64. **Ochrona sieci** Składnik *Ochrona sieci* (zwany także Intrusion Detection System, IDS) monitoruje przychodzący ruch sieciowy pod kątem aktywności charakterystycznej dla ataków sieciowych. Gdy Kaspersky Endpoint Security wykryje próbę ataku sieciowego na komputerze użytkownika, zablokuje połączenie sieciowe z komputerem atakującym. Opisy znanych typów ataków sieciowych oraz sposoby ich zwalczania znajdują się w bazach danych aplikacji. Lista ataków sieciowych, wykrywanych przez komponent Ochrona sieci, jest uaktualniana podczas aktualizacji baz danych i modułów aplikacji. **Zapora sieciowa** Zapora sieciowa blokuje nieautoryzowane połączenia z komputerem podczas pracy w Internecie lub sieci lokalnej. Zapora sieciowa kontroluje również aktywność sieciową aplikacji na komputerze. Pozwala to chronić korporacyjną sieć LAN przed kradzieżą tożsamości i innymi atakami. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i predefiniowanych *reguł sieciowych*. **Ochrona przed atakami BadUSB** Komponent Ochrona przed atakami BadUSB zapobiega podłączeniu do komputera zainfekowanych urządzeń USB emulujących klawiaturę. **Ochrona AMSI** Komponent Ochrona AMSI jest przeznaczony do obsługi Antimalware Scan Interface firmy Microsoft. *Antimalware Scan Interface (AMSI)* umożliwia aplikacjom firm trzecich z obsługą AMSI wysyłanie obiektów (na przykład, skryptów PowerShell) do Kaspersky Endpoint Security w celu przeprowadzenia dodatkowego skanowania i otrzymania wyników ze skanowania tych obiektów.

Sekcja	Składnik
Zaawansowana ochrona przed zagrożeniami 	**Kaspersky Security Network** *Kaspersky Security Network (KSN)* jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobów sieciowych oraz oprogramowania. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi programu Kaspersky Endpoint Security na nowe zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów. Jeśli uczestniczysz w Kaspersky Security Network, usługi KSN zapewniają Kaspersky Endpoint Security informacje o reputacji przeskanowanych adresów internetowych, a także informacje o kategorii i reputacji przeskanowanych plików. **Wykrywanie zachowań** Komponent Wykrywanie zachowań gromadzi dane na temat działań aplikacji na komputerze i dostarcza te informacje innym składnikom ochrony w celu udoskonalenia ich działania. Komponent Wykrywanie zachowań używa sygnatur strumieni zachowań (BSS) dla aplikacji. Jeśli aktywność aplikacji odpowiada sygnaturze strumienia zachowań, Kaspersky Endpoint Security wykona wybrane działanie. Funkcjonalność Kaspersky Endpoint Security oparta na sygnaturach strumieni zachowań zapewnia proaktywną ochronę komputera. Komponent Wykrywanie zachowań dodatkowo monitoruje porty sieciowe w poszukiwaniu procesów aplikacji, które mogą zagrozić bezpieczeństwu komputera. Aplikacja pobiera informacje o takich procesach z baz danych programów antywirusowych. **Anti-Cryptor** Komponent Anti-Cryptor analizuje aktywność w folderach współdzielonych. Jeśli to działanie jest zgodne z sygnaturą strumieni zachowań, która jest typowa dla zewnętrznego szyfrowania, Kaspersky Endpoint Security wykonuje wybraną akcję. **Ochrona przed exploitami** Komponent Ochrona przed exploitami wykrywa kod programu, który wykorzystuje luki na komputerze, aby użyć uprawnień administratora lub wykonać szkodliwe aktywności. Na przykład, exploity mogą używać ataku typ buffer overflow (przepełnienie bufora). Aby to zrobić, exploit wysyła dużą ilość danych do aplikacji zawierającej lukę. Podczas przetwarzania tych danych aplikacja zawierająca lukę wykona szkodliwy kod. W wyniku tego ataku exploit może uruchomić nieautoryzowaną instalację szkodliwego programu. Po wykryciu, że próba uruchomienia pliku wykonywalnego z aplikacji zawierającej luki nie została zainicjowana przez użytkownika, Kaspersky Endpoint Security zablokuje uruchomienie tego pliku lub poinformuje użytkownika. Komponent Ochrona przed exploitami dodatkowo monitoruje porty sieciowe w poszukiwaniu procesów aplikacji, które mogą zagrozić bezpieczeństwu komputera. Aplikacja pobiera informacje o takich procesach z baz danych programów antywirusowych. **Ochrona przed włamaniami** Ochrona przed włamaniami uniemożliwia aplikacjom wykonywanie działań niebezpiecznych dla systemu operacyjnego i zapewnia kontrolę dostępu do zasobów systemu operacyjnego i danych osobowych. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network. **Silnik korygujący** Silnik korygujący umożliwia Kaspersky Endpoint Security wycofanie działań, które zostały wykonane przez szkodliwe oprogramowanie w systemie operacyjnym.

Sekcja	Składnik
Kontrola zabezpieczeń 	**Kontrola aplikacji** Kontrola aplikacji zarządza uruchamianiem aplikacji na komputerach użytkowników. Pozwala to na wdrożenie polityki bezpieczeństwa firmy podczas korzystania z aplikacji. Kontrola aplikacji zmniejsza także ryzyko infekcji komputera poprzez ograniczenie dostępu do aplikacji. **Kontrola urządzeń** Kontrola urządzeń zarządza dostępem użytkownika do urządzeń, które są instalowane na komputerze lub są podłączone do komputera (na przykład: dyski twarde, kamery lub moduły Wi-Fi). Umożliwia to ochronę komputera przed infekcją, gdy takie urządzenia są podłączone, oraz zapobieganie utracie lub wyciekowi danych. **Kontrola sieci** Kontrola sieci zarządza dostępem użytkowników zasobów sieciowych. Pomaga to zmniejszyć ruch sieciowy i nieodpowiednie dysponowanie czasem pracy. Gdy użytkownik próbuje otworzyć stronę internetową ograniczoną przez Kontrolę sieci, Kaspersky Endpoint Security zablokuje dostęp lub wyświetli ostrzeżenie. **Adaptacyjna kontrola anomalii** Komponent Adaptacyjna kontrola anomalii monitoruje i blokuje działania, które nie są typowe dla komputerów w sieci firmowej. Adaptacyjna kontrola anomalii wykorzystuje zestaw reguł do śledzenia nietypowych zachowań (na przykład reguła *Uruchomienie procesora poleceń Microsoft Office z aplikacji biurowej*). Reguły są tworzone przez specjalistów z Kaspersky w oparciu o typowe scenariusze złośliwej aktywności. Można skonfigurować, w jaki sposób Adaptacyjna kontrola aplikacji obsługuje każdą regułę i, na przykład, zezwolić na wykonywanie skryptów PowerShell, które automatyzują określone zadania przepływu pracy. Kaspersky Endpoint Security aktualizuje zestaw reguł wraz z bazami danych aplikacji. **Kontrola dziennika** Komponent Kontrola dziennika monitoruje integralność chronionego środowiska na podstawie analizy dziennika zdarzeń systemu Windows. Gdy aplikacja wykryje oznaki nietypowego zachowania w systemie, informuje o tym administratora, gdyż zachowanie to może świadczyć o próbie cyberataku. **Monitor integralności systemu** Monitorowanie integralności systemu monitoruje zmiany w systemie operacyjnym, które mogą wskazywać na naruszenia bezpieczeństwa komputera. Po wykryciu takich zmian Kaspersky Endpoint Security generuje odpowiednie zdarzenia i powiadamia administratora.
Zadania 	**Skanowanie w poszukiwaniu złośliwego oprogramowania** Kaspersky Endpoint Security skanuje komputer pod kątem wirusów i innych zagrożeń. Skanowanie w poszukiwaniu złośliwego oprogramowania pomaga wykluczyć możliwość rozprzestrzeniania szkodliwego oprogramowania, które nie zostało wykryte przez składniki ochrony, na przykład, ze względu na niski poziom ochrony. **Aktualizacja baz danych i modułów aplikacji** Kaspersky Endpoint Security pobiera uaktualnienia baz danych i modułów aplikacji. Aktualizacja zapewnia ochronę komputera przed najnowszymi wirusami i innymi zagrożeniami. Domyślnie aplikacja jest aktualizowana automatycznie, ale w razie konieczności możesz zawsze uruchomić aktualizację baz danych i modułów aplikacji ręcznie. **Wycofanie ostatniej aktualizacji** Kaspersky Endpoint Security wycofuje ostatnią aktualizację baz danych i modułów. Umożliwi to w razie czego wycofanie baz danych i modułów aplikacji do ich poprzedniej wersji, na przykład, gdy nowa wersja baz danych zawiera nieprawidłową sygnaturę powodującą, że Kaspersky Endpoint Security blokuje bezpieczną aplikację. **Sprawdzanie integralności aplikacji** Kaspersky Endpoint Security sprawdza, czy moduły aplikacji w folderze instalacyjnym aplikacji nie są uszkodzone lub zmodyfikowane. Jeśli moduł aplikacji posiada nieprawidłowy podpis cyfrowy, moduł zostanie uznany za uszkodzony.
Szyfrowanie danych 	**Szyfrowanie plików** Komponent umożliwia utworzenie reguł szyfrowania plików. Możesz wybrać predefiniowane foldery do szyfrowania, ręcznie wybrać folder lub wybrać pojedyncze pliki według rozszerzenia. **Szyfrowanie całego dysku** Komponent umożliwia szyfrowanie dysku twardego przy użyciu funkcji Kaspersky Disk Encryption lub Szyfrowanie dysków funkcją BitLocker. **Szyfrowanie dysków wymiennych** Komponent umożliwia ochronę danych na dyskach wymiennych. Możesz użyć funkcji Szyfrowanie całego dysku (FDE) lub Szyfrowanie plików (FLE).

Sekcja	Składnik
Detection and Response 	**Endpoint Detection and Response Optimum** Wbudowany agent dla rozwiązania Kaspersky Endpoint Detection and Response Optimum (zwany dalej „EDR Optimum"). *Kaspersky Endpoint Detection and Response* to rozwiązanie do ochrony infrastruktury IT korporacji przed zaawansowanymi cyberzagrożeniami. Funkcjonalność rozwiązania łączy automatyczne wykrywanie zagrożeń z możliwością reagowania na te zagrożenia w celu przeciwdziałania zaawansowanym atakom, w tym nowym exploitom, oprogramowaniu ransomware, atakom bezplikowym, a także metodom z użyciem legalnych narzędzi systemowych. Więcej informacji o rozwiązaniu znajdziesz w pomocy dla Kaspersky Endpoint Detection and Response Optimum. **Endpoint Detection and Response Expert** Wbudowany agent dla rozwiązania Kaspersky Endpoint Detection and Response Expert (zwany dalej „EDR Expert"). EDR Expert oferuje więcej funkcji monitorowania zagrożeń i reakcji na nie niż EDR Optimum. Więcej informacji o rozwiązaniu znajdziesz w pomocy dla Kaspersky Endpoint Detection and Response Expert. **Endpoint Detection and Response Expert (on-premises)** i **Network Detection and Response (KATA)** Wbudowany agent do zarządzania komponentami Endpoint Detection and Response oraz Network Detection and Response, który jest częścią rozwiązania Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* to rozwiązanie zaprojektowane w celu szybkiego wykrywania złożonych zagrożeń, takich jak ataki ukierunkowane, zaawansowane trwałe zagrożenia (APT), ataki zero-day i inne. Kaspersky Anti Targeted Attack Platform składa się z trzech jednostek funkcjonalnych: • Kaspersky Anti Targeted Attack Platform (*KATA*) • Kaspersky Endpoint Detection and Response (*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) Można zakupić wszystkie jednostki funkcjonalne lub poszczególne jednostki funkcjonalne osobno. Szczegółowe informacje na temat rozwiązania można znaleźć w systemie pomocy dla Kaspersky Anti Targeted Attack Platform. **Sandbox** Wbudowany agent dla Sandbox. Komponent *Sandbox* wykrywa i automatycznie blokuje zaawansowane zagrożenia na komputerach. Sandbox analizuje zachowanie obiektów w celu wykrywania szkodliwej aktywności oraz aktywności charakterystycznej dla ataków docelowych ukierunkowanych na infrastrukturę IT organizacji. Sandbox analizuje i skanuje obiekty na specjalnych serwerach z wdrożonymi obrazami wirtualnymi systemów operacyjnych Microsoft Windows (serwery Sandbox). Szczegółowe informacje na temat rozwiązania można znaleźć w systemie pomocy dla Kaspersky Sandbox i dla Kaspersky Anti Targeted Attack Platform. **Managed Detection and Response** Wbudowany agent do obsługi działania rozwiązania Kaspersky Managed Detection and Response. Rozwiązanie *Kaspersky Managed Detection and Response (MDR)* automatycznie wykrywa i analizuje incydenty naruszenia bezpieczeństwa w Twojej infrastrukturze. W tym celu MDR używa danych telemetrycznych, otrzymanych z punktów końcowych i uczenia maszynowego. MDR wysyła dane incydentu do ekspertów z Kaspersky. Eksperci mogą następnie przetworzyć incydent i, na przykład, dodać nowy wpis do antywirusowych baz danych. Zamiast tego eksperci mogą opublikować zalecenia odnośnie przetwarzania incydentu i, na przykład, zasugerować odizolowanie komputera od sieci. Szczegółowe informacje dotyczące sposobu działania rozwiązania można znaleźć w pomocy do Kaspersky Managed Detection and Response.

Tryby aplikacji: Standardowy, EDR Agent, Light Agent

Kaspersky Endpoint Security for Windows jest częścią wielu rozwiązań Kaspersky. W zależności od rozwiązania należy wybrać tryb działania aplikacji.



Tryb standardowy

Jest to główny i domyślny tryb aplikacji. Aplikację w tym trybie można zainstalować jako część rozwiązań Kaspersky EPP (Endpoint Protection Platform). Na przykład Kaspersky Endpoint Security w trybie standardowym jest częścią rozwiązania Kaspersky Endpoint Security for Business. Kaspersky Endpoint Security zapewnia kompleksową ochronę stacji roboczych i serwerów przed różnymi zagrożeniami, atakami sieciowymi i oszustwami. W trybie standardowym dostępne są również wbudowane agenty, które umożliwiają integrację z rozwiązaniami Kaspersky Detection and Response, w tym EDR, MDR, KUMA i innymi.



EDR Agent

Ten tryb umożliwia wdrożenie rozwiązań Kaspersky Detection and Response wraz z rozwiązaniami EPP innych firm. Rozwiązania do wykrywania i reagowania obejmują Kaspersky Managed Detection and Response (MDR) oraz Kaspersky Anti Targeted Attack Platform (KATA). EDR Agent obsługuje również rozwiązanie Kaspersky SIEM, Kaspersky Unified Monitoring and Analysis Platform (KUMA).

W tym trybie standardowe komponenty ochrony, takie jak Ochrona plików i Ochrona WWW, są niedostępne. Standardową ochronę komputera dostarcza rozwiązanie EPP innej firmy. Agent EDR stale monitoruje procesy uruchomione na tych komputerach, otwarte połączenia sieciowe i modyfikowane pliki oraz współpracuje z rozwiązaniami do wykrywania i reagowania.



Light Agent

Ten tryb służy do ochrony środowisk wirtualnych. Rozwiązanie Kaspersky Endpoint Security w trybie Light Agent jest częścią rozwiązania Kaspersky Hybrid Cloud Security. Tryb Light Agent chroni maszyny wirtualne z gościnnymi systemami operacyjnymi dla stacji roboczych i serwerów. W tym trybie dostępne są takie same komponenty ochrony i sterowania, jak w trybie standardowym. Różnica polega na tym, że obiekty są skanowane w poszukiwaniu wirusów i innego złośliwego oprogramowania przez specjalny komponent rozwiązania zainstalowany na oddzielnej maszynie wirtualnej SVM (Secure Virtual Machine). W ten sposób Light Agent zapewnia bezpieczeństwo infrastruktury, wykorzystując zasoby SVM zamiast zasobów maszyny wirtualnej.

Pakiet dystrybucyjny

Pakiet dystrybucyjny zawiera następujące pakiety dystrybucyjne:

- **AES256**

  Ten pakiet dystrybucyjny przeznaczony jest do instalacji na komputerach z architekturą x86/x64. Ten pakiet dystrybucyjny zawiera narzędzia kryptograficzne, które implementują algorytm szyfrowania AES (Advanced Encryption Standard) o efektywnej długości klucza wynoszącej 256 bitów.

- **AES56**

  Ten pakiet dystrybucyjny przeznaczony jest do instalacji na komputerach z architekturą x86/x64. Ten pakiet dystrybucyjny zawiera narzędzia kryptograficzne, które implementują algorytm szyfrowania AES o efektywnej długości klucza wynoszącej 56 bitów.

- **Arm64**

  Ten pakiet dystrybucyjny jest przeznaczony do instalacji na komputerach opartych na architekturze ARM. Ten pakiet dystrybucyjny nie jest przeznaczony do instalacji na serwerach.

Przed instalacją należy upewnić się, czy pakiet dystrybucyjny jest zgodny z architekturą procesora. Jeżeli pakiet dystrybucyjny nie jest zgodny z architekturą procesora, instalator zakończy instalację, wyświetlając komunikat o błędzie.

Pakiet dystrybucyjny jest samorozpakowującym się archiwum w formacie EXE. Aby wyświetlić zawartość pakietu dystrybucyjnego, należy wypakować archiwum do osobnego folderu. Każdy pakiet dystrybucyjny zawiera następujące pliki:

`kes_win.msi`	Pakiet instalacyjny Kaspersky Endpoint Security.
`setup_kes.exe`	Pliki wymagane do instalacji aplikacji przy użyciu jednej z dostępnych metod.
`kes_win.kud`	Plik do tworzenia pakietów instalacyjnych dla Kaspersky Endpoint Security.
`klcfginst.msi`	Pakiet instalacyjny wtyczki do zarządzania aplikacjami w Konsoli administracyjnej Kaspersky Security Center.
`bases.cab`	Pliki pakietu aktualizacyjnego, które są używane podczas instalacji.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Pliki do usuwania niekompatybilnego oprogramowania.
`incompatible.txt`	Plik zawierający listę oprogramowania, które może powodować problemy z kompatybilnością z Kaspersky Endpoint Security. Kaspersky nie gwarantuje kompatybilności Kaspersky Endpoint Security z oprogramowaniem z listy.
`ksn_<language ID>.txt`	Plik, w którym możesz przeczytać warunki uczestnictwa w Kaspersky Security Network.
`license.txt`	Plik, w którym możesz przeczytać Umowę licencyjną i Politykę prywatności.
`installer.ini`	Plik, który zawiera wewnętrzne ustawienia pakietu dystrybucyjnego.
`kes.cab`	Pliki interfejsu graficznego aplikacji.
`aes256.cab` / `aes56.cab`	Pliki algorytmu kryptograficznego AES (nie są zawarte w pakiecie dystrybucyjnym Arm64).
`package.kcat`	Plik z podpisami zestawu dystrybucyjnego aplikacji. Podpis cyfrowy gwarantuje autentyczność i integralność pakietu dystrybucyjnego aplikacji.

Nie jest zalecane zmienianie wartości tych ustawień. Jeśli chcesz zmienić opcje instalacji, użyj pliku setup.ini.

Wymagania sprzętowe i programowe

W tym artykule wymieniono wersje oprogramowania, na których aplikacja została przetestowana i dla których gwarantowane jest jej prawidłowe działanie. Aplikacja może również działać z innymi wersjami oprogramowania, ale te konfiguracje nie przeszły pełnego cyklu testów i nie znajdują się na liście wersji z gwarantowaną obsługą.

Aby aplikacja Kaspersky Endpoint Security działała poprawnie, komputer powinien spełniać określone wymagania:

Aby zainstalować aplikację, musisz mieć uprawnienia administratora na komputerze.

Minimalne wymagania ogólne

Minimalne wymagania	Stacja robocza (x86/x64)	Serwer (x86/x64)	Arm
Pamięć	2 GB	2 GB	2 GB
Procesor	1 GHz, obsługa instrukcji SSE2	1,4 GHz, obsługa instrukcji SSE2	1 GHz, architektura Armv8.1
Pamięć RAM	Stacja robocza (x86): 1 GB Stacja robocza (x64): 2 GB	2 GB Uwaga: serwer wymaga 8 GB pamięci w celu zainstalowania aplikacji z wbudowanym agentem w celu integracji z Kaspersky Anti Targeted Attack Platform.	4 GB
Microsoft .NET Framework	Wersja 4 lub nowsza	Wersja 4 lub nowsza	Wersja 4,8 lub nowsza

Stacje robocze

Obsługiwane systemy operacyjne dla stacji roboczych:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise wielosesyjny
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

Systemy operacyjne Windows, począwszy od wersji 11 24H2, obsługują technologię UDP Receive Segment Coalescing Offload (URO). Technologia ta jest włączona domyślnie, jeśli na komputerze zainstalowano zgodną kartę sieciową i sterowniki. Wyłączenie technologii URO na komputerze użytkownika może znacząco obniżyć wydajność aplikacji.

Zapewnienie poprawnego działania Kaspersky Endpoint Security wymaga uruchomienia usługi Windows Security Center (wscsvc) na komputerze użytkownika.

Nie można zainstalować Kaspersky Endpoint Security w systemie Microsoft Windows 7 bez zainstalowanych aktualizacji systemu operacyjnego: KB4490628 (12 marca 2019 r.) i KB4474419 (23 września 2019 r.). Aby uzyskać szczegółowe informacje, zapoznaj się z Bazą wiedzy na stronie działu pomocy technicznej.

Więcej informacji na temat obsługi systemu operacyjnego Microsoft Windows 10 można znaleźć w Bazie wiedzy na stronie działu pomocy technicznej.

Więcej informacji na temat obsługi systemu operacyjnego Microsoft Windows 11 można znaleźć w Bazie wiedzy na stronie działu pomocy technicznej.

Serwery

Kaspersky Endpoint Security obsługuje podstawowe komponenty aplikacji na komputerach działających pod kontrolą systemu operacyjnego Windows dla serwerów. Możesz użyć Kaspersky Endpoint Security for Windows zamiast Kaspersky Security for Windows Server na serwerach i klastrach w Twojej organizacji (Cluster Mode). Aplikacja obsługuje także Server Core Mode (zobacz znane problemy).

Obsługiwane systemy operacyjne dla serwerów:

- Windows Small Business Server 2011 Essentials / Standard (64-bitowy)

  Microsoft Small Business Server 2011 Standard (64-bitowy) jest obsługiwany tylko wtedy, gdy zainstalowany jest pakiet Service Pack 1 dla systemu Microsoft Windows Server 2008 R2.

- Windows MultiPoint Server 2011 (64-bitowy)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (w tym tryb Server Core)
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (w tym tryb Server Core)
- Windows Server 2016 Essentials / Standard / Datacenter (w tym tryb Server Core)
- Windows Server 2019 Essentials / Standard / Datacenter (w tym tryb Server Core)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (w tym tryb Server Core)
- Windows Server 2025 Standard / Datacenter

Kaspersky Endpoint Security nie może zostać zainstalowany w systemie Microsoft Windows Server 2008 R2 bez zainstalowanych aktualizacji systemu operacyjnego: KB4490628 (12 marca 2019 r.) i KB4474419 (23 września 2019 r.).

Więcej informacji na temat obsługi systemów operacyjnych Microsoft Windows Server 2016 i Microsoft Windows Server 2019 można znaleźć w Bazie wiedzy na stronie działu pomocy technicznej.

Więcej informacji na temat obsługi systemu operacyjnego Microsoft Windows Server 2022 można znaleźć w Bazie wiedzy na stronie działu pomocy technicznej.

Nieobsługiwane systemy operacyjne dla serwerów:

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2

- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

Platformy wirtualne

Obsługiwane platformy wirtualne do działania aplikacji w trybie standardowym:

- VMware Workstation Pro 26H1
- Aktualizacja VMware ESXi 8.0 3i
- Windows Server 2025
- Citrix Virtual Apps and Desktops 7 2507 LTSR
- Citrix Provisioning 2507 LTSR
- XenServer 8.4

Aplikacja obsługuje maszyny wirtualne z systemem Windows 11 Pro Arm64 utworzone przy użyciu platformy Hyper-V.

Maszyny wirtualne do instalacji klienta Light Agent

Instalacja Kaspersky Endpoint Security w trybie Light Agent na maszynach wirtualnych opartych na architekturze ARM nie jest obsługiwana.

BIOS na maszynach wirtualnych musi obsługiwać specyfikację SMBIOS w wersji 2.1 lub nowszej.

Na maszynach wirtualnych muszą być zainstalowane następujące pakiety i narzędzia:

- W przypadku korzystania z Microsoft Hyper-V – pakiet Integration Services.
- W przypadku korzystania z VMware vSphere – pakiet VMware Tools.
- W przypadku korzystania z XenServer – pakiet XenTools.
- W przypadku korzystania z HUAWEI FusionSphere – pakiet HUAWEI Tools.
- W przypadku korzystania z hiperwizorów opartych na KVM — QEMU Guest Agent.

Artykuł Pomoc dotycząca Kaspersky Security for Virtualization Light Agent opisuje wymagania dotyczące infrastruktury wirtualnej, aby można było na niej uruchomić aplikację w trybie Light Agent.

Aby aplikacja działała prawidłowo, należy używać wirtualnego interfejsu sieciowego o przepustowości co najmniej 100 Mbit/s.

Serwery terminalowe

Obsługiwane typy serwerów terminalowych:

- Microsoft Remote Desktop Services oparty na Windows Server 2008 R2 SP1
- Microsoft Remote Desktop Services oparty na Windows Server 2012
- Microsoft Remote Desktop Services oparty na Windows Server 2012 R2
- Microsoft Remote Desktop Services oparty na Windows Server 2016
- Microsoft Remote Desktop Services oparty na Windows Server 2019
- Microsoft Remote Desktop Services oparty na Windows Server 2022
- Microsoft Remote Desktop Services oparty na Windows Server 2025
- Citrix RDSH z Citrix Virtual Apps and Desktops 7 2507 LTSR

Obsługa Kaspersky Security Center

Kaspersky Endpoint Security obsługuje pracę z następującymi wersjami Kaspersky Security Center:

- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16

- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2

Porównanie dostępnych funkcji aplikacji w zależności od typu systemu operacyjnego

Zestaw dostępnych funkcji Kaspersky Endpoint Security zależy od typu systemu operacyjnego: stacja robocza lub serwer (patrz tabela poniżej).

Począwszy od wersji Kaspersky Endpoint Security for Windows 12.8, można konfigurować różne zestawy komponentów dla różnych typów systemów operacyjnych w pakiecie instalacyjnym. Oznacza to, że możesz wdrażać aplikację na stacjach roboczych i serwerach, korzystając z tego samego pakietu instalacyjnego.

Instalacja Kaspersky Endpoint Security w trybie Light Agent na maszynach wirtualnych opartych na architekturze ARM nie jest obsługiwana.

Porównanie funkcji Kaspersky Endpoint Security

Funkcja	Stacja robocza	Stacja robocza oparta na architekturze ARM	Serwer	Tryb Server Core
Zaawansowana ochrona przed zagrożeniami				
Kaspersky Security Network	✓	✓	✓	✓
Wykrywanie zachowań	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓
Ochrona przed exploitami	✓	✓	✓	✓
Ochrona przed włamaniami	✓	✓	–	–
Silnik korygujący	✓	✓	✓	✓
Podstawowa ochrona przed zagrożeniami				
Ochrona plików	✓	✓	✓	✓
Ochrona WWW	✓	✓	✓	–
Ochrona poczty	✓	✓	✓	–
Zapora sieciowa	✓	✓	✓	✓
Ochrona sieci	✓	✓	✓	✓
Ochrona przed atakami BadUSB	✓	✓	✓	–
Ochrona AMSI	✓	✓	✓	✓
Kontrola zabezpieczeń				
Kontrola dziennika	–	–	✓	–
Kontrola aplikacji	✓	✓	✓	✓
Kontrola urządzeń	✓	✓	✓	✓
Kontrola sieci	✓	✓	✓	–
Adaptacyjna kontrola anomalii	✓	✓	–	–
Monitor integralności systemu	–	–	✓	–
Cloud Discovery	✓	✓	–	–

Funkcja	Stacja robocza	Stacja robocza oparta na architekturze ARM	Serwer	Tryb Server Core
Szyfrowanie danych				
Kaspersky Disk Encryption	✓	–	–	–
Szyfrowanie dysków funkcją BitLocker	✓	✓	✓	✓
Szyfrowanie plików	✓	–	–	–
Szyfrowanie dysków wymiennych	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	–	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
$IsKUMATelemetry ? "Integracja KUMA": "Integracja SIEM	✓	✓	✓	✓

Porównanie funkcji aplikacji w zależności od narzędzi do zarządzania

Zestaw funkcji dostępnych w Kaspersky Endpoint Security zależy od narzędzi do zarządzania (patrz tabela poniżej).

Możesz zarządzać aplikacją za pomocą następujących konsol Kaspersky Security Center:

- Konsola administracyjna. Przystawka Microsoft Management Console (MMC) zainstalowana na stacji roboczej administratora.
- Web Console. Składnik Kaspersky Security Center, który jest zainstalowany na Serwerze administracyjnym. Możesz pracować w konsoli Web Console za pomocą przeglądarki na dowolnym komputerze, który ma dostęp do Serwera administracyjnego.

Możesz także zarządzać aplikacją za pomocą konsoli Kaspersky Security Center Cloud Console. Konsola *Kaspersky Security Center Cloud Console* to wersja chmurowa Kaspersky Security Center. To oznacza, że Serwer administracyjny i inne komponenty Kaspersky Security Center są zainstalowane w infrastrukturze chmury Kaspersky. Szczegółowe informacje na temat zarządzania aplikacją za pośrednictwem Kaspersky Security Center Cloud Console można znaleźć w pomocy do Kaspersky Security Center Cloud Console.

Kaspersky Endpoint Security jest częścią rozwiązania Kaspersky Next Pro View. Aby uzyskać więcej informacji na temat dostępnych funkcji aplikacji, gdy działa ona jako część tego rozwiązania, zobacz Pomoc Kaspersky Next.

Porównanie funkcji Kaspersky Endpoint Security

Funkcja	Kaspersky Security Center		Kaspersky Security Center
	Konsola administracyjna	Web Console	Cloud Console
Zaawansowana ochrona przed zagrożeniami			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–

Funkcja	Kaspersky Security Center		Kaspersky Security Center
	Konsola administracyjna	Web Console	Cloud Console
Wykrywanie zachowań	✓	✓	✓
Anti-Cryptor			
Ochrona przed exploitami	✓	✓	✓
Ochrona przed włamaniami	✓	✓	✓
Silnik korygujący	✓	✓	✓
Podstawowa ochrona przed zagrożeniami			
Ochrona plików	✓	✓	✓
Ochrona WWW	✓	✓	✓
Ochrona poczty	✓	✓	✓
Zapora sieciowa	✓	✓	✓
Ochrona sieci	✓	✓	✓
Ochrona przed atakami BadUSB	✓	✓	✓
Ochrona AMSI	✓	✓	✓
Kontrola zabezpieczeń			
Kontrola dziennika	✓	✓	✓
Kontrola aplikacji	✓	✓	✓
Kontrola urządzeń	✓	✓	✓
Kontrola sieci	✓	✓	✓
Adaptacyjna kontrola anomalii	✓	✓	✓
Monitor integralności systemu	✓	✓	✓
Cloud Discovery	–	–	✓
Szyfrowanie danych			
Kaspersky Disk Encryption	✓	✓	–
Szyfrowanie dysków funkcją BitLocker	✓	✓	✓
Szyfrowanie plików	✓	✓	–
Szyfrowanie dysków wymiennych	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
$IsKUMATelemetry ? "Integracja KUMA": "Integracja SIEM	✓	✓	✓
Zadania			
Dodaj klucz	✓	✓	✓
Zmiana składników aplikacji	✓	✓	✓
Inwentaryzacja	✓	✓	✓
Aktualizacja	✓	✓	✓
Wycofywanie aktualizacji	✓	✓	✓

Funkcja	Kaspersky Security Center		Kaspersky Security Center
	Konsola administracyjna	Web Console	Cloud Console
Skanowanie w poszukiwaniu złośliwego oprogramowania	✓	✓	✓
Sprawdzanie integralności aplikacji	✓	✓	–
Wyczyść dane	✓	✓	✓
Zarządzanie kontami Agenta autoryzacji (Kaspersky Disk Encryption)	✓	✓	–
Skanowanie IOC (EDR)	–	✓	✓
Przenieś plik do Kwarantanny (EDR)	–	✓	✓
Uzyskaj plik (EDR)	–	✓	✓
Usuń plik (EDR)	–	✓	✓
Rozpocznij proces (EDR)	–	✓	✓
Zakończ proces (EDR)	–	✓	✓

Kompatybilność z innymi aplikacjami

Aplikacja Kaspersky Endpoint Security jest niezgodna z niektórymi aplikacjami firmy Kaspersky, a także niektórymi aplikacjami innych firm. Dlatego przed instalacją, aktualizacją wersji aplikacji i zmianą komponentów aplikacji Kaspersky Endpoint Security skanuje komputer w celu sprawdzenia, czy znajdują się na nim takie aplikacje.

Kompatybilność z aplikacjami innych firm

Kaspersky Endpoint Security jest niekompatybilny z aplikacjami będącymi częścią systemów ochrony punktów końcowych innych firm (Endpoint Protection Platform, EPP). Kaspersky Endpoint Security może również napotkać problemy z kompatybilnością z innymi aplikacjami. Aby określić kompatybilność, Kaspersky Endpoint Security sprawdza listę oprogramowania przygotowaną przez Kaspersky. Lista ta znajduje się w pliku incompatible.txt. Ten plik znajduje się w pakiecie dystrybucyjnym.

Kaspersky nie gwarantuje kompatybilności Kaspersky Endpoint Security z oprogramowaniem z listy. Jeśli zostanie wykryta aplikacja z listy, instalator zatrzyma wdrażanie Kaspersky Endpoint Security. Instalator może automatycznie usunąć niektóre aplikacje z listy. Jeśli chcesz zignorować ryzyko i chcesz zainstalować Kaspersky Endpoint Security oraz oprogramowanie z listy na tym samym komputerze, możesz pominąć sprawdzanie komputera (patrz poniższe instrukcje).

POBIERZ PLIK INCOMPATIBLE.TXT

Kompatybilność z aplikacjami Kaspersky

Program Kaspersky Endpoint Security jest niekompatybilny z następującymi aplikacjami firmy Kaspersky:

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.

- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Endpoint Sensor jako część rozwiązania Kaspersky Anti Targeted Attack Platform i Kaspersky Endpoint Detection and Response.
- Kaspersky Endpoint Agent jako część rozwiązań Detection and Response firmy Kaspersky.

  Kaspersky przełącza wszystkie funkcje Detection and Response na działanie z wbudowanym agentem Kaspersky Endpoint Security zamiast z Kaspersky Endpoint Agent. Począwszy od wersji 12.1 aplikacja obsługuje wszystkie rozwiązania Detection and Response.

- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security for Windows Server

  Zaczynając od Kaspersky Endpoint Security 12.0, możesz przeprowadzić migrację z Kaspersky Security for Windows Server do Kaspersky Endpoint Security for Windows i używać tego samego rozwiązania do ochrony stacji roboczych i serwerów.

- Kaspersky Embedded Systems Security.

Jeśli aplikacje firmy Kaspersky z tej listy są zainstalowane na komputerze, Kaspersky Endpoint Security usunie te aplikacje. Przed kontynuowaniem instalacji Kaspersky Endpoint Security należy zaczekać na zakończenie tego procesu.

Pominięcie sprawdzania oprogramowania, które może powodować problemy z kompatybilnością

Jeśli Kaspersky Endpoint Security wykryje oprogramowanie z listy incompatible.txt, instalacja aplikacji zostanie zakończona. Aby kontynuować instalację, należy usunąć tę aplikację. Jeżeli jednak dostawca innego oprogramowania zaznaczył w swojej dokumentacji, że jego oprogramowanie jest kompatybilne z Endpoint Protection Platform (EPP), możesz zainstalować Kaspersky Endpoint Security na komputerze zawierającym aplikację tego dostawcy. Na przykład dostawca rozwiązania Endpoint Detection and Response (EDR) może zadeklarować kompatybilność z systemami EPP innych firm. Jeśli tak jest, musisz rozpocząć instalację Kaspersky Endpoint Security bez uruchamiania sprawdzania zainstalowanego oprogramowania. Aby to zrobić, należy przekazać instalatorowi następujące parametry:

- `SKIPPRODUCTCHECK=1` Wyłącz sprawdzanie zainstalowanego oprogramowania. Lista oprogramowania, które może być przyczyną problemów ze zgodnością jest dostępna w pliku incompatible.txt, który znajduje się w

pakiecie dystrybucyjnym. Jeśli dla tego parametru nie zostanie ustawiona żadna wartość i zostanie wykryte oprogramowanie z listy, instalacja Kaspersky Endpoint Security zostanie zakończona.

- `SKIPPRODUCTUNINSTALL=1` Wyłącz automatyczne usuwanie wykrytego oprogramowania z listy incompatible.txt. Jeśli dla tego parametru nie zostanie ustawiona żadna wartość, Kaspersky Endpoint Security spróbuje usunąć oprogramowanie, które może powodować problemy z kompatybilnością.

- `CLEANERSIGNCHECK=0` Wyłącz weryfikację podpisu cyfrowego aplikacji znalezionych podczas kontroli. Jeśli ten parametr nie jest ustawiony, weryfikacja podpisów cyfrowych jest wyłączona podczas wdrażania aplikacji za pośrednictwem Kaspersky Security Center. Gdy aplikacja jest instalowana lokalnie, weryfikacja podpisu cyfrowego jest domyślnie włączona.

Podczas lokalnej instalacji aplikacji można przekazać parametry w wierszu poleceń.

Jeśli podczas procesu instalacji pominięto skanowanie oprogramowania, które może powodować problemy ze zgodnością, Kaspersky Endpoint Security może powtórzyć to sprawdzanie, gdy składniki aplikacji ulegną zmianie. Aby pominąć skanowanie zainstalowanego oprogramowania, należy skonfigurować zadanie *Zmiana składników aplikacji*.

Na przykład:

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

Aby zdalnie zainstalować Kaspersky Endpoint Security, należy dodać odpowiednie parametry do pliku generującego pakiet instalacyjny o nazwie `kes_win.kud` w `[Setup]` (patrz poniżej). Plik `kes_win.kud` znajduje się w pakiecie dystrybucyjnym.

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

Instalowanie i dezinstalowanie aplikacji

Program Kaspersky Endpoint Security może zostać zainstalowany na komputerze na następujące sposoby:

- lokalnie, za pomocą Kreatora instalacji.
- lokalnie, z poziomu wiersza poleceń.
- zdalnie, przy użyciu Kaspersky Security Center.
- zdalnie, za pośrednictwem Edytora zarządzania zasadami grupy Microsoft Windows (więcej informacji można znaleźć na stronie pomocy technicznej firmy Microsoft).
- zdalnie, za pomocą programu System Center Configuration Manager.

Możliwe jest skonfigurowanie ustawień instalacji aplikacji na kilka sposobów. Jeśli jednocześnie korzystasz z kilku metod konfigurowania ustawień, Kaspersky Endpoint Security stosuje ustawienia z najwyższym priorytetem. Kaspersky Endpoint Security wykorzystuje następującą kolejność priorytetów:

1. Ustawienia uzyskane z pliku setup.ini.
2. Ustawienia uzyskane z pliku installer.ini.
3. Ustawienia uzyskane z wiersza poleceń.
4. Ustawienia otrzymane z pliku konfiguracyjnego (install.cfg).

Przed rozpoczęciem instalacji Kaspersky Endpoint Security (także instalacji zdalnej) zalecamy zakończenie działania wszystkich uruchomionych aplikacji.

Podczas instalacji Kaspersky Endpoint Security system operacyjny może wyświetlać własne komunikaty. Podczas instalacji aplikacji mogą również zostać przerwane połączenia sieciowe i internetowe.

Podczas instalowania, aktualizacji lub odinstalowywania Kaspersky Endpoint Security mogą wystąpić błędy. Aby uzyskać więcej informacji na temat rozwiązywania tych błędów, zapoznaj się z Bazą wiedzy pomocy technicznej.

Wdrożenie za pośrednictwem Kaspersky Security Center

Kaspersky Endpoint Security może zostać zainstalowany na komputerach w obrębie sieci korporacyjnej na kilka sposobów. Możesz użyć scenariusza zdalnej instalacji najodpowiedniejszego dla Twojej organizacji lub połączyć kilka scenariuszy zdalnej instalacji. Przed zainstalowaniem aplikacji należy upewnić się, że na komputerze jest zainstalowany agent sieciowy Kaspersky Security Center. *Agent sieciowy* upraszcza interakcję Serwera administracyjnego z komputerem klienckim.

Kaspersky Security Center obsługuje następujące główne metody zdalnej instalacji:

- Instalowanie aplikacji przy użyciu Kreatora wdrażania ochrony.

  Standardowa metoda instalacji jest odpowiednia, jeśli jesteś usatysfakcjonowany domyślnymi ustawieniami Kaspersky Endpoint Security, a Twoja organizacja posiada prostą infrastrukturę, która nie wymaga specjalnych konfiguracji.

- Instalowanie aplikacji przy pomocy zadania zdalnej instalacji.

  Uniwersalna metoda instalacji, która umożliwia skonfigurowanie ustawień Kaspersky Endpoint Security i elastyczne zarządzanie zadaniami zdalnej instalacji. Instalacja Kaspersky Endpoint Security obejmuje następujące kroki:

  1. Tworzenie pakietu instalacyjnego.
  2. Tworzenie zadania zdalnej instalacji.

Kaspersky Security Center także obsługuje inne metody instalowania Kaspersky Endpoint Security, takie jak zdalna instalacja w obrębie obrazu systemu operacyjnego. Więcej informacji o innych metodach zdalnej instalacji można znaleźć w pomocy do Kaspersky Security Center.

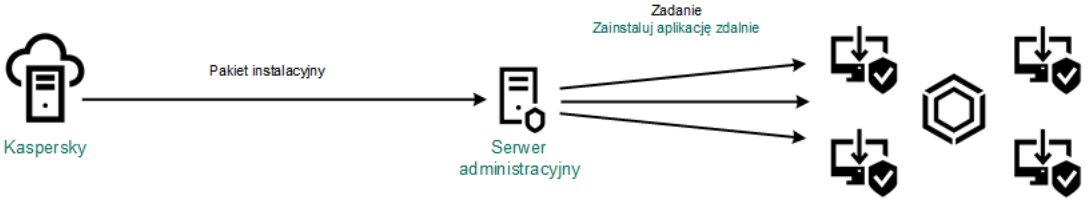
Standardowa instalacja aplikacji

Kaspersky Security Center oferuje Kreator wdrażania ochrony do zainstalowania aplikacji na komputerach firmowych. Kreator wdrażania ochrony obejmuje następujące główne działania:

1. Wybieranie pakietu instalacyjnego Kaspersky Endpoint Security.

   Pakiet instalacyjny to zestaw plików utworzonych do zdalnej instalacji aplikacji firmy Kaspersky za pośrednictwem Kaspersky Security Center. Pakiet instalacyjny zawiera zakres ustawień potrzebnych do zainstalowania aplikacji i uruchomienia jej natychmiast po zainstalowaniu. Pakiet instalacyjny jest tworzony przy użyciu plików z rozszerzeniami .kpd i .kud zawartych w pakiecie dystrybucyjnym aplikacji. Pakiet instalacyjny Kaspersky Endpoint Security jest taki sam dla wszystkich obsługiwanych wersji systemu Windows i typów architektury procesora.

2. Tworzenie zadania *Zdalna instalacja aplikacji* serwera administracyjnego Kaspersky Security Center.



Zdalna instalacja Kaspersky Endpoint Security

Jak uruchomić Kreatora wdrażania ochrony w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zaawansowane** → **Zdalna instalacja**.
3. Kliknij odnośnik **Roześlij pakiet instalacyjny na zarządzane urządzenia (stacje robocze)**.

Zostanie uruchomiony Kreator wdrażania ochrony. Postępuj zgodnie z instrukcjami Kreatora.

Porty TCP o numerach 139 i 445 oraz porty UDP o numerach 137 i 138 muszą być otwarte na komputerze klienckim.

Krok 1. Wybieranie pakietu instalacyjnego

Wybierz pakiet instalacyjny Kaspersky Endpoint Security z listy. Jeśli lista nie zawiera pakietu instalacyjnego dla Kaspersky Endpoint Security, możesz utworzyć pakiet w kreatorze.

Możesz skonfigurować ustawienia pakietu instalacyjnego w Kaspersky Security Center. Na przykład, możesz wybrać komponenty aplikacji, które zostaną zainstalowane na komputerze.

Agent sieciowy zostanie również zainstalowany razem z Kaspersky Endpoint Security. *Agent sieciowy* upraszcza interakcję Serwera administracyjnego z komputerem klienckim. Jeśli Agent sieciowy jest już zainstalowany na komputerze, nie zostanie zainstalowany ponownie.

Krok 2. Wybieranie źródła pakietu instalacyjnego

Wybierz źródło **Roześlij pakiet Kaspersky Security Center**.

Krok 3. Wybieranie urządzeń dla instalacji

Wybierz komputery, na których zostanie zainstalowany Kaspersky Endpoint Security. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Agent sieciowy nie jest zainstalowany na urządzeniach nieprzypisanych. 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, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 4. Definiowanie ustawień zadania zdalnej instalacji

Skonfiguruj następujące dodatkowe ustawienia aplikacji:

- **Wymuś pobranie pakietu instalacyjnego**. Wybierz metodę instalacji aplikacji:
  - **Przy użyciu Agenta sieciowego**. Agent sieciowy odpowiada za dostarczenie pakietu instalacyjnego Kaspersky Endpoint Security na komputery klienckie. Jeśli Agent sieciowy nie jest zainstalowany, zadanie zakończy się błędem. W takim przypadku należy dodać pakiet instalacyjny Agenta sieciowego do zadania *Zdalna instalacja aplikacji* i umożliwić dostarczanie plików za pomocą zasobów systemu operacyjnego. Następnie Agent sieciowy zostanie zainstalowany z wykorzystaniem zasobów systemu operacyjnego. Następnie Kaspersky Endpoint Security zostanie zainstalowany przez narzędzia Agenta sieciowego.
  - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**. Pakiet instalacyjny jest dostarczany na komputery klienckie przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny. Więcej informacji o punktach dystrybucji znajdziesz w pomocy do Kaspersky Security Center.
  - **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**. Pliki zostaną dostarczone na komputery klienckie przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny. Możesz wybrać tę opcję, jeśli na komputerze klienckim nie ma zainstalowanego Agenta sieciowego, ale komputer kliencki jest w tej samej sieci co Serwer administracyjny.
- **Zachowanie dla urządzeń zarządzanych poprzez inne Serwery administracyjne**. Wybierz metodę instalacji Kaspersky Endpoint Security. Jeśli w sieci jest zainstalowanych więcej niż jeden Serwer administracyjny, te Serwery administracyjne mogą widzieć te same komputery klienckie. Może to spowodować, na przykład, zdalne zainstalowanie aplikacji na tym samym komputerze kilka razy poprzez różne Serwery administracyjne lub inne konflikty.
- **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana**. Odznacz to pole, jeśli chcesz, na przykład, zainstalować wcześniejszą wersję aplikacji.
- **Przypisz instalację Agenta sieciowego do zasad grupy Active Directory**. Ręczna instalacja Agenta sieciowego przy użyciu zasobów Active Directory. Aby zainstalować Agenta sieciowego, zadanie zdalnej instalacji musi być uruchomione z uprawnieniami administratora domeny.

Krok 5. Wybieranie klucza licencyjnego

Dodaj klucz do pakietu instalacyjnego w celu aktywowania aplikacji. Ten krok jest opcjonalny. Jeśli Serwer administracyjny zawiera klucz licencyjny z funkcją automatycznej dystrybucji, klucz zostanie automatycznie dodany w późniejszym czasie. Możesz także aktywować aplikację w późniejszym czasie podczas korzystania z zadania *Dodaj klucz*.

Krok 6. Wybieranie ustawienia ponownego uruchomienia systemu operacyjnego

Wybierz akcję, jaka ma zostać wykonana, jeśli wymagane jest ponowne uruchomienie komputera. Ponowne uruchomienie nie jest wymagane podczas instalowania Kaspersky Endpoint Security. Ponowne uruchomienie jest wymagane tylko wtedy, gdy przed instalacją musisz usunąć niekompatybilne aplikacje. Ponowne uruchomienie może być też wymagane podczas aktualizowania wersji aplikacji.

Krok 7. Usuwanie niekompatybilnych aplikacji przed zainstalowaniem aplikacji

Uważnie przeczytaj listę niekompatybilnych aplikacji i zezwól na odinstalowanie tych aplikacji. Jeśli na komputerze są zainstalowane niekompatybilne aplikacje, instalacja Kaspersky Endpoint Security zakończy się błędem.

Krok 8. Wybieranie konta w celu uzyskania dostępu do urządzeń

Wybierz konto do zainstalowania Agenta sieciowego przy użyciu narzędzi systemu operacyjnego. W tym przypadku uprawnienia administratora są wymagane do uzyskania dostępu do komputera. Możesz dodać kilka kont. Jeśli konto nie posiada wystarczających uprawnień, Kreator instalacji użyje następnego konta. Jeśli instalujesz Kaspersky Endpoint Security przy użyciu narzędzi Agenta sieciowego, nie musisz wybrać konta.

Krok 9. Rozpoczynanie instalacji

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Jak uruchomić Kreatora wdrażania ochrony w Web Console i Cloud Console?

W oknie głównym Web Console wybierz **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Kreator wdrażania ochrony**.

Zostanie uruchomiony Kreator wdrażania ochrony. Postępuj zgodnie z instrukcjami Kreatora.

Porty TCP o numerach 139 i 445 oraz porty UDP o numerach 137 i 138 muszą być otwarte na komputerze klienckim.

Krok 1. Wybieranie pakietu instalacyjnego

Wybierz pakiet instalacyjny Kaspersky Endpoint Security z listy. Jeśli lista nie zawiera pakietu instalacyjnego dla Kaspersky Endpoint Security, możesz utworzyć pakiet w kreatorze. Aby utworzyć pakiet instalacyjny, nie jest konieczne wyszukanie pakietu dystrybucyjnego i zapisanie go w pamięci komputera. W Kaspersky Security Center możesz przejrzeć listę pakietów dystrybucyjnych znajdujących się na serwerach Kaspersky, a pakiet instalacyjny zostanie utworzony automatycznie. Kaspersky zaktualizuje listę po publikacji nowych wersji aplikacji.

Możesz skonfigurować ustawienia pakietu instalacyjnego w Kaspersky Security Center. Na przykład, możesz wybrać komponenty aplikacji, które zostaną zainstalowane na komputerze.

Krok 2. Wybieranie klucza licencyjnego

Dodaj klucz do pakietu instalacyjnego w celu aktywowania aplikacji. Ten krok jest opcjonalny. Jeśli Serwer administracyjny zawiera klucz licencyjny z funkcją automatycznej dystrybucji, klucz zostanie automatycznie dodany w późniejszym czasie. Możesz także aktywować aplikację w późniejszym czasie podczas korzystania z zadania *Dodaj klucz*.

Krok 3. Wybieranie Agenta sieciowego

Wybierz wersję Agenta sieciowego, która zostanie zainstalowana wraz z Kaspersky Endpoint Security. *Agent sieciowy* upraszcza interakcję Serwera administracyjnego z komputerem klienckim. Jeśli Agent sieciowy jest już zainstalowany na komputerze, nie zostanie zainstalowany ponownie.

Krok 4. Wybieranie urządzeń dla instalacji

Wybierz komputery, na których zostanie zainstalowany Kaspersky Endpoint Security. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Agent sieciowy nie jest zainstalowany na urządzeniach nieprzypisanych. 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, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 5. Konfigurowanie ustawień zaawansowanych

Skonfiguruj następujące dodatkowe ustawienia aplikacji:

- **Wymuś pobranie pakietu instalacyjnego**. Wybierz metodę instalacji aplikacji:
  - **Przy użyciu Agenta sieciowego**. Agent sieciowy odpowiada za dostarczenie pakietu instalacyjnego Kaspersky Endpoint Security na komputery klienckie. Jeśli Agent sieciowy nie jest zainstalowany, zadanie zakończy się błędem. W takim przypadku należy dodać pakiet instalacyjny Agenta sieciowego do zadania *Zdalna instalacja aplikacji* i umożliwić dostarczanie plików za pomocą zasobów systemu operacyjnego. Następnie Agent sieciowy zostanie zainstalowany z wykorzystaniem zasobów systemu operacyjnego. Następnie Kaspersky Endpoint Security zostanie zainstalowany przez narzędzia Agenta sieciowego.
  - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**. Pakiet instalacyjny jest dostarczany na komputery klienckie przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny. Więcej informacji o punktach dystrybucji znajdziesz w pomocy do Kaspersky Security Center.
  - **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**. Pliki zostaną dostarczone na komputery klienckie przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny. Możesz wybrać tę opcję, jeśli na komputerze klienckim nie ma zainstalowanego Agenta sieciowego, ale komputer kliencki jest w tej samej sieci co Serwer administracyjny.
- **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana**. Odznacz to pole, jeśli chcesz, na przykład, zainstalować wcześniejszą wersję aplikacji.
- **Przypisz pakiet instalacyjny do zasad grupy Active Directory**. Kaspersky Endpoint Security jest instalowany przy użyciu Agenta sieciowego lub ręcznie przy użyciu Active Directory. Aby zainstalować Agenta sieciowego, zadanie zdalnej instalacji musi być uruchomione z uprawnieniami administratora domeny.

Krok 6. Wybieranie ustawienia ponownego uruchomienia systemu operacyjnego

Wybierz akcję, jaka ma zostać wykonana, jeśli wymagane jest ponowne uruchomienie komputera. Ponowne uruchomienie nie jest wymagane podczas instalowania Kaspersky Endpoint Security. Ponowne uruchomienie jest wymagane tylko wtedy, gdy przed instalacją musisz usunąć niekompatybilne aplikacje. Ponowne uruchomienie może być też wymagane podczas aktualizowania wersji aplikacji.

Krok 7. Usuwanie niekompatybilnych aplikacji przed zainstalowaniem aplikacji

Uważnie przeczytaj listę niekompatybilnych aplikacji i zezwól na odinstalowanie tych aplikacji. Jeśli na komputerze są zainstalowane niekompatybilne aplikacje, instalacja Kaspersky Endpoint Security zakończy się błędem.

Krok 8. Przypisywanie do grupy administracyjnej

Wybierz grupę administracyjną, do której komputery zostaną przeniesione po zainstalowaniu Agenta sieciowego. Komputery należy przenieść do grupy administracyjnej, aby można było zastosować zasady i zadania grupowe. Jeśli komputer jest już w dowolnej grupie administracyjnej, komputer nie zostanie przeniesiony. Jeśli nie wybierzesz grupy administracyjnej, komputery zostaną dodane do grupy **Urządzenia nieprzypisane**.

Krok 9. Wybieranie konta w celu uzyskania dostępu do urządzeń

Wybierz konto do zainstalowania Agenta sieciowego przy użyciu narzędzi systemu operacyjnego. W tym przypadku uprawnienia administratora są wymagane do uzyskania dostępu do komputera. Możesz dodać kilka kont. Jeśli konto nie posiada wystarczających uprawnień, Kreator instalacji użyje następnego konta. Jeśli instalujesz Kaspersky Endpoint Security przy użyciu narzędzi Agenta sieciowego, nie musisz wybrać konta.

Krok 10. Uruchamianie instalacji

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Tworzenie pakietu instalacyjnego

Pakiet instalacyjny to zestaw plików utworzonych do zdalnej instalacji aplikacji firmy Kaspersky za pośrednictwem Kaspersky Security Center. Pakiet instalacyjny zawiera zakres ustawień potrzebnych do zainstalowania aplikacji i uruchomienia jej natychmiast po zainstalowaniu. Pakiet instalacyjny jest tworzony przy użyciu plików z rozszerzeniami .kpd i .kud zawartych w pakiecie dystrybucyjnym aplikacji. Pakiet instalacyjny Kaspersky Endpoint Security jest taki sam dla wszystkich obsługiwanych wersji systemu Windows i typów architektury procesora.

Jak utworzyć pakiet instalacyjny w Konsoli administracyjnej (MMC)?

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Zaawansowane** → **Zdalna instalacja** → **Pakiety instalacyjne**.

   Spowoduje to otwarcie listy pakietów instalacyjnych, które zostały pobrane do Kaspersky Security Center.

2. Kliknij **Utwórz pakiet instalacyjny**.

Zostanie uruchomiony Kreator tworzenia nowego pakietu. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu pakietu instalacyjnego

Wybierz opcję **Utwórz pakiet instalacyjny dla aplikacji Kaspersky**.

Krok 2. Definiowanie nazwy pakietu instalacyjnego

Wprowadź nazwę pakietu instalacyjnego, na przykład: *Kaspersky Endpoint Security for Windows 14.1*.

Krok 3. Wybieranie pakietu dystrybucyjnego do instalacji

Kliknij przycisk **Przeglądaj** i wybierz plik `kes_win.kud`, który jest zawarty w pakiecie dystrybucyjnym.

W razie konieczności zaktualizuj bazy danych antywirusów w pakiecie instalacyjnym za pomocą pola wyboru **Kopiuj uaktualnienia z repozytorium do pakietów instalacyjnych**.

Krok 4. Umowa Licencyjna Użytkownika Końcowego i Polityka prywatności

Przeczytaj i zaakceptuj warunki Umowy Licencyjnej Użytkownika Końcowego i Polityki prywatności.

Pakiet instalacyjny zostanie utworzony i dodany do Kaspersky Security Center. Korzystając z pakietu instalacyjnego, możesz zainstalować Kaspersky Endpoint Security na komputerach w sieci firmowej lub zaktualizować wersję aplikacji.

W ustawieniach pakietu instalacyjnego można wybrać komponenty aplikacji dla różnych typów systemów operacyjnych. Oznacza to, że pakiet instalacyjny zawiera dwa zestawy komponentów: dla stacji roboczych i serwerów. Przed wdrożeniem pakietu instalacyjnego instalator wykrywa typ systemu operacyjnego i instaluje tylko te komponenty aplikacji, które zostały wybrane dla tego typu systemu operacyjnego. Dzięki temu możesz używać tego samego pakietu instalacyjnego na stacjach roboczych i serwerach.

Pakiet instalacyjny zawiera antywirusowe bazy danych z repozytorium Serwera administracyjnego. Możesz zaktualizować bazy danych w pakiecie instalacyjnym, aby zmniejszyć ruch sieciowy podczas aktualizacji baz danych po zainstalowaniu Kaspersky Endpoint Security.

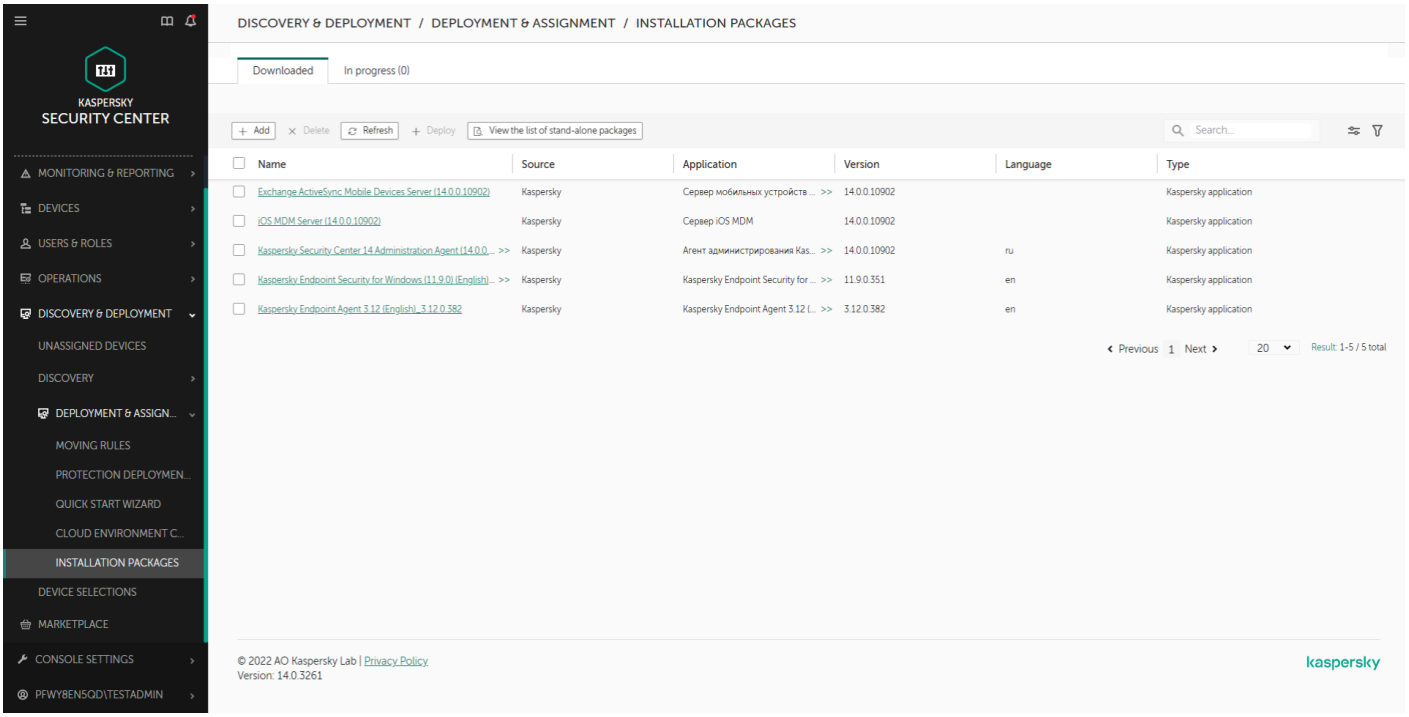
Jak utworzyć pakiet instalacyjny w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Wykrywanie i wdrażanie → Wdrażanie i przypisywanie → Pakiety instalacyjne**.

   Spowoduje to otwarcie listy pakietów instalacyjnych, które zostały pobrane do Kaspersky Security Center.

2. Kliknij **Dodaj**.

Zostanie uruchomiony Kreator tworzenia nowego pakietu. Postępuj zgodnie z instrukcjami Kreatora.



Lista pakietów instalacyjnych

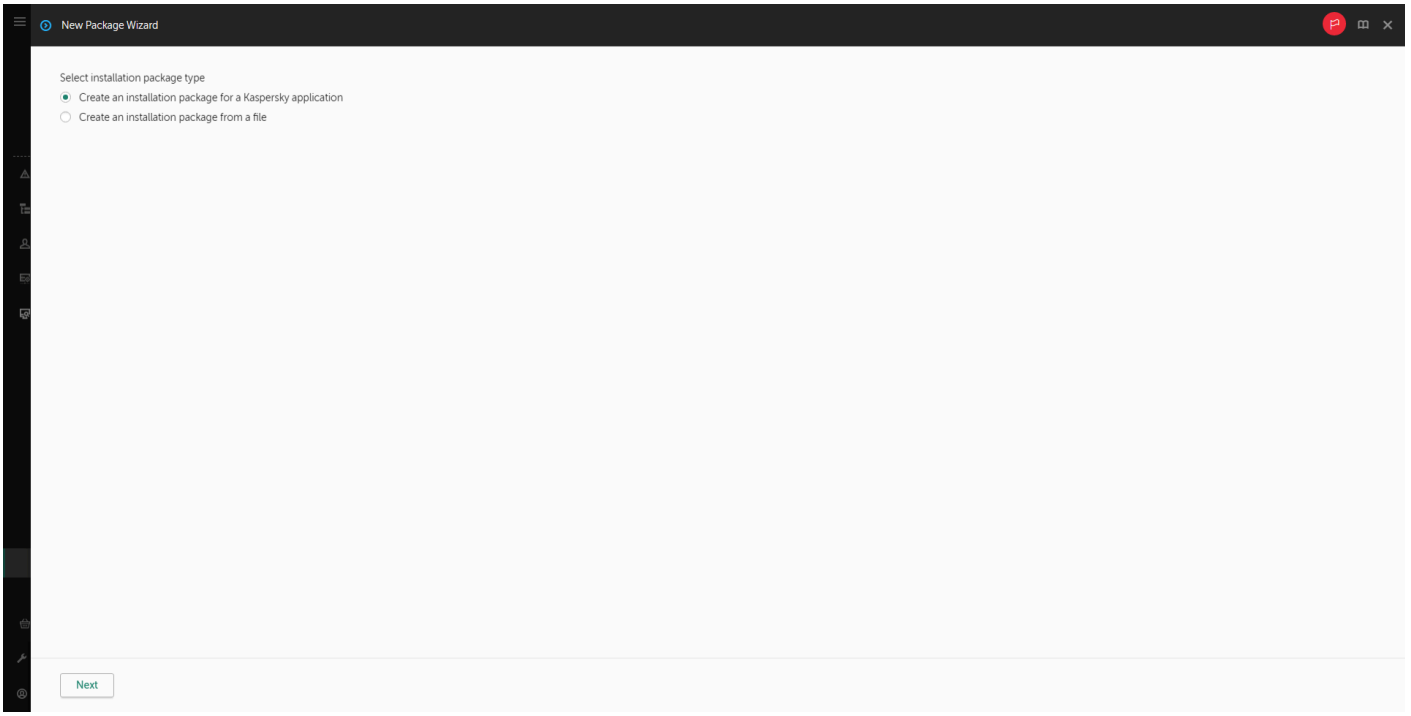
Krok 1. Wybieranie typu pakietu instalacyjnego

Wybierz opcję **Utwórz pakiet instalacyjny dla aplikacji Kaspersky**.

Kreator utworzy pakiet instalacyjny z pakietu dystrybucyjnego znajdującego się na serwerach Kaspersky. Lista jest aktualizowana automatycznie, gdy zostaną opublikowane nowe wersje aplikacji. Zalecane jest wybranie tej opcji dla instalacji Kaspersky Endpoint Security.

Możliwe jest także utworzenie pakietu instalacyjnego z pliku.

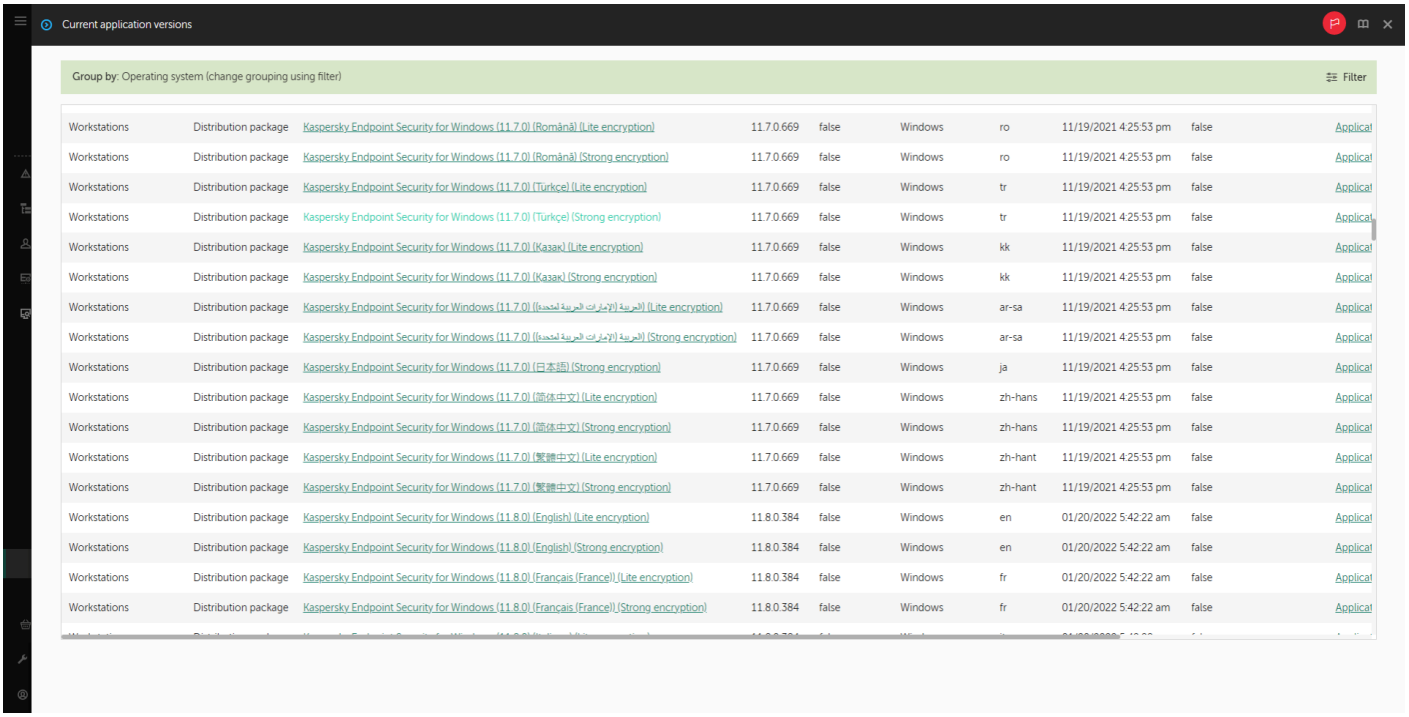
Utworzenie pakietu instalacyjnego Kaspersky Endpoint Security z pliku jest możliwe tylko w Kaspersky Security Center Web Console.



Rodzaje pakietów instalacyjnych

Krok 2. Pakiety instalacyjne

Wybierz pakiet instalacyjny Kaspersky Endpoint Security for Windows. Zostanie uruchomiony proces tworzenia pakietu instalacyjnego. Podczas tworzenia pakietu instalacyjnego należy zaakceptować warunki Umowy licencyjnej i Polityki prywatności.

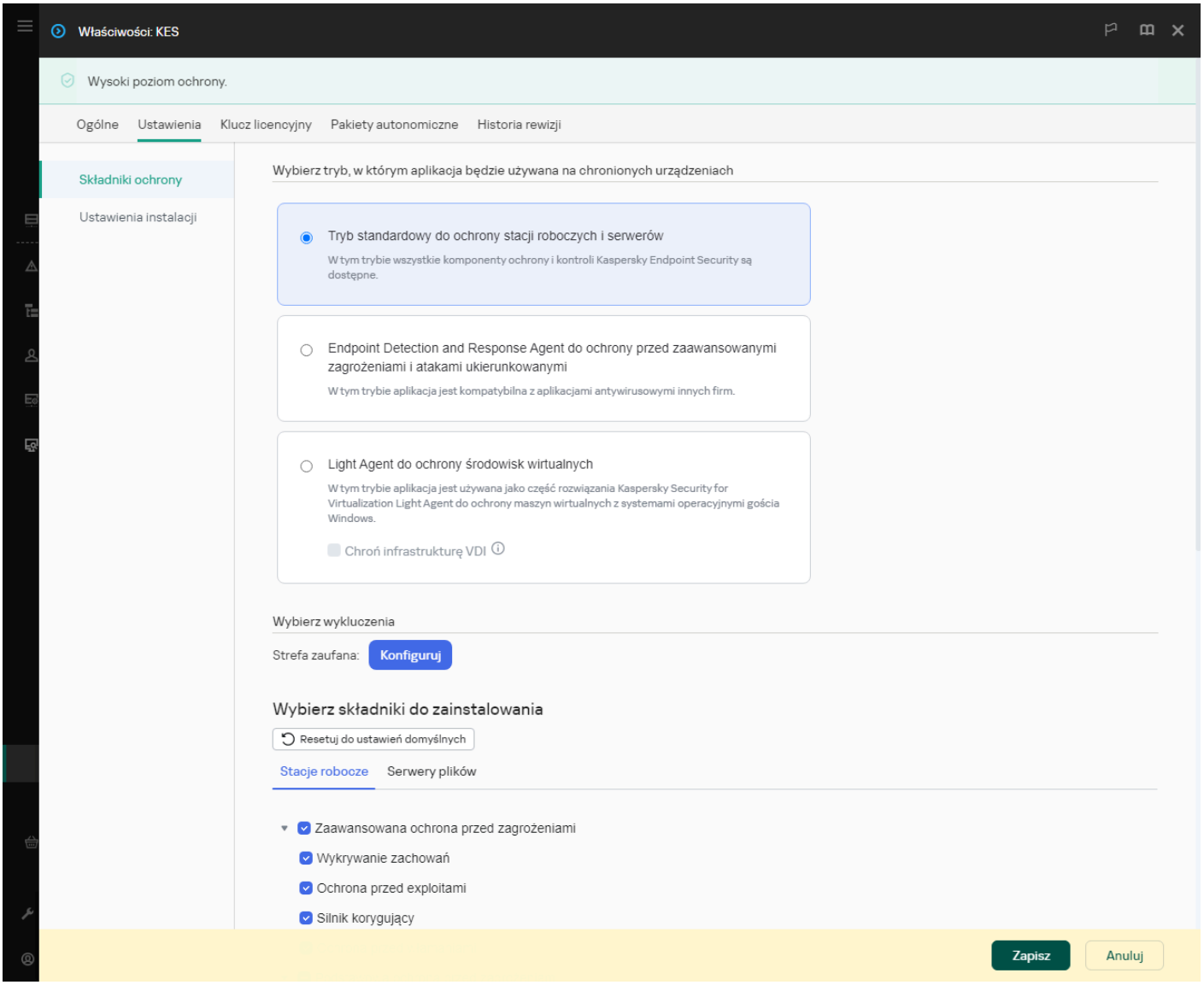


Lista pakietów instalacyjnych na serwerach Kaspersky

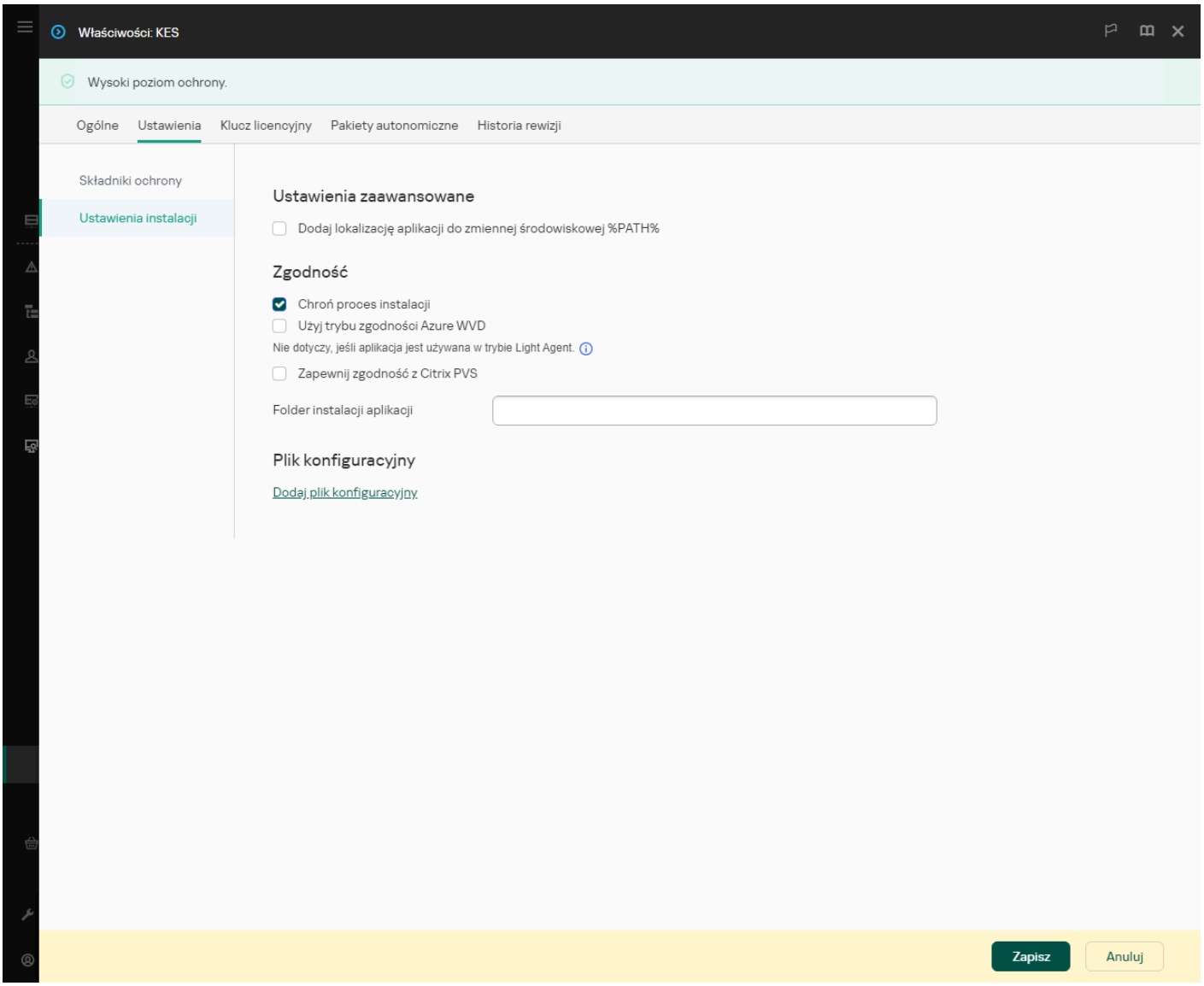
Pakiet instalacyjny zostanie utworzony i dodany do Kaspersky Security Center. Korzystając z pakietu instalacyjnego, możesz zainstalować Kaspersky Endpoint Security na komputerach w sieci firmowej lub zaktualizować wersję aplikacji.

W ustawieniach pakietu instalacyjnego można wybrać komponenty aplikacji dla różnych typów systemów operacyjnych. Oznacza to, że pakiet instalacyjny zawiera dwa zestawy komponentów: dla stacji roboczych i serwerów. Przed wdrożeniem pakietu instalacyjnego instalator wykrywa typ systemu operacyjnego i instaluje tylko te komponenty aplikacji, które zostały wybrane dla tego typu systemu operacyjnego. Dzięki temu możesz używać tego samego pakietu instalacyjnego na stacjach roboczych i serwerach.

Pakiet instalacyjny zawiera antywirusowe bazy danych z repozytorium Serwera administracyjnego. Możesz zaktualizować bazy danych w pakiecie instalacyjnym, aby zmniejszyć ruch sieciowy podczas aktualizacji baz danych po zainstalowaniu Kaspersky Endpoint Security.



Komponenty zawarte w pakiecie instalacyjnym



Ustawienia instalacji pakietu instalacyjnego

Ustawienia pakietu instalacyjnego

Sekcja	Opis
Składniki ochrony	**Tryb standardowy**. Domyślna konfiguracja. Ta konfiguracja umożliwia korzystanie ze wszystkich komponentów aplikacji, w tym komponentów zapewniających obsługę rozwiązań do Detection and Response. Ta konfiguracja służy do kompleksowej ochrony komputera przed różnymi zagrożeniami, atakami sieciowymi i oszustwami. **Endpoint Detection and Response Agent**. W tej konfiguracji można zainstalować wyłącznie komponenty zapewniające obsługę rozwiązań wykrywania i reagowania: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), jak również KUMA. Ta konfiguracja jest wymagana, jeśli w Twojej organizacji wdrożona jest platforma Endpoint Protection Platform (EPP) innej firmy wraz z rozwiązaniem Kaspersky Detection and Response. Dzięki temu Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent jest kompatybilny z aplikacjami EPP innych firm. **Light Agent do ochrony środowisk wirtualnych**. Ta konfiguracja jest przeznaczona do aplikacji stanowiącej część rozwiązania Kaspersky Security for Virtualization Light Agent. Klienta Light Agent należy zainstalować na każdej maszynie wirtualnej, która ma być chroniona za pomocą tego rozwiązania. W tej konfiguracji nie można używać komponentów Szyfrowania danych ani Adaptacyjnej kontroli anomalii. Jeśli instalujesz klienta Light Agent na szablonie maszyny wirtualnej, który będzie używany do tworzenia *nietrwałych maszyn wirtualnych*, zaznacz pole **Chroń infrastrukturę VDI** (VDI oznacza Virtual Desktop Infrastructure). Tryb ochrony VDI pomaga zoptymalizować działanie Kaspersky Endpoint Security na nietrwałych maszynach wirtualnych. W tym trybie Light Agent odrzuca aktualizacje aplikacji wymagające ponownego uruchomienia maszyny wirtualnej. Po otrzymaniu aktualizacji aplikacji wymagających ponownego uruchomienia Light Agent generuje zdarzenie informujące o konieczności zaktualizowania szablonu chronionych maszyn wirtualnych.
Wykluczenia	Począwszy od Kaspersky Endpoint Security 12.6 for Windows, wykluczenia skanowania i zaufane aplikacje są dodawane do strefy zaufanej. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach. Począwszy od Kaspersky Endpoint Security 12.8 for Windows można instalować aplikację w trybie Light Agent w celu ochrony środowisk wirtualnych. Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje mogą pomóc w szybkiej konfiguracji Kaspersky Endpoint Security w środowiskach wirtualnych Citrix i VMware. Możesz również skonfigurować strefę zaufaną później we właściwościach zasad: wykluczenia ze skanowania i zaufane aplikacje.

Sekcja	Opis
Wybierz składniki do zainstalowania	W tej sekcji możesz wybrać komponenty aplikacji, które będą dostępne. Zestaw komponentów aplikacji możesz zmienić w późniejszym terminie, korzystając z zadania *Zmiana składników aplikacji*. Możesz tworzyć osobne zestawy komponentów dla stacji roboczych i serwerów. Przed wdrożeniem pakietu instalacyjnego instalator wykrywa typ systemu operacyjnego i instaluje tylko te komponenty aplikacji, które zostały wybrane dla tego typu systemu operacyjnego. Dzięki temu możesz używać tego samego pakietu instalacyjnego na stacjach roboczych i serwerach. Zestaw dostępnych komponentów zależy od konfiguracji aplikacji: **Tryb standardowy** Komponent Ochrona przed atakami BadUSB, komponent Detection and Response oraz komponenty szyfrowania danych nie są instalowane domyślnie. Te komponenty mogą zostać dodane w ustawieniach pakietu instalacyjnego. **Endpoint Detection and Response Agent** W tej konfiguracji dostępne są wyłącznie wbudowane agenty rozwiązań Kaspersky Detection and Response. **Light Agent do ochrony środowisk wirtualnych** W tej konfiguracji można używać niemal wszystkich dostępnych w aplikacji komponentów w konfiguracji **Tryb standardowy**, z wyjątkiem komponentów szyfrowania danych i Adaptacyjnej kontroli anomalii.
Klucz licencyjny	W tej sekcji możesz aktywować aplikację. Aby aktywować aplikację, należy wybrać klucz licencyjny. Przed zrobieniem tego należy dodać klucz do Serwera administracyjnego. Więcej informacji na temat dodawania kluczy do Serwera administracyjnego Kaspersky Security Center można znaleźć w pomocy do Kaspersky Security Center.
Niekompatybilne aplikacje	Uważnie przeczytaj listę niekompatybilnych aplikacji i zezwól na odinstalowanie tych aplikacji. Jeśli na komputerze są zainstalowane niekompatybilne aplikacje, instalacja Kaspersky Endpoint Security zakończy się błędem.
Ustawienia instalacji	**Dodaj ścieżkę do pliku avp.com do zmiennej systemowej %PATH%**. Możesz dodać ścieżkę instalacji do zmiennej %PATH% dla wygodnego korzystania z interfejsu wiersza poleceń. **Chroń proces instalacji**. Ochrona instalacji obejmuje ochronę przed zastąpieniem pakietu dystrybucyjnego szkodliwymi aplikacjami, blokowaniem dostępu do folderu instalacyjnego Kaspersky Endpoint Security, a także blokowaniem dostępu do sekcji rejestru systemu zawierającego klucze aplikacji. Jeżeli aplikacja nie może zostać zainstalowana (na przykład podczas zdalnej instalacji przy użyciu Windows Remote Desktop), zalecane jest wyłączenie ochrony procesu instalacji. **Zapewnij zgodność z Citrix PVS**. Możesz włączyć obsługę Citrix Provisioning Services, aby zainstalować Kaspersky Endpoint Security na maszynie wirtualnej. **Użyj trybu zgodności Azure WVD**. Ta funkcja zapewnia prawidłowe wyświetlanie stanu maszyny wirtualnej Azure w konsoli Kaspersky Anti Targeted Attack Platform. Aby monitorować wydajność komputera, Kaspersky Endpoint Security wysyła dane telemetryczne do serwerów KATA. Dane telemetryczne obejmują identyfikator komputera (Sensor ID). Tryb zgodności Azure WVD umożliwia przypisanie do tych maszyn wirtualnych trwałego unikatowego identyfikatora Sensor ID. Jeśli tryb zgodności jest wyłączony, Sensor ID może ulec zmianie po ponownym uruchomieniu komputera ze względu na sposób działania maszyn wirtualnych platformy Azure. Może to spowodować pojawienie się duplikatów maszyn wirtualnych w konsoli. **Folder instalacji aplikacji**. Możesz zmienić ścieżkę instalacji Kaspersky Endpoint Security na komputerze klienckim. Domyślnie, aplikacja jest instalowana w folderze `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.1`. **Plik konfiguracyjny**. Instalowanie aplikacji ze wstępnie zdefiniowanymi ustawieniami. Aby to zrobić, musisz przesłać plik, który definiuje ustawienia Kaspersky Endpoint Security. Możesz utworzyć plik konfiguracyjny w interfejsie lokalnym aplikacji.

Aktualizowanie baz danych w pakiecie instalacyjnym

Pakiet instalacyjny zawiera antywirusowe bazy danych z repozytorium Serwera administracyjnego, które są aktualne podczas tworzenia pakietu instalacyjnego. Po utworzeniu pakietu instalacyjnego możesz zaktualizować antywirusowe bazy danych w pakiecie instalacyjnym. Pozwala to zmniejszyć ruch sieciowy podczas aktualizacji antywirusowych baz danych po zainstalowaniu Kaspersky Endpoint Security.

Aby zaktualizować antywirusowe bazy danych w repozytorium Serwera administracyjnego, użyj zadania serwera administracyjnego *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Aby uzyskać więcej informacji na temat aktualizacji antywirusowych baz danych w repozytorium Serwera administracyjnego, zapoznaj się z systemem pomocy dla Kaspersky Security Center.

Możesz zaktualizować bazy danych w pakiecie instalacyjnym tylko w Konsoli administracyjnej i konsoli Kaspersky Security Center Web Console. Nie ma możliwości aktualizacji baz danych w pakiecie instalacyjnym w konsoli Security Center Kaspersky Security Center Cloud Console.

Jak zaktualizować antywirusowe bazy danych w pakiecie instalacyjnym za pomocą Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz folder **Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

   Spowoduje to otwarcie listy pakietów instalacyjnych, które zostały pobrane do Kaspersky Security Center.
3. Otwórz właściwości pakietu instalacyjnego.
4. W sekcji **Ogólne** kliknij **Aktualizuj bazy danych**.

W rezultacie antywirusowe bazy danych w pakiecie instalacyjnym zostaną zaktualizowane z repozytorium Serwera administracyjnego. Plik `bases.cab` znajdujący się w pakiecie dystrybucyjnym zostanie zastąpiony folderem `bases`. Pliki pakietu aktualizacji będą znajdować się w folderze.

Jak aktualizować antywirusowe bazy danych w pakiecie instalacyjnym za pośrednictwem konsoli Web Console?

1. W oknie głównym Web Console wybierz **Wykrywanie i wdrażanie → Wdrażanie i przypisywanie → Pakiety instalacyjne**.

   Spowoduje to otwarcie listy pakietów instalacyjnych pobranych do Web Console.
2. Kliknij nazwę pakietu instalacyjnego Kaspersky Endpoint Security, w którym chcesz zaktualizować antywirusowe bazy danych.

   Zostanie otwarte okno właściwości pakietu instalacyjnego.
3. Na zakładce **Informacje ogólne** kliknij odnośnik **Aktualizuj bazy danych**.

W rezultacie antywirusowe bazy danych w pakiecie instalacyjnym zostaną zaktualizowane z repozytorium Serwera administracyjnego. Plik `bases.cab` znajdujący się w pakiecie dystrybucyjnym zostanie zastąpiony folderem `bases`. Pliki pakietu aktualizacji będą znajdować się w folderze.

Tworzenie zadania zdalnej instalacji

Zadanie *Zdalna instalacja aplikacji* jest przeznaczone do zdalnej instalacji Kaspersky Endpoint Security. Zadanie *Zdalna instalacja aplikacji* pozwala wdrożyć pakiet instalacyjny aplikacji na wszystkich komputerach w organizacji. Przed wdrożeniem pakietu instalacyjnego można zaktualizować antywirusowe bazy danych wewnątrz pakietu i wybrać dostępne komponenty aplikacji we właściwościach pakietu instalacyjnego.

Jak utworzyć zadanie zdalnej instalacji w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zadania**.

   Zostanie otwarta lista zadań.
3. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Serwer administracyjny Kaspersky Security Center → Zdalna instalacja aplikacji**.

Krok 2. Wybieranie pakietu instalacyjnego

Wybierz pakiet instalacyjny Kaspersky Endpoint Security z listy. Jeśli lista nie zawiera pakietu instalacyjnego dla Kaspersky Endpoint Security, możesz utworzyć pakiet w kreatorze.

Możesz skonfigurować ustawienia pakietu instalacyjnego w Kaspersky Security Center. Na przykład, możesz wybrać komponenty aplikacji, które zostaną zainstalowane na komputerze.

Agent sieciowy zostanie również zainstalowany razem z Kaspersky Endpoint Security. *Agent sieciowy* upraszcza interakcję Serwera administracyjnego z komputerem klienckim. Jeśli Agent sieciowy jest już zainstalowany na komputerze, nie zostanie zainstalowany ponownie.

Krok 3. Dodatkowe

Wybierz pakiet instalacyjny Agenta sieciowego. Wybrana wersja Agenta sieciowego zostanie zainstalowana wraz z Kaspersky Endpoint Security.

Krok 4. Ustawienia

Skonfiguruj następujące dodatkowe ustawienia aplikacji:

- **Wymuś pobranie pakietu instalacyjnego**. Wybierz metodę instalacji aplikacji:
  - **Przy użyciu Agenta sieciowego**. Agent sieciowy odpowiada za dostarczenie pakietu instalacyjnego Kaspersky Endpoint Security na komputery klienckie. Jeśli Agent sieciowy nie jest zainstalowany, zadanie zakończy się błędem. W takim przypadku należy dodać pakiet instalacyjny Agenta sieciowego do zadania *Zdalna instalacja aplikacji* i umożliwić dostarczanie plików za pomocą zasobów systemu operacyjnego. Następnie Agent sieciowy zostanie zainstalowany z wykorzystaniem zasobów systemu operacyjnego. Następnie Kaspersky Endpoint Security zostanie zainstalowany przez narzędzia Agenta sieciowego.
  - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**. Pakiet instalacyjny jest dostarczany na komputery klienckie przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny. Więcej informacji o punktach dystrybucji znajdziesz w pomocy do Kaspersky Security Center.
  - **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**. Pliki zostaną dostarczone na komputery klienckie przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny. Możesz wybrać tę opcję, jeśli na komputerze klienckim nie ma zainstalowanego Agenta sieciowego, ale komputer kliencki jest w tej samej sieci co Serwer administracyjny.

- **Zachowanie dla urządzeń zarządzanych poprzez inne Serwery administracyjne**. Wybierz metodę instalacji Kaspersky Endpoint Security. Jeśli w sieci jest zainstalowanych więcej niż jeden Serwer administracyjny, te Serwery administracyjne mogą widzieć te same komputery klienckie. Może to spowodować, na przykład, zdalne zainstalowanie aplikacji na tym samym komputerze kilka razy poprzez różne Serwery administracyjne lub inne konflikty.

- **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana**. Odznacz to pole, jeśli chcesz, na przykład, zainstalować wcześniejszą wersję aplikacji.

Krok 5. Wybieranie ustawienia ponownego uruchomienia systemu operacyjnego

Wybierz akcję, jaka ma zostać wykonana, jeśli wymagane jest ponowne uruchomienie komputera. Ponowne uruchomienie nie jest wymagane podczas instalowania Kaspersky Endpoint Security. Ponowne uruchomienie jest wymagane tylko wtedy, gdy przed instalacją musisz usunąć niekompatybilne aplikacje. Ponowne uruchomienie może być też wymagane podczas aktualizowania wersji aplikacji.

Krok 6. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zostanie zainstalowany Kaspersky Endpoint Security. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.

- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Agent sieciowy nie jest zainstalowany na urządzeniach nieprzypisanych. 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, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 7. Wybieranie konta do uruchomienia zadania

Wybierz konto do zainstalowania Agenta sieciowego przy użyciu narzędzi systemu operacyjnego. W tym przypadku uprawnienia administratora są wymagane do uzyskania dostępu do komputera. Możesz dodać kilka kont. Jeśli konto nie posiada wystarczających uprawnień, Kreator instalacji użyje następnego konta. Jeśli instalujesz Kaspersky Endpoint Security przy użyciu narzędzi Agenta sieciowego, nie musisz wybrać konta.

Krok 8. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz uruchamiania zadania, na przykład, ręcznie lub gdy komputer jest w trybie bezczynności.

Krok 9. Definiowanie nazwy zadania

Wprowadź nazwę zadania na przykład: *Zainstaluj Kaspersky Endpoint Security for Windows 14.1*.

Krok 10. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania. Aplikacja zostanie zainstalowana w trybie cichym. Po instalacji, ikona zostanie dodana do obszaru powiadomień komputera użytkownika. Jeśli ikona wygląda w następujący sposób , upewnij się, że aktywowałeś aplikację.

Jak utworzyć zadanie zdalnej instalacji w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Security Center**.
2. Z listy rozwijalnej **Typ zadania** wybierz **Zdalna instalacja aplikacji**.
3. W polu **Nazwa zadania** wpisz krótki opis, na przykład, *Instalacja Kaspersky Endpoint Security dla menadżerów*.
4. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

Krok 2. Wybieranie komputerów dla instalacji

W tym kroku wybierz komputery, na których ma być zainstalowany Kaspersky Endpoint Security zgodnie z obszarem wybranego zadania.

Krok 3. Konfigurowanie pakietu instalacyjnego

W tym kroku skonfiguruj pakiet instalacyjny:

1. Wybierz pakiet instalacyjny Kaspersky Endpoint Security for Windows (14.1).

2. Wybierz pakiet instalacyjny Agenta sieciowego.

   Wybrana wersja Agenta sieciowego zostanie zainstalowana wraz z Kaspersky Endpoint Security. *Agent sieciowy* upraszcza interakcję Serwera administracyjnego z komputerem klienckim. Jeśli Agent sieciowy jest już zainstalowany na komputerze, nie zostanie zainstalowany ponownie.

3. W sekcji **Wymuś pobranie pakietu instalacyjnego** wybierz metodę instalacji aplikacji:

   - **Przy użyciu Agenta sieciowego**. Agent sieciowy odpowiada za dostarczenie pakietu instalacyjnego Kaspersky Endpoint Security na komputery klienckie. Jeśli Agent sieciowy nie jest zainstalowany, zadanie zakończy się błędem. W takim przypadku należy dodać pakiet instalacyjny Agenta sieciowego do zadania *Zdalna instalacja aplikacji* i umożliwić dostarczanie plików za pomocą zasobów systemu operacyjnego. Następnie Agent sieciowy zostanie zainstalowany z wykorzystaniem zasobów systemu operacyjnego. Następnie Kaspersky Endpoint Security zostanie zainstalowany przez narzędzia Agenta sieciowego.

   - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**. Pakiet instalacyjny jest dostarczany na komputery klienckie przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny. Więcej informacji o punktach dystrybucji znajdziesz w pomocy do Kaspersky Security Center.

   - **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**. Pliki zostaną dostarczone na komputery klienckie przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny. Możesz wybrać tę opcję, jeśli na komputerze klienckim nie ma zainstalowanego Agenta sieciowego, ale komputer kliencki jest w tej samej sieci co Serwer administracyjny.

4. W polu **Maksymalna liczba dla jednoczesnego pobierania** ustaw ograniczenie liczby żądań pobrania pakietu instalacyjnego, wysłanych do Serwera administracyjnego. Ograniczenie liczby żądań pomoże w ograniczeniu przeciążenia sieci.

5. W polu **Maksymalna liczba prób instalacji** ustaw ograniczenie liczby prób zainstalowania aplikacji. Jeśli instalacja Kaspersky Endpoint Security zakończy się błędem, zadanie automatycznie uruchomi ponownie instalację.

6. Jeśli to konieczne, odznacz pole wyboru **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana**. Umożliwi to, na przykład, zainstalowanie jednej z poprzednich wersji aplikacji.

7. Jeśli to konieczne, odznacz pole wyboru **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**. Umożliwia to uniknięcie pobrania pakietu dystrybucyjnego aplikacji, jeśli system operacyjny komputera nie spełni wymagań oprogramowania. Jeśli jesteś pewien, że system operacyjny komputera spełnia wymagania oprogramowania, możesz pominąć tę weryfikację.

8. Jeśli to konieczne, zaznacz pole wyboru **Przypisz pakiet instalacyjny do zasad grupy Active Directory**. Kaspersky Endpoint Security jest instalowany przy użyciu Agenta sieciowego lub ręcznie przy użyciu Active Directory. Aby zainstalować Agenta sieciowego, zadanie zdalnej instalacji musi być uruchomione z uprawnieniami administratora domeny.

9. Jeśli to konieczne, zaznacz pole wyboru **Poproś użytkowników o zamknięcie uruchomionych aplikacji**. Instalacja Kaspersky Endpoint Security zużywa zasoby komputera. Dla wygody użytkownika Kreator instalacji aplikacji wyświetli pytanie o zamknięcie uruchomionych aplikacji przed instalacją. Umożliwi to uniknięcie przerw w działaniu innych aplikacji i zapobiegnie możliwym problemom z komputerem.

10. W sekcji **Zachowanie urządzeń zarządzanych poprzez inne Serwery administracyjne** wybierz metodę instalacji Kaspersky Endpoint Security. Jeśli w sieci jest zainstalowanych więcej niż jeden Serwer administracyjny, te Serwery administracyjne mogą widzieć te same komputery klienckie. Może to spowodować, na przykład, zdalne zainstalowanie aplikacji na tym samym komputerze kilka razy poprzez różne Serwery administracyjne lub inne konflikty.

Krok 4. Wybieranie konta do uruchomienia zadania

Wybierz konto do zainstalowania Agenta sieciowego przy użyciu narzędzi systemu operacyjnego. W tym przypadku uprawnienia administratora są wymagane do uzyskania dostępu do komputera. Możesz dodać kilka kont. Jeśli konto nie posiada wystarczających uprawnień, Kreator instalacji użyje następnego konta. Jeśli instalujesz Kaspersky Endpoint Security przy użyciu narzędzi Agenta sieciowego, nie musisz wybrać konta.

Krok 5. Kończenie tworzenia zadania

Zakończ działanie kreatora, klikając przycisk **Zakończ**. Nowe zadanie zostanie wyświetlone na liście zadań. Aby uruchomić zadanie, zaznacz pole obok zadania i kliknij przycisk **Uruchom**. Aplikacja zostanie zainstalowana w trybie cichym. Po instalacji, ikona zostanie dodana do obszaru powiadomień komputera użytkownika. Jeśli ikona wygląda w następujący sposób , upewnij się, że aktywowałeś aplikację.

Instalowanie aplikacji lokalnie przy użyciu kreatora

Interfejs Kreatora instalacji aplikacji składa się z szeregu okien odpowiadających krokom instalacji aplikacji. Upewnij się, że konto użytkownika, na którym uruchamiasz Kreatora instalacji, znajduje się w grupie administratorów.

W celu zainstalowania aplikacji lub jej aktualizacji z poprzedniej wersji przy użyciu Kreatora instalacji:

1. Skopiuj folder pakietu dystrybucyjnego na komputer użytkownika.

2. Uruchom setup_kes.exe.

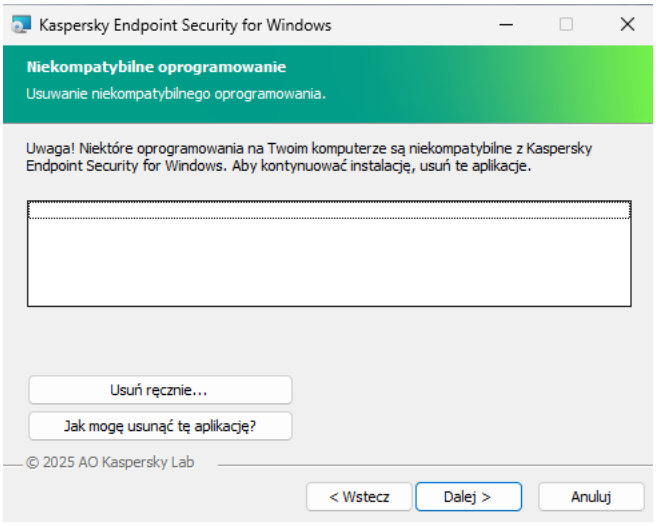
   Zostanie uruchomiony Kreator instalacji.

Przygotowanie do instalacji

Przed zainstalowaniem aplikacji Kaspersky Endpoint Security lub jej aktualizacją z poprzedniej wersji, należy sprawdzić, czy spełnione są następujące wymagania:

- Sprawdzić pod kątem oprogramowania, z którym Kaspersky Endpoint Security może mieć problemy z kompatybilnością (lista oprogramowania jest dostępna w pliku incompatible.txt, który jest zawarty w zestawie dystrybucyjnym).
- Spełnione są wymagania sprzętowe i programowe.
- Czy jest obecny Microsoft .NET Framework.
- Użytkownik ma uprawnienia do zainstalowania produktu.

Jeżeli jakiekolwiek z powyższych wymagań nie jest spełnione, wyświetlony zostanie odpowiedni komunikat. Na przykład powiadomienie o niekompatybilnym oprogramowaniu (patrz rysunek poniżej).



Usuwanie niekompatybilnego oprogramowania

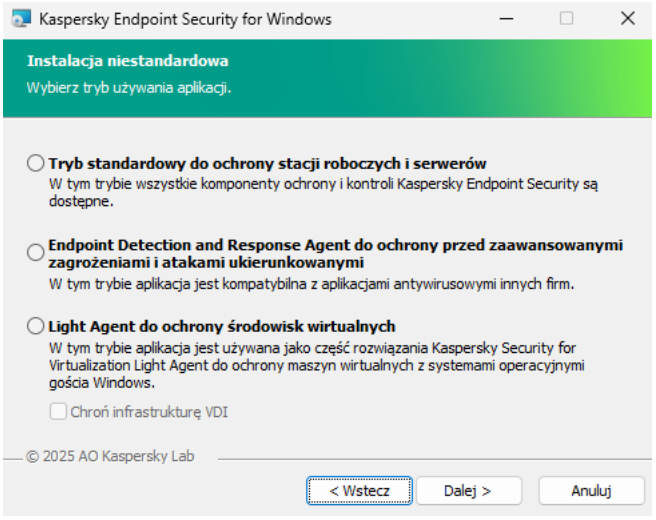
Jeżeli komputer spełnia wymienione wymagania, Kreator instalacji wyszuka aplikacje firmy Kaspersky, które mogą powodować konflikt podczas współdziałania z Kaspersky Endpoint Security. Po odnalezieniu takich programów zasugerowane zostanie ich ręczne usunięcie.

Jeśli wykryte aplikacje obejmują poprzednie wersje Kaspersky Endpoint Security, wszystkie dane, które można przenieść (dane aktywacji i ustawienia aplikacji), zostaną zachowane i użyte podczas instalacji Kaspersky Endpoint Security 14.1 for Windows, a poprzednia wersja aplikacji zostanie automatycznie usunięta. Dotyczy to następujących wersji aplikacji:

- Kaspersky Endpoint Security 12.1 for Windows (wersja 12.1.0.506)
- Kaspersky Endpoint Security 12.2 for Windows (wersja 12.2.0.462)
- Kaspersky Endpoint Security 12.3 for Windows (wersja 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (wersja 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (wersja 12.5.0.539)

- Kaspersky Endpoint Security 12.6 for Windows (wersja 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (wersja 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (wersja 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (wersja 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (wersja 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (wersja 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (wersja 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (wersja 14.0.0.504)

Konfiguracja Kaspersky Endpoint Security



Wybór konfiguracji aplikacji

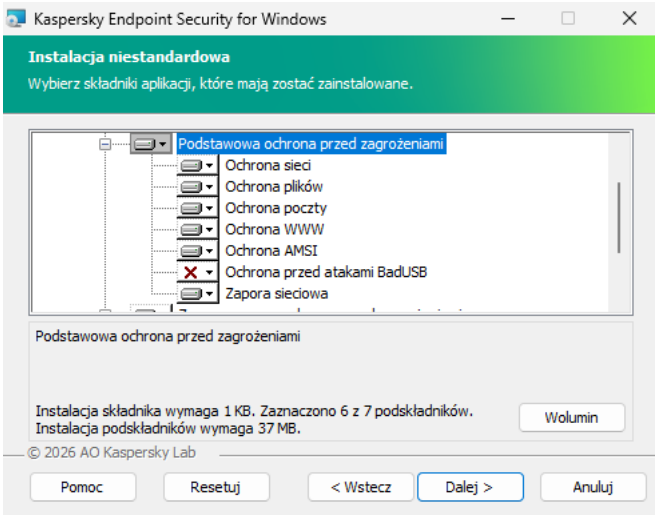
Tryb standardowy. Domyślna konfiguracja. Ta konfiguracja umożliwia korzystanie ze wszystkich komponentów aplikacji, w tym komponentów zapewniających obsługę rozwiązań do Detection and Response. Ta konfiguracja służy do kompleksowej ochrony komputera przed różnymi zagrożeniami, atakami sieciowymi i oszustwami.

Endpoint Detection and Response Agent. W tej konfiguracji można zainstalować wyłącznie komponenty zapewniające obsługę rozwiązań wykrywania i reagowania: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), jak również KUMA. Ta konfiguracja jest wymagana, jeśli w Twojej organizacji wdrożona jest platforma Endpoint Protection Platform (EPP) innej firmy wraz z rozwiązaniem Kaspersky Detection and Response. Dzięki temu Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent jest kompatybilny z aplikacjami EPP innych firm.

Light Agent do ochrony środowisk wirtualnych. Ta konfiguracja jest przeznaczona do aplikacji stanowiącej część rozwiązania Kaspersky Security for Virtualization Light Agent. Klienta Light Agent należy zainstalować na każdej maszynie wirtualnej, która ma być chroniona za pomocą tego rozwiązania. W tej konfiguracji nie można używać komponentów Szyfrowania danych ani Adaptacyjnej kontroli anomalii. Jeśli instalujesz klienta Light Agent na szablonie maszyny wirtualnej, który będzie używany do tworzenia *nietrwałych maszyn wirtualnych*, zaznacz pole **Chroń infrastrukturę VDI** (VDI oznacza Virtual Desktop Infrastructure). Tryb ochrony VDI pomaga zoptymalizować działanie Kaspersky Endpoint Security na nietrwałych maszynach wirtualnych. W tym trybie Light Agent odrzuca aktualizacje aplikacji wymagające ponownego uruchomienia maszyny wirtualnej. Po otrzymaniu aktualizacji aplikacji wymagających ponownego uruchomienia Light Agent generuje zdarzenie informujące o konieczności zaktualizowania szablonu chronionych maszyn wirtualnych.

Komponenty Kaspersky Endpoint Security

Podczas procesu instalacji możesz wybrać komponenty Kaspersky Endpoint Security, które zostaną zainstalowane (patrz rysunek poniżej). Komponent Ochrona plików jest obowiązkowym komponentem, który musi zostać zainstalowany. Nie możesz anulować jego instalacji.



Wybieranie komponentów aplikacji do zainstalowania

Domyślnie, do zainstalowania są wybrane wszystkie składniki aplikacji, za wyjątkiem następujących komponentów:

- Ochrona przed atakami BadUSB.
- Składniki Szyfrowania danych.
- Składniki Detection and Response.

Możesz zmienić dostępne komponenty aplikacji po zainstalowaniu aplikacji. Aby to zrobić, musisz ponownie uruchomić Kreatora instalacji i wybrać zmianę dostępnych składników.

Jeśli musisz zainstalować komponenty Detection and Response, Kaspersky Endpoint Security obsługuje następujące konfiguracje:

- Tylko Endpoint Detection and Response Optimum
- Tylko Endpoint Detection and Response Expert (cloud)
- Tylko Endpoint Detection and Response Expert (on-premises)

- Tylko Network Detection and Response (KATA)
- Tylko Sandbox
- Endpoint Detection and Response Optimum i Sandbox
- Endpoint Detection and Response Expert (cloud) i Sandbox
- Endpoint Detection and Response Expert (on-premises) i Sandbox
- Network Detection and Response (KATA) i Endpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) i Managed Detection and Response

Kaspersky Endpoint Security weryfikuje wybór komponentów przed zainstalowaniem aplikacji. Jeśli wybrana konfiguracja komponentów Detection and Response nie jest obsługiwana, Kaspersky Endpoint Security nie może zostać zainstalowany.

Wybór folderu do zainstalowania aplikacji

Możesz zmienić ścieżkę instalacji Kaspersky Endpoint Security na komputerze klienckim. Domyślnie, aplikacja jest instalowana w folderze `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.1`.

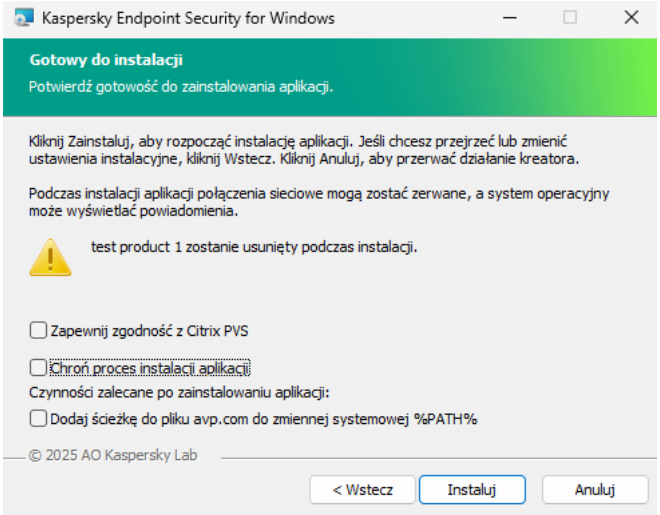
Konfigurowanie strefy zaufanej

Począwszy od Kaspersky Endpoint Security 12.6 for Windows, wykluczenia skanowania I zaufane aplikacje są dodawane do strefy zaufanej. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach.

Począwszy od Kaspersky Endpoint Security 12.8 for Windows można instalować aplikację w trybie Light Agent w celu ochrony środowisk wirtualnych. Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje mogą pomóc w szybkiej konfiguracji Kaspersky Endpoint Security w środowiskach wirtualnych Citrix i VMware.

Możesz również skonfigurować strefę zaufaną później we właściwościach zasad: wykluczenia ze skanowania I zaufane aplikacje.

Ustawienia zaawansowane



Zaawansowane ustawienia instalacji aplikacji

Chroń proces instalacji aplikacji. Ochrona instalacji obejmuje ochronę przed zastąpieniem pakietu dystrybucyjnego szkodliwymi aplikacjami, blokowaniem dostępu do folderu instalacyjnego Kaspersky Endpoint Security, a także blokowaniem dostępu do sekcji rejestru systemu zawierającego klucze aplikacji. Jeżeli aplikacja nie może zostać zainstalowana (na przykład podczas zdalnej instalacji przy użyciu Windows Remote Desktop), zalecane jest wyłączenie ochrony procesu instalacji.

Zapewnij zgodność z Citrix PVS. Możesz włączyć obsługę Citrix Provisioning Services, aby zainstalować Kaspersky Endpoint Security na maszynie wirtualnej.

Dodaj ścieżkę do pliku avp.com do zmiennej systemowej %PATH%. Możesz dodać ścieżkę instalacji do zmiennej %PATH% dla wygodnego korzystania z interfejsu wiersza poleceń.

Zdalne instalowanie aplikacji przy użyciu System Center Configuration Manager

Te instrukcje dotyczą System Center Configuration Manager 2012 R2.

W celu zdalnego zainstalowania aplikacji przy użyciu System Center Configuration Manager:

1. Otwórz konsolę Configuration Manager.
2. W prawej części okna, w sekcji **App management** wybierz **Packages**.
3. W górnej części konsoli, w panelu sterowania, kliknij przycisk **Create package**.

   Zostanie uruchomiony *kreator nowych pakietów i aplikacji*.

4. W kreatorze nowych pakietów i aplikacji:

   a. W sekcji **Package**:

   - W polu **Name** wprowadź nazwę pakietu instalacyjnego.
   - W polu **Source folder** określ ścieżkę dostępu do folderu zawierającego pakiet dystrybucyjny Kaspersky Endpoint Security.

   b. W sekcji **Application type** wybierz opcję **Standard program**.

   c. W sekcji **Standard program**:

   - W polu **Name** wprowadź unikatową nazwę pakietu instalacyjnego (na przykład, nazwę aplikacji i jej wersję).
   - W polu **Command line** określ opcje instalacji Kaspersky Endpoint Security z poziomu wiersza poleceń.
   - Kliknij przycisk **Browse**, aby wskazać ścieżkę dostępu do pliku wykonywalnego aplikacji.
   - Upewnij się, że na liście **Run mode** wybrano element **Run with administrative rights**.

   d. W sekcji **Requirements**:

   - Zaznacz pole **Run another program first**, jeśli przez zainstalowaniem Kaspersky Endpoint Security chcesz uruchomić inna aplikację.

     Wybierz aplikację z listy rozwijalnej **Application** lub określ ścieżkę do pliku wykonywalnego tej aplikacji, klikając przycisk **Browse**.

   - W sekcji **Platform requirements** zaznacz opcję **This program can run only on specified platforms**, jeśli chcesz, aby aplikacja była instalowana tylko w określonych systemach operacyjnych.

     Na poniższej liście zaznacz obok systemów operacyjnych, w których zostanie zainstalowany Kaspersky Endpoint Security.

   Ten krok jest opcjonalny.

   e. W sekcji **Summary** sprawdź wszystkie sprowadzone wartości ustawień i kliknij **Next**.

   Utworzony pakiet instalacyjny pojawi się w sekcji **Packages**, na liście dostępnych pakietów instalacyjnych.

5. Z otwartego menu kontekstowego pakietu instalacyjnego wybierz **Deploy**.

   Zostanie uruchomiony kreator *Deployment Wizard*.

6. W kreatorze Deployment Wizard:

   a. W sekcji **General**:

   - W polu **Software** wprowadź unikatową nazwę pakietu instalacyjnego lub wybierz pakiet instalacyjny z listy, klikając przycisk **Browse**.
   - W polu **Collection** wprowadź nazwę zbioru komputerów, na których aplikacja zostanie zainstalowana, lub wybierz zbiór, klikając przycisk **Browse**.

   b. W sekcji **Contains** dodaj punkty dystrybucji (więcej informacji można znaleźć w dokumentacji dla System Center Configuration Manager).

c. Jeśli to konieczne, określ wartości innych ustawień w kreatorze Deployment Wizard. Te ustawienia są opcjonalne dla zdalnej instalacji Kaspersky Endpoint Security.

d. W sekcji **Summary** sprawdź wszystkie sprowadzone wartości ustawień i kliknij **Next**.

Po zakończeniu pracy kreatora Deployment Wizard, zostanie utworzone zadanie dla zdalnej instalacji Kaspersky Endpoint Security.

Opis ustawień instalacji pliku setup.ini

Plik setup.ini jest używany przy instalacji aplikacji z poziomu wiersza poleceń lub za pomocą Edytora zasad grupy systemu Microsoft Windows. Aby zastosować ustawienia z pliku setup.ini, umieść ten plik w folderze zawierającym pakiet dystrybucyjny Kaspersky Endpoint Security.

Pliku setup.ini należy używać wyłącznie w przypadku instalowania aplikacji w trybie cichym.

Nie można dodać ścieżki do pliku konfiguracyjnego install.cfg w pliku setup.ini. Aplikacja pomija również plik konfiguracyjny install.cfg, jeśli znajduje się w folderze zawierającym pakiet dystrybucyjny Kaspersky Endpoint Security. Aby zastosować ustawienia z pliku konfiguracyjnego install.cfg, musisz określić ścieżkę do pliku w następującym poleceniu instalacji aplikacji: `CONFIGPATH=<path to the configuration file>`.

POBIERZ PLIK SETUP.INI

Plik setup.ini zawiera następujące sekcje:

- `[Setup]` – ustawienia ogólne instalacji aplikacji.
- `[Components]` – wybór komponentów aplikacji przeznaczonych do zainstalowania w trybie Standard. Jeżeli nie określono żadnego składnika, zostaną zainstalowane wszystkie składniki dostępne dla systemu operacyjnego. Ochrona plików jest obowiązkowym komponentem i jest instalowana na komputerze bez względu na ustawienia wskazane w tej sekcji.
- `[Tasks]` – wybór zadań, które mają zostać włączone do listy zadań Kaspersky Endpoint Security. Jeżeli nie określono żadnego zadania, wszystkie zadania zostają włączone do listy zadań Kaspersky Endpoint Security.

Zamiast wartości `1` możesz użyć wartości `yes`, `on`, `enable`, `enabled`, and `true`. Zamiast wartości `0` możesz użyć wartości `no`, `off`, `disable`, `disabled`, and `false`.

Ustawienia pliku setup.ini

Sekcja	Parametr	Opis
`[Setup]`	`InstallDir`	Ścieżka do folderu instalacyjnego aplikacji.
	`ActivationCode`	Kod aktywacyjny Kaspersky Endpoint Security.

Sekcja	Parametr	Opis
	`Eula`	Akceptacja lub odrzucenie warunków Umowy licencyjnej. Umowa licencyjna jest zawarta w pakiecie dystrybucyjnym Kaspersky Endpoint Security. Akceptacja warunków Umowy licencyjnej jest niezbędna do zainstalowania aplikacji lub jej aktualizacji.
	`PrivacyPolicy`	Akceptacja Polityki prywatności. Treść Polityki prywatności znajduje się w pakiecie dystrybucyjnym Kaspersky Endpoint Security. Aby zainstalować aplikację lub zaktualizować wersję aplikacji, musisz zaakceptować Politykę prywatności.
	`KSN`	Akceptacja lub odmowa uczestnictwa w Kaspersky Security Network (KSN). Jeśli nie ustawiono wartości dla tego parametru, Kaspersky Endpoint Security wyświetli monit o potwierdzenie zgody lub odmowę uczestniczenia w KSN przy pierwszym uruchomieniu Kaspersky Endpoint Security. Dostępne wartości: • `1` – zgoda na uczestniczenie w KSN. • `0` – odmowa uczestniczenia w KSN (wartość domyślna). Pakiet dystrybucyjny Kaspersky Endpoint Security jest zoptymalizowany do użycia z Kaspersky Security Network. Jeśli zdecydowałeś się nie uczestniczyć w Kaspersky Security Network, powinieneś zaktualizować Kaspersky Endpoint Security od razu po zakończeniu instalacji.
	`CLEANERSIGNCHECK`	Weryfikacja podpisów cyfrowych plików wykrytego oprogramowania z listy incompatible.txt. Aby usunąć oprogramowanie, Kaspersky Endpoint Security uruchamia plik instalatora oprogramowania. Jeśli w pliku instalatora nie ma podpisu cyfrowego, Kaspersky Endpoint Security uznaje plik za niezaufany i wstrzymuje usuwanie oprogramowania, aby uniknąć uruchomienia potencjalnie szkodliwego kodu. Jeśli aplikacja nie może zweryfikować podpisu cyfrowego pliku wykrytego oprogramowania, instalacja Kaspersky Endpoint Security zostanie zatrzymana z błędem. Wartość domyślna różni się w zależności od metody instalacji oprogramowania: • `0` oznacza, że weryfikacja podpisu cyfrowego jest wyłączona (wartość domyślna, jeśli została wdrożona za pośrednictwem Kaspersky Security Center). • `1` oznacza, że weryfikacja podpisu cyfrowego jest włączona (wartość domyślna, jeśli aplikacja jest instalowana lokalnie).
	`Login`	Ustaw nazwę użytkownika, aby uzyskać dostęp do funkcji i ustawień Kaspersky Endpoint Security (komponent Ochrona hasłem). Nazwa użytkownika jest ustawiana wraz z parametrami `Password` i `PasswordArea`. Nazwa użytkownika KLAdmin jest używana domyślnie.
	`Password`	Określ hasło dostępu do funkcji i ustawień Kaspersky Endpoint Security (hasło jest określane wraz z parametrami `Login` i `PasswordArea`). Jeśli określiłeś hasło, ale nie określiłeś nazwy użytkownika z parametrem `Login`, domyślnie używana będzie nazwa użytkownika KLAdmin.
	`PasswordArea`	Zakres działania hasła dostępu do funkcji i ustawień Kaspersky Endpoint Security. Jeśli użytkownik spróbuje wykonać działanie, które znajduje się w tym obszarze, Kaspersky Endpoint Security wyświetli monit o podanie danych uwierzytelniających konta użytkownika (parametry `Login` i `Password`). Użyj znaku `;`, aby określić kilka wartości. Dostępne wartości: • `SET` – modyfikowanie ustawień aplikacji. • `EXIT` – zakończenie działania aplikacji. • `DISPROTECT` – wyłączanie komponentów ochrony i zatrzymywanie zadań skanowania. • `DISPOLICY` – wyłączanie zasady Kaspersky Security Center. • `UNINST` – usunięcie aplikacji z komputera. • `DISCTRL` – wyłączenie składników kontroli. • `REMOVELIC` – usuwanie klucza. • `REPORTS` – wyświetlanie raportów. • `EXPORT` – eksportowanie ustawień aplikacji. Na przykład, `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.

Sekcja	Parametr	Opis
	`SelfProtection`	Włączenie lub wyłączenie mechanizmu ochrony instalacji aplikacji. Dostępne wartości: • `1` – mechanizm ochrony instalacji aplikacji jest włączony (domyślna wartość). • `0` – mechanizm ochrony instalacji aplikacji jest wyłączony. Ochrona instalacji obejmuje ochronę przed zastąpieniem pakietu dystrybucyjnego szkodliwymi aplikacjami, blokowaniem dostępu do folderu instalacyjnego Kaspersky Endpoint Security, a także blokowaniem dostępu do sekcji rejestru systemu zawierającego klucze aplikacji. Jeżeli aplikacja nie może zostać zainstalowana (na przykład podczas zdalnej instalacji przy użyciu Windows Remote Desktop), zalecane jest wyłączenie ochrony procesu instalacji.
	`PROTECTOSSERVICES`	Ochrona funkcjonalności usług systemu operacyjnego. Ochrona usług systemu operacyjnego zapobiega zakłócaniu ich działania przez aplikacje innych firm. Do takich usług zalicza się na przykład usługę automatycznego uruchamiania aplikacji. • `1` oznacza, że ochrona usług systemu operacyjnego jest włączona (wartość domyślna). • `0` oznacza, że ochrona usług systemu operacyjnego jest wyłączona.
	`EnableAzureSupport`	Włączanie lub wyłączanie trybu zgodności Azure WVD. Dostępne wartości: • `1` – Tryb zgodności Azure WVD jest włączony. • `0` – Tryb zgodności Azure WVD jest wyłączony (wartość domyślna). Ta funkcja zapewnia prawidłowe wyświetlanie stanu maszyny wirtualnej Azure w konsoli Kaspersky Anti Targeted Attack Platform. Aby monitorować wydajność komputera, Kaspersky Endpoint Security wysyła dane telemetryczne do serwerów KATA. Dane telemetryczne obejmują identyfikator komputera (Sensor ID). Tryb zgodności Azure WVD umożliwia przypisanie do tych maszyn wirtualnych trwałego unikatowego identyfikatora Sensor ID. Jeśli tryb zgodności jest wyłączony, Sensor ID może ulec zmianie po ponownym uruchomieniu komputera ze względu na sposób działania maszyn wirtualnych platformy Azure. Może to spowodować pojawienie się duplikatów maszyn wirtualnych w konsoli.
	`Reboot`	Automatyczne ponowne uruchamianie komputera, jeśli jest wymagane po zainstalowaniu lub zaktualizowaniu aplikacji. Jeśli dla tego parametru nie zostanie ustawiona żadna wartość, automatyczne ponowne uruchomienie komputera zostanie zablokowane. Ponowne uruchomienie nie jest wymagane podczas instalowania Kaspersky Endpoint Security. Ponowne uruchomienie jest wymagane tylko wtedy, gdy przed instalacją musisz usunąć niekompatybilne aplikacje. Ponowne uruchomienie może być też wymagane podczas aktualizowania wersji aplikacji.
	`AddEnvironment`	W zmiennej systemowej %PATH% dodaje ścieżkę dostępu do plików wykonywalnych znajdujących się w folderze instalacyjnym Kaspersky Endpoint Security. Dostępne wartości: • `1` – do zmiennej %PATH% zostaje dodana ścieżka dostępu do plików wykonywalnych znajdujących się w folderze instalacyjnym Kaspersky Endpoint Security. • `0` – do zmiennej %PATH% nie zostaje dodana ścieżka dostępu do plików wykonywalnych znajdujących się w folderze instalacyjnym Kaspersky Endpoint Security.
	`AMPPL`	Włącza lub wyłącza ochronę procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL (Antimalware Protected Process Light). Więcej informacji na temat technologii AM-PPL znajdziesz na stronie internetowej firmy Microsoft. Technologia AM-PPL jest dostępna dla systemu Windows 10 w wersji 1703 (RS2) lub nowszej oraz systemów operacyjnych Windows Server 2019. Dostępne wartości: • `1` – ochrona procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL jest włączona. • `0` – ochrona procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL jest wyłączona.

Sekcja	Parametr	Opis
	UPGRADEMODE	Tryb aktualizacji aplikacji: • Seamless oznacza aktualizację aplikacji z ponownym uruchomieniem komputera (wartość domyślna). • Force oznacza aktualizację aplikacji bez konieczności ponownego uruchomienia. Począwszy od wersji 11.10.0 możesz aktualizować aplikację bez konieczności ponownego uruchamiania. Aby zaktualizować wcześniejszą wersję aplikacji, musisz ponownie uruchomić komputer. Począwszy od wersji 11.11.0 możesz aktualizować aplikację bez konieczności ponownego uruchamiania. Ponowne uruchomienie nie jest wymagane podczas instalowania Kaspersky Endpoint Security. Tak więc tryb aktualizacji aplikacji zostanie określony w ustawieniach aplikacji. Parametr ten możesz zmienić w ustawieniach aplikacji lub w zasadach. Podczas aktualizacji już zainstalowanej aplikacji priorytet parametru określonego w pliku setup.ini wyższy niż parametru określonego w ustawieniach aplikacji lub w wierszu poleceń. Na przykład, jeśli w pliku setup.ini zostanie określony tryb aktualizacji Force, a w ustawieniach aplikacji zostanie określony tryb Seamless, aktualizacja zostanie zainstalowana bez ponownego uruchomienia (Force). Jeśli używasz pliku setup.ini, w którym nie określono parametru UPGRADEMODE, instalator użyje wartości domyślnej (Seamless) i zainstaluje aktualizację po ponownym uruchomieniu komputera.
	SetupReg	Włącza zapisywanie kluczy rejestru z pliku setup.reg do rejestru. Wartość parametru SetupReg: setup.reg.
	EnableTraces	Włączanie lub wyłączanie śledzenia aplikacji. Po uruchomieniu program Kaspersky Endpoint Security zapisuje pliki śledzenia w folderze %ProgramData%\Kaspersky Lab\KES.14.1\Traces. Dostępne wartości: • 1 – śledzenie jest włączone. • 0 – śledzenie jest wyłączone (wartość domyślna).
	TracesLevel	Poziom szczegółowości śledzenia. Dostępne wartości: • 100 (krytyczny). Tylko wiadomości dotyczące błędów krytycznych. • 200 (wysoki). Wiadomości o wszystkich błędach, w tym błędach krytycznych. • 300 (diagnostyczny). Wiadomości o wszystkich błędach, a także ostrzeżenia. • 400 (ważny). Wszystkie wiadomości o błędach, ostrzeżenia i dodatkowe informacje. • 500 (normalny). Wiadomości o wszystkich błędach i ostrzeżeniach, a także szczegółowe informacje o działaniu aplikacji w trybie normalnym (domyślnie). • 600 (niski). Wszystkie wiadomości.
	RESTAPI	Zarządzanie aplikacją za pośrednictwem interfejsu API REST. Aby zarządzać aplikacją za pośrednictwem interfejsu API REST, należy podać nazwę użytkownika (parametr RESTAPI_User). Dostępne wartości: • 1 – zarządzanie za pośrednictwem interfejsu API REST jest dozwolone. • 0 – zarządzanie za pośrednictwem interfejsu API REST jest zablokowane (wartość domyślna). Aby zarządzać aplikacją za pośrednictwem interfejsu API REST, zarządzanie przy użyciu systemów administracyjnych musi być dozwolone. W tym celu ustaw parametr AdminKitConnector=1. Jeśli zarządzasz aplikacją za pośrednictwem interfejsu API REST, zarządzanie aplikacją przy użyciu systemów administracyjnych firmy Kaspersky jest niemożliwe.
	RESTAPI_User	Nazwa użytkownika konta domeny Windows używanego do zarządzania aplikacją za pośrednictwem interfejsu API REST. Zarządzanie aplikacją za pośrednictwem interfejsu API REST jest dostępne tylko dla tego użytkownika. Wpisz nazwę użytkownika w formacie <DOMAIN>\<UserName> (na przykład: RESTAPI_User=COMPANY\Administrator). Możesz wybrać tylko jednego użytkownika do pracy z interfejsem API REST. Dodanie nazwy użytkownika jest wymaganiem wstępnym zarządzania aplikacją za pośrednictwem interfejsu API REST.
	RESTAPI_Port	Port używany do zarządzania aplikacją za pośrednictwem interfejsu API REST. Domyślnie używany jest port 6782. Upewnij się, że port jest wolny.
	RESTAPI_Certificate	Certyfikat do identyfikowania żądań (na przykład, RESTAPI_Certificate=C:\cert.pem). Bezpieczna interakcja Kaspersky Endpoint Security z klientem REST wymaga skonfigurowania identyfikacji żądania. W tym celu należy zainstalować certyfikat i podpisać ładunek każdego żądania.

Sekcja	Parametr	Opis
	`StandaloneMode`	Instalowanie aplikacji w trybie Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* to aplikacja instalowana na poszczególnych stacjach roboczych i serwerach w infrastrukturze informatycznej organizacji w celu obsługi rozwiązań: Kaspersky Managed Detection and Response i Kaspersky Anti Targeted Attack Platform. EDR Agent jest kompatybilny z aplikacjami EPP innych firm. Dzięki temu możesz korzystać z zabezpieczeń infrastruktury innych firm wraz z funkcją Detection and Response firmy Kaspersky. Aby zainstalować EDR Agent, w sekcji `[Components]`, wybierz komponenty `StandaloneKATA`, `StandaloneNDR` lub `StandaloneMDR`. EDR Agent nie obsługuje innych komponentów aplikacji. Dostępne wartości: • `1` do instalacji aplikacji w trybie EDR Agent. • `0` do instalacji aplikacji w trybie Standardowym (domyślnym).
	`KSVLAMode`	Instalowanie aplikacji w trybie Light Agent. Ta konfiguracja jest przeznaczona do aplikacji stanowiącej część rozwiązania Kaspersky Security for Virtualization Light Agent. Klienta Light Agent należy zainstalować na każdej maszynie wirtualnej, która ma być chroniona za pomocą tego rozwiązania. Dostępne wartości: • `1` do instalacji aplikacji w trybie Light Agent. • `0` do instalacji aplikacji w trybie Standardowym (domyślnym).
	`InstallOnVDI`	Włączanie trybu ochrony VDI podczas instalowania aplikacji w trybie Light Agent (`KSVLAMode=1`). Tryb ochrony VDI pomaga zoptymalizować działanie Kaspersky Endpoint Security na nietrwałych maszynach wirtualnych. W tym trybie Light Agent odrzuca aktualizacje aplikacji wymagające ponownego uruchomienia maszyny wirtualnej. Po otrzymaniu aktualizacji aplikacji wymagających ponownego uruchomienia Light Agent generuje zdarzenie informujące o konieczności zaktualizowania szablonu chronionych maszyn wirtualnych. Dostępne wartości: • `1` do włączenia trybu ochrony VDI. • `0` do wyłączenia trybu ochrony VDI (domyślnie).
	`KESExclusions`	Dodawanie wstępnie zdefiniowanych wykluczenia ze skanowania i zaufanych aplikacji podczas instalowania aplikacji na serwerze. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Na przykład predefiniowane wykluczenia skanowania dla serwerów SQL obejmują pliki baz danych MDF i LDF. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach. Dostępne wartości: • `1` włącza predefiniowane wykluczenia ze skanowania i zaufane aplikacje. • `0` wyłącza predefiniowane wykluczenia ze skanowania i zaufane aplikacje (domyślnie).
	`LAExclusions`	Dodawanie wstępnie zdefiniowanych wykluczenia ze skanowania i zaufanych aplikacji podczas instalowania aplikacji na maszynie wirtualnej (tryb Light Agent). Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje mogą pomóc w szybkiej konfiguracji Kaspersky Endpoint Security w środowiskach wirtualnych Citrix i VMware. Dostępne wartości: • `1` włącza predefiniowane wykluczenia ze skanowania i zaufane aplikacje. • `0` wyłącza predefiniowane wykluczenia ze skanowania i zaufane aplikacje (domyślnie).
	`EnableUniqueSensorID`	Tworzenie unikalnego identyfikatora komputera (Sensor ID) podczas instalacji lub aktualizacji aplikacji. Identyfikator Sensor ID jest wykorzystywana w rozwiązaniu Kaspersky Anti Targeted Attack Platform do identyfikowania komputerów wysyłających dane telemetryczne na serwer. Podczas tworzenia Sensor ID aplikacja wykorzystuje algorytm uwzględniający konfigurację komputera, np. numer seryjny płyty głównej. W niektórych przypadkach, na przykład podczas korzystania z aplikacji w środowisku wirtualnym, identyfikator Sensor ID może być zduplikowany. W rezultacie Kaspersky Anti Targeted Attack Platform nie może zidentyfikować komputera, z którego wysłano dane telemetryczne. Aby utworzyć unikalny Sensor ID, należy ustawić parametr `EnableUniqueSensorID=1`. W rezultacie aplikacja użyje innego algorytmu do utworzenia Sensor ID, który bierze pod uwagę również inne dane dotyczące komputera. Dzięki temu identyfikator Sensor ID jest unikalny. Domyślnie parametr nie jest ustawiony. Aplikacja dziedziczy Sensor ID w następujących przypadkach: • Aktualizacja wersji aplikacji • migracja konfiguracji [KES+KEA] do konfiguracji [KES+wbudowany agent] Instalator próbuje odziedziczyć identyfikator <1> w ramach jej naprawy.Sensor ID. Jeśli identyfikatora Sensor ID nie można przywrócić, aplikacja utworzy nowy identyfikator Sensor ID.

Sekcja	Parametr	Opis
	`CitrixCompatibility`	Włączanie obsługi Citrix Provisioning Services, aby zainstalować Kaspersky Endpoint Security na maszynie wirtualnej.
`[Components]`	`ALL`	Instalacja wszystkich komponentów. Jeśli dla parametru określono wartość `1`, zostaną zainstalowane wszystkie komponenty, niezależnie od ustawień instalacji pojedynczych składników. Ze względu na sposób obsługi rozwiązań Detection and Response komponenty Endpoint Detection and Response Optimum oraz Sandbox są instalowane na komputerze. Komponent Endpoint Detection and Response Expert (cloud) nie jest kompatybilny z tą konfiguracją.
	`MailThreatProtection`	Ochrona poczty.
	`WebThreatProtection`	Ochrona WWW.
	`AMSI`	Ochrona AMSI.
	`HostIntrusionPrevention`	Ochrona przed włamaniami.
	`BehaviorDetection`	Wykrywanie zachowań.
	`ExploitPrevention`	Ochrona przed exploitami.
	`RemediationEngine`	Silnik korygujący.
	`Firewall`	Zapora sieciowa.
	`NetworkThreatProtection`	Ochrona sieci.
	`WebControl`	Kontrola sieci.
	`DeviceControl`	Kontrola urządzeń.
	`ApplicationControl`	Kontrola aplikacji.
	`AdaptiveAnomaliesControl`	Adaptacyjna kontrola anomalii.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Kontrola dziennika
	`AntiCryptor`	Anti-Cryptor
	`FileThreatProtection`	Ochrona plików.
	`SystemIntegrityMonitor`	Monitor integralności systemu.
	`FileEncryption`	Biblioteki Szyfrowania na poziomie plików.
	`DiskEncryption`	Biblioteki Szyfrowania całego dysku.
	`MSBitLocker`	Biblioteki zarządzania szyfrowaniem BitLocker.
	`BadUSBAttackPrevention`	Ochrona przed atakami BadUSB.
	`EDR`	Endpoint Detection and Response Optimum Ten komponent nie jest kompatybilny z komponentem Endpoint Detection and Response Expert (cloud) (`EDRCloud`) ani Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) Ten komponent nie jest kompatybilny z komponentem Endpoint Detection and Response Optimum (`EDR`) ani Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).

Sekcja	Parametr	Opis
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) Ten komponent nie jest kompatybilny z komponentem Endpoint Detection and Response Expert (cloud) (`EDRCloud`) ani Endpoint Detection and Response Optimum (`EDR`).
	`SB`	Kaspersky Sandbox lub KATA Sandbox. *Kaspersky Sandbox* jest samodzielnym rozwiązaniem typu Detection and Response firmy Kaspersky. *KATA Sandbox* jest komponentem rozwiązania Kaspersky Anti Targeted Attack Platform.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) Ten komponent nie jest kompatybilny z komponentem Endpoint Detection and Response Expert (cloud) (`EDRCloud`) ani Endpoint Detection and Response Optimum (`EDR`).
	`AdminKitConnector`	Zarządzanie aplikacjami za pomocą systemów administracyjnych. Systemy administracyjne obejmują, na przykład, Kaspersky Security Center. Oprócz systemów administracyjnych Kaspersky możesz korzystać z rozwiązań innych firm. Kaspersky Endpoint Security oferuje w tym celu interfejs API. Dostępne wartości: • `1` – dozwolone jest zarządzanie aplikacjami za pomocą systemów administracyjnych (wartość domyślna). • `0` – zarządzanie aplikacjami jest dozwolone tylko przez interfejs lokalny.
	`KUMAIntegration`	Integracja z KUMA.
	`StandaloneKATA`	Instalacja aplikacji w trybie Endpoint Detection and Response Agent (EDR Agent) do integracji z platformą Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Instalacja aplikacji w trybie Endpoint Detection and Response Agent (EDR Agent) do integracji z Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Instalacja aplikacji w trybie Endpoint Detection and Response Agent (EDR Agent) do integracji z platformą Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Instalacja aplikacji w trybie Endpoint Detection and Response Agent (EDR Agent) do integracji z KUMA.
`[Tasks]`	`ScanMyComputer`	Zadanie Pełnego skanowania. Dostępne wartości: • `1` – zadanie zostaje włączone do listy zadań Kaspersky Endpoint Security. • `0` – zadanie nie zostaje włączone do listy zadań Kaspersky Endpoint Security.
	`ScanCritical`	Zadanie Skanowanie obszarów krytycznych. Dostępne wartości: • `1` – zadanie zostaje włączone do listy zadań Kaspersky Endpoint Security. • `0` – zadanie nie zostaje włączone do listy zadań Kaspersky Endpoint Security.
	`Updater`	Zadanie aktualizacji. Dostępne wartości: • `1` – zadanie zostaje włączone do listy zadań Kaspersky Endpoint Security. • `0` – zadanie nie zostaje włączone do listy zadań Kaspersky Endpoint Security.

Zmiana składników aplikacji

Podczas instalacji aplikacji możesz wybrać komponenty, które będą dostępne. Dostępne komponenty aplikacji można zmienić na następujące sposoby:

- Lokalnie, za pomocą Kreatora instalacji.

Komponenty aplikacji są zmieniane przy użyciu normalnej metody dla systemu operacyjnego Windows, czyli za pomocą Panelu sterowania. Uruchom Kreatora instalacji aplikacji i wybierz opcję zmiany dostępnych składników aplikacji. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Ta metoda nie jest dostępna, jeśli aplikacja została zainstalowana za pośrednictwem Kaspersky Security Center. Dopiero później możesz zmienić wybór komponentów aplikacji w Panelu sterowania, po zainstalowaniu aplikacji lokalnie.

- Zdalnie, przy użyciu Kaspersky Security Center.

  Zadanie *Zmiana składników aplikacji* umożliwia zmianę składników Kaspersky Endpoint Security po zainstalowaniu aplikacji.

Zmieniając komponenty aplikacji, należy mieć na uwadze następujące kwestie:

- Na komputerach z systemem Windows Server nie można zainstalować wszystkich składników Kaspersky Endpoint Security (na przykład składnik Adaptacyjna kontrola anomalii nie jest dostępny).
- Jeśli dyski twarde w Twoim komputerze są chronione przez Szyfrowanie całego dysku (FDE), nie możesz usunąć komponentu Szyfrowanie całego dysku. Aby usunąć składnik Szyfrowanie całego dysku, odszyfruj wszystkie dyski twarde komputera.
- Jeśli na komputerze znajdują się zaszyfrowane pliki (FLE) lub użytkownik korzysta z zaszyfrowanych dysków wymiennych (FDE lub FLE), dostęp do plików i dysków wymiennych po usunięciu komponentów Szyfrowanie danych będzie niemożliwy. Dostęp do plików i dysków wymiennych można uzyskać poprzez ponowne zainstalowanie komponentów Szyfrowanie danych.
- Jeśli aplikacja jest zainstalowany w trybie Light Agent w infrastrukturze VDI, nie można zmienić komponentów zestawu.

Jak dodawać lub usuwać komponenty aplikacji w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Wybierz składniki do zainstalowania**.

Krok 2. Ustawienia zadania zmiany składników aplikacji

Wybierz konfigurację aplikacji:

- **Standardowy tryb ochrony hostów**. Domyślna konfiguracja. Ta konfiguracja umożliwia korzystanie ze wszystkich komponentów aplikacji, w tym komponentów zapewniających obsługę rozwiązań do Detection and Response. Ta konfiguracja służy do kompleksowej ochrony komputera przed różnymi zagrożeniami, atakami sieciowymi i oszustwami.

- **Endpoint Detection and Response Agent do ochrony przed zaawansowanymi zagrożeniami i atakami ukierunkowanymi**. W tej konfiguracji można zainstalować wyłącznie komponenty zapewniające obsługę rozwiązań wykrywania i reagowania: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), jak również KUMA. Ta konfiguracja jest wymagana, jeśli w Twojej organizacji wdrożona jest platforma Endpoint Protection Platform (EPP) innej firmy wraz z rozwiązaniem Kaspersky Detection and Response. Dzięki temu Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent jest kompatybilny z aplikacjami EPP innych firm.

  Podczas zmiany konfiguracji aplikacji w celu umożliwienia agentowi EDR współpracy z MDR należy upewnić się, że włączone są komponenty odpowiedzialne za odbieranie danych telemetrycznych.

- **Klient Light Agent do ochrony środowisk wirtualnych**. Ta konfiguracja jest przeznaczona do aplikacji stanowiącej część rozwiązania Kaspersky Security for Virtualization Light Agent. Klienta Light Agent należy zainstalować na każdej maszynie wirtualnej, która ma być chroniona za pomocą tego rozwiązania. W tej konfiguracji nie można używać komponentów Szyfrowania danych ani Adaptacyjnej kontroli anomalii. Jeśli instalujesz klienta Light Agent na szablonie maszyny wirtualnej, który będzie używany do tworzenia *nietrwałych maszyn wirtualnych*, zaznacz pole **Chroń infrastrukturę VDI** (VDI oznacza Virtual Desktop Infrastructure). Tryb ochrony VDI pomaga zoptymalizować działanie Kaspersky Endpoint Security na nietrwałych maszynach wirtualnych. W tym trybie Light Agent odrzuca aktualizacje aplikacji wymagające ponownego uruchomienia maszyny wirtualnej. Po otrzymaniu aktualizacji aplikacji wymagających ponownego uruchomienia Light Agent generuje zdarzenie informujące o konieczności zaktualizowania szablonu chronionych maszyn wirtualnych.

Wybierz składniki aplikacji, które będą dostępne na komputerze użytkownika.

Krok 3. Ustawienia zaawansowane

Skonfiguruj ustawienia zaawansowane zadania (patrz tabela poniżej).

Krok 4. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 5. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz uruchamiania zadania, na przykład, ręcznie lub gdy komputer jest w trybie bezczynności.

Krok 6. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład: *Dodaj składnik Kontrola aplikacji*.

Krok 7. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Jak dodawać lub usuwać składniki aplikacji w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.
2. Z listy rozwijalnej **Typ zadania** wybierz **Zmiana składników aplikacji**.
3. W polu **Nazwa zadania** wpisz krótki opis, na przykład, *Dodaj składnik Kontrola aplikacji*.
4. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

Krok 2. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Na przykład, wybierz oddzielną grupę administracyjną lub skompiluj wybór.

Krok 3. Kończenie tworzenia zadania

Zaznacz pole wyboru **Otwórz szczegóły zadania po jego utworzeniu** i zakończ działanie kreatora.

W właściwościach zadania wybierz zakładkę **Ustawienia aplikacji**. Następnie wybierz konfigurację aplikacji:

- **Tryb standardowy do ochrony stacji roboczych i serwerów**. Domyślna konfiguracja. Ta konfiguracja umożliwia korzystanie ze wszystkich komponentów aplikacji, w tym komponentów zapewniających obsługę rozwiązań do Detection and Response. Ta konfiguracja służy do kompleksowej ochrony komputera przed różnymi zagrożeniami, atakami sieciowymi i oszustwami.

- **Endpoint Detection and Response Agent do ochrony przed zaawansowanymi zagrożeniami i atakami ukierunkowanymi**. W tej konfiguracji można zainstalować wyłącznie komponenty zapewniające obsługę rozwiązań wykrywania i reagowania: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), jak również KUMA. Ta konfiguracja jest wymagana, jeśli w Twojej organizacji wdrożona jest platforma Endpoint Protection Platform (EPP) innej firmy wraz z rozwiązaniem Kaspersky Detection and Response. Dzięki temu Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent jest kompatybilny z aplikacjami EPP innych firm.

  Podczas zmiany konfiguracji aplikacji w celu umożliwienia agentowi EDR współpracy z MDR należy upewnić się, że włączone są komponenty odpowiedzialne za odbieranie danych telemetrycznych.

- **Light Agent do ochrony środowisk wirtualnych**. Ta konfiguracja jest przeznaczona do aplikacji stanowiącej część rozwiązania Kaspersky Security for Virtualization Light Agent. Klienta Light Agent należy zainstalować na każdej maszynie wirtualnej, która ma być chroniona za pomocą tego rozwiązania. W tej konfiguracji nie można używać komponentów Szyfrowania danych ani Adaptacyjnej kontroli anomalii. Jeśli instalujesz klienta Light Agent na szablonie maszyny wirtualnej, który będzie używany do tworzenia *nietrwałych maszyn wirtualnych*, zaznacz pole **Chroń infrastrukturę VDI** (VDI oznacza Virtual Desktop Infrastructure). Tryb ochrony VDI pomaga zoptymalizować działanie Kaspersky Endpoint Security na nietrwałych maszynach wirtualnych. W tym trybie Light Agent odrzuca aktualizacje aplikacji wymagające ponownego uruchomienia maszyny wirtualnej. Po otrzymaniu aktualizacji aplikacji wymagających ponownego uruchomienia Light Agent generuje zdarzenie informujące o konieczności zaktualizowania szablonu chronionych maszyn wirtualnych.

Wybierz składniki aplikacji, które będą dostępne na komputerze użytkownika. Skonfiguruj ustawienia zaawansowane zadania (patrz tabela poniżej).

W rezultacie, zestaw składników Kaspersky Endpoint Security na komputerach użytkowników zostanie zmieniony w trybie cichym. Ustawienia dostępnych składników zostaną wyświetlone w lokalnym interfejsie aplikacji. Składniki, które nie znajdują się w aplikacji, są wyłączone, a ustawienia tych komponentów nie są dostępne.

Podczas instalowania, aktualizacji lub odinstalowywania Kaspersky Endpoint Security mogą wystąpić błędy. Aby uzyskać więcej informacji na temat rozwiązywania tych błędów, zapoznaj się z Bazą wiedzy pomocy technicznej.

Parametr	Opis
Ustawienia zadania	**Usuń niekompatybilne aplikacje innych firm**. Domyślnie Kaspersky Endpoint Security sprawdza zainstalowane aplikacje pod kątem zgodności. Lista oprogramowania, które może być przyczyną problemów ze zgodnością, jest dostępna w pliku incompatible.txt. Plik ten znajduje się w pakiecie dystrybucyjnym. Jeśli skanowanie zainstalowanego oprogramowania jest włączone, po wykryciu aplikacji z listy program Kaspersky Endpoint Security zatrzymuje zadanie. Możesz wyłączyć skanowanie zainstalowanego oprogramowania, jeśli dokumentacja dostawcy oprogramowania innej firmy określa jego zgodność z Endpoint Protection Platform (EPP). **Usuń niekompatybilne aplikacje firm trzecich**. Automatyczne usuwanie aplikacji z listy pliku incompatible.txt przed zmianą zestawu komponentów. Jeśli ta funkcjonalność jest włączona, Kaspersky Endpoint Security próbuje usunąć aplikacje, które mogą powodować problemy ze zgodnością, aby móc kontynuować zadanie. **Użyj trybu zgodności Azure WVD**. Ta funkcja zapewnia prawidłowe wyświetlanie stanu maszyny wirtualnej Azure w konsoli Kaspersky Anti Targeted Attack Platform. Aby monitorować wydajność komputera, Kaspersky Endpoint Security wysyła dane telemetryczne do serwerów KATA. Dane telemetryczne obejmują identyfikator komputera (Sensor ID). Tryb zgodności Azure WVD umożliwia przypisanie do tych maszyn wirtualnych trwałego unikatowego identyfikatora Sensor ID. Jeśli tryb zgodności jest wyłączony, Sensor ID może ulec zmianie po ponownym uruchomieniu komputera ze względu na sposób działania maszyn wirtualnych platformy Azure. Może to spowodować pojawienie się duplikatów maszyn wirtualnych w konsoli.
Wykluczenia	Począwszy od Kaspersky Endpoint Security 12.6 for Windows, wykluczenia skanowania I zaufane aplikacje są dodawane do strefy zaufanej. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach. Począwszy od Kaspersky Endpoint Security 12.8 for Windows można instalować aplikację w trybie Light Agent w celu ochrony środowisk wirtualnych. Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje mogą pomóc w szybkiej konfiguracji Kaspersky Endpoint Security w środowiskach wirtualnych Citrix i VMware. Możesz również skonfigurować strefę zaufaną później we właściwościach zasad: wykluczenia ze skanowania I zaufane aplikacje.
Tryb oddzielny / Tryb powiązany	Możesz tworzyć osobne zestawy komponentów dla stacji roboczych i serwerów — **Tryb oddzielny**. Przed wdrożeniem pakietu instalacyjnego instalator wykrywa typ systemu operacyjnego i instaluje tylko te komponenty aplikacji, które zostały wybrane dla tego typu systemu operacyjnego. Dzięki temu możesz używać tego samego pakietu instalacyjnego na stacjach roboczych i serwerach. **Tryb powiązany** oferuje listę często używanych komponentów dla stacji roboczych i serwerów. Dostępność poszczególnych komponentów zależy od typu systemu operacyjnego. Zalecamy utworzenie podczas używania tego trybu osobnego pakietu instalacyjnego dla stacji roboczych i osobnego pakietu instalacyjnego dla serwerów. Wspólną listę komponentów w pakiecie instalacyjnym można skonfigurować tylko w trybie standardowym.
Użyj hasła do modyfikacji zestawu składników aplikacji	Administratorzy zazwyczaj włączają Ochronę hasłem, aby ograniczyć dostęp do Kaspersky Endpoint Security. Oznacza to, że aby zmodyfikować wybór składników aplikacji, należy wprowadzić poświadczenia użytkownika, który ma uprawnienia **Dezinstalacja / modyfikacja / przywracanie aplikacji**. Na przykład możesz użyć konta KLAdmin.
Użyj hasła, aby odinstalować Kaspersky Endpoint Agent i Kaspersky Security for Windows Server	Administratorzy zazwyczaj włączają Ochronę hasłem w ustawieniach tych zadań, aby ograniczyć dostęp do Kaspersky Endpoint Agent (KEA) i Kaspersky Security for Windows Server (KSWS). Oznacza to, że jeśli przeprowadzasz migrację z konfiguracji [KES+KEA] do [KES+wbudowany agent] lub z KSWS do KES, musisz wprowadzić hasło, aby usunąć te aplikacje.

Aktualizowanie poprzedniej wersji aplikacji

Jeśli aktualizujesz poprzednią wersję aplikacji do nowszej wersji, powinieneś wziąć pod uwagę następujące kwestie:

- Lokalizacja nowej wersji Kaspersky Endpoint Security musi być zgodna z lokalizacją zainstalowanej wersji aplikacji. Jeśli lokalizacje aplikacji nie odpowiadają sobie, aktualizacja aplikacji zakończy się błędem.
- Przed rozpoczęciem aktualizacji zalecamy zamknięcie wszystkich aktywnych aplikacji.
- Przed aktualizacją Kaspersky Endpoint Security blokuje funkcjonalność Szyfrowanie całego dysku. Jeśli nie można odblokować Szyfrowania całego dysku, instalacja aktualizacji nie zostanie uruchomiona. Po zaktualizowaniu aplikacji przywrócona zostanie funkcjonalność Szyfrowanie całego dysku.

Kaspersky Endpoint Security obsługuje aktualizacje następujących wersji aplikacji:

- Kaspersky Endpoint Security 12.1 for Windows (wersja 12.1.0.506)
- Kaspersky Endpoint Security 12.2 for Windows (wersja 12.2.0.462)
- Kaspersky Endpoint Security 12.3 for Windows (wersja 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (wersja 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (wersja 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (wersja 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (wersja 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (wersja 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (wersja 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (wersja 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (wersja 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (wersja 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (wersja 14.0.0.504)

Podczas instalowania, aktualizacji lub odinstalowywania Kaspersky Endpoint Security mogą wystąpić błędy. Aby uzyskać więcej informacji na temat rozwiązywania tych błędów, zapoznaj się z Bazą wiedzy pomocy technicznej.

Metody aktualizacji aplikacji

Program Kaspersky Endpoint Security można aktualizować na komputerze na następujące sposoby:

- Przy użyciu usługi aktualizacji Kaspersky (Seamless Update – SMU).
- lokalnie, za pomocą Kreatora instalacji.
- lokalnie, z poziomu wiersza poleceń.
- zdalnie, przy użyciu Kaspersky Security Center.
- zdalnie, za pośrednictwem Edytora zarządzania zasadami grupy Microsoft Windows (więcej informacji można znaleźć na stronie pomocy technicznej firmy Microsoft).
- zdalnie, za pomocą programu System Center Configuration Manager.

Jeśli aplikacja wdrożona w sieci korporacyjnej zawiera zestaw składników innych niż domyślny, aktualizacja aplikacji za pomocą Konsoli administracyjnej (MMC) różni się od aktualizacji aplikacji za pomocą Web Console i Cloud Console. Podczas aktualizacji Kaspersky Endpoint Security należy wziąć pod uwagę następujące kwestie:

- Kaspersky Security Center Web Console lub Kaspersky Security Center Cloud Console.

  Jeśli utworzyłeś pakiet instalacyjny dla nowej wersji aplikacji z domyślnym zestawem składników, wówczas zestaw składników na komputerze użytkownika nie zostanie zmieniony. Aby korzystać z Kaspersky Endpoint Security z domyślnym zestawem składników, należy otworzyć właściwości pakietu instalacyjnego, zmienić zestaw składników, a następnie przywrócić oryginalny zestaw składników i zapisać zmiany.

- Serwer administracyjny Kaspersky Security Center.

  Zestaw komponentów aplikacji po aktualizacji będzie pasował do zestawu komponentów w pakiecie instalacyjnym. Oznacza to, że jeśli nowa wersja aplikacji zawiera domyślny zestaw składników, wówczas, na przykład, funkcja Ochrona przed atakami BadUSB zostanie usunięta z komputera, ponieważ ten składnik jest wykluczony z domyślnego zestawu. Aby kontynuować korzystanie z aplikacji z tym samym zestawem składników co przed aktualizacją, wybierz wymagane składniki w ustawieniach pakietu instalacyjnego.

Aktualizacja aplikacji bez ponownego uruchomienia

Aktualizacja aplikacji bez ponownego uruchomienia zapewnia nieprzerwaną pracę serwera podczas aktualizacji wersji aplikacji.

Aktualizacja aplikacji bez ponownego uruchomienia ma następujące ograniczenia:

- Począwszy od wersji 11.10.0 możesz aktualizować aplikację bez konieczności ponownego uruchamiania. Aby zaktualizować wcześniejszą wersję aplikacji, musisz ponownie uruchomić komputer.

- Począwszy od wersji 11.11.0 można instalować poprawki bez konieczności ponownego uruchamiania. Aby zainstalować poprawki dla wcześniejszych wersji aplikacji, może być wymagane ponowne uruchomienie komputera.

- Aktualizacja aplikacji bez ponownego uruchomienia nie jest dostępna na komputerach z włączonym szyfrowaniem danych (szyfrowanie Kaspersky (FDE), BitLocker, szyfrowanie na poziomie plików (FLE)). Aby zaktualizować aplikację na komputerach z włączonym szyfrowaniem danych, komputer musi zostać uruchomiony ponownie.

- Aplikacji nie można uaktualnić na maszynie wirtualnej bez ponownego uruchomienia. Aby uaktualnić aplikację na maszynie wirtualnej, musisz ponownie uruchomić maszynę wirtualną.

Po uaktualnieniu aplikacji, zainstalowaniu poprawki, zmianie zestawu komponentów aplikacji lub przywróceniu Kaspersky Endpoint Security uruchamia się ponownie w celu rozpoczęcia korzystania z nowej wersji. Ponowne uruchomienie Kaspersky Endpoint Security może potrwać do jednej minuty. W tym czasie poziom ochrony zostanie zredukowany. Po ponownym uruchomieniu aplikacji poziom ochrony komputera zostanie przywrócony.

Jak wybrać tryb aktualizacji aplikacji w Konsoli administracyjnej (MMC)

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne → Interakcja użytkownika**.

5. W boku **Ustawienia aktualizacji aplikacji** wybierz lub odznacz pole wyboru **Zainstaluj aktualizacje aplikacji bez ponownego uruchomienia**, aby skonfigurować tryb aktualizacji aplikacji.

6. Zapisz swoje zmiany.

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Ustawienia ogólne → Ustawienia aplikacji**.

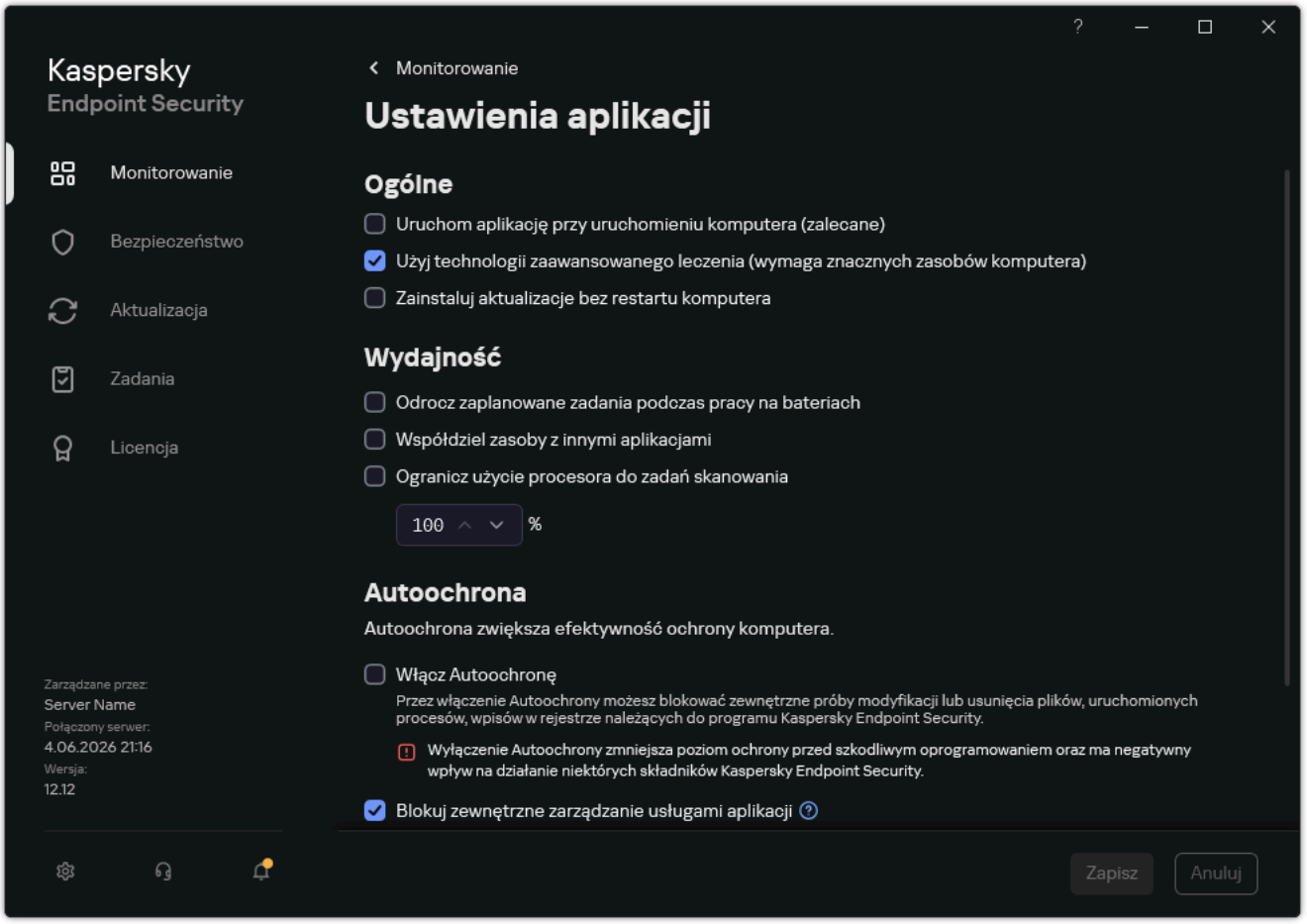
4. W boku **Ustawienia zaawansowane** wybierz lub odznacz pole wyboru **Zainstaluj aktualizacje aplikacji bez ponownego uruchomienia**, aby skonfigurować tryb aktualizacji aplikacji.

5. Zapisz swoje zmiany.

Jak wybrać tryb aktualizacji aplikacji w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne → Ustawienia aplikacji**.



Ustawienia Kaspersky Endpoint Security for Windows

3. W boku **Ogólne** wybierz lub odznacz pole wyboru **Zainstaluj aktualizacje bez restartu komputera**, aby skonfigurować tryb aktualizacji aplikacji.

4. Zapisz swoje zmiany.

Po zakończeniu procedury uaktualniania aplikacji bez ponownego uruchamiania komputera zostanie na nim zainstalowana nowa wersja Kaspersky Endpoint Security. Poprzednia wersja aplikacji zostanie automatycznie usunięta.

Nie można rozpocząć aktualizacji aplikacji, dopóki poprzednia aktualizacja nie zostanie całkowicie zakończona.

Możesz sprawdzić status aktualizacji Kaspersky Endpoint Security, używając raportu wersji aplikacji Kaspersky w konsoli Kaspersky Security Center.

Aktualizacja SMU aplikacji

Aby zaktualizować aplikację przy użyciu usługi aktualizacji Kaspersky (Seamless Update; SMU), nie musisz uruchamiać instalatora, w przeciwieństwie do innych metod aktualizacji. Kaspersky Endpoint Security otrzymuje nową wersję aplikacji wraz z antywirusowymi bazami danych z tego samego źródła.

Aktualizacja SMU umożliwia zaktualizowanie aplikacji na wszystkich komputerach w Twojej organizacji do najnowszej wersji. Przed zastosowaniem aktualizacji SMU zalecamy przetestowanie nowej wersji aplikacji na kilku komputerach. Aby to zrobić, należy ręcznie zaktualizować aplikację na tych komputerach (np. lokalnie, korzystając z Kreatora konfiguracji). Podczas wykonywania aktualizacji SMU nie można wybierać pojedynczych komputerów.

Harmonogram aktualizacji aplikacji ustalany jest przez pracowników Kaspersky. Aby mieć pewność, że nowa wersja aplikacji będzie działać bezproblemowo, Kaspersky udostępnia aktualizacje krok po kroku. Oznacza to, że aktualizację SMU możesz otrzymać nawet dwa miesiące po wydaniu nowej wersji.

Aktualizacją SMU aplikacji można zarządzać za pomocą zadania *Aktualizacja baz danych i modułów aplikacji*. Aby nowa wersja aplikacji znajdowała się w tym samym pakiecie co antywirusowe bazy danych, należy zezwolić na aktualizację *modułów aplikacji* w ustawieniach zadania *Aktualizacja baz danych i modułów aplikacji*. Również w ustawieniach zadania *Aktualizacja baz danych i modułów aplikacji*, można zezwolić na aktualizację aplikacji bez ponownego uruchamiania.

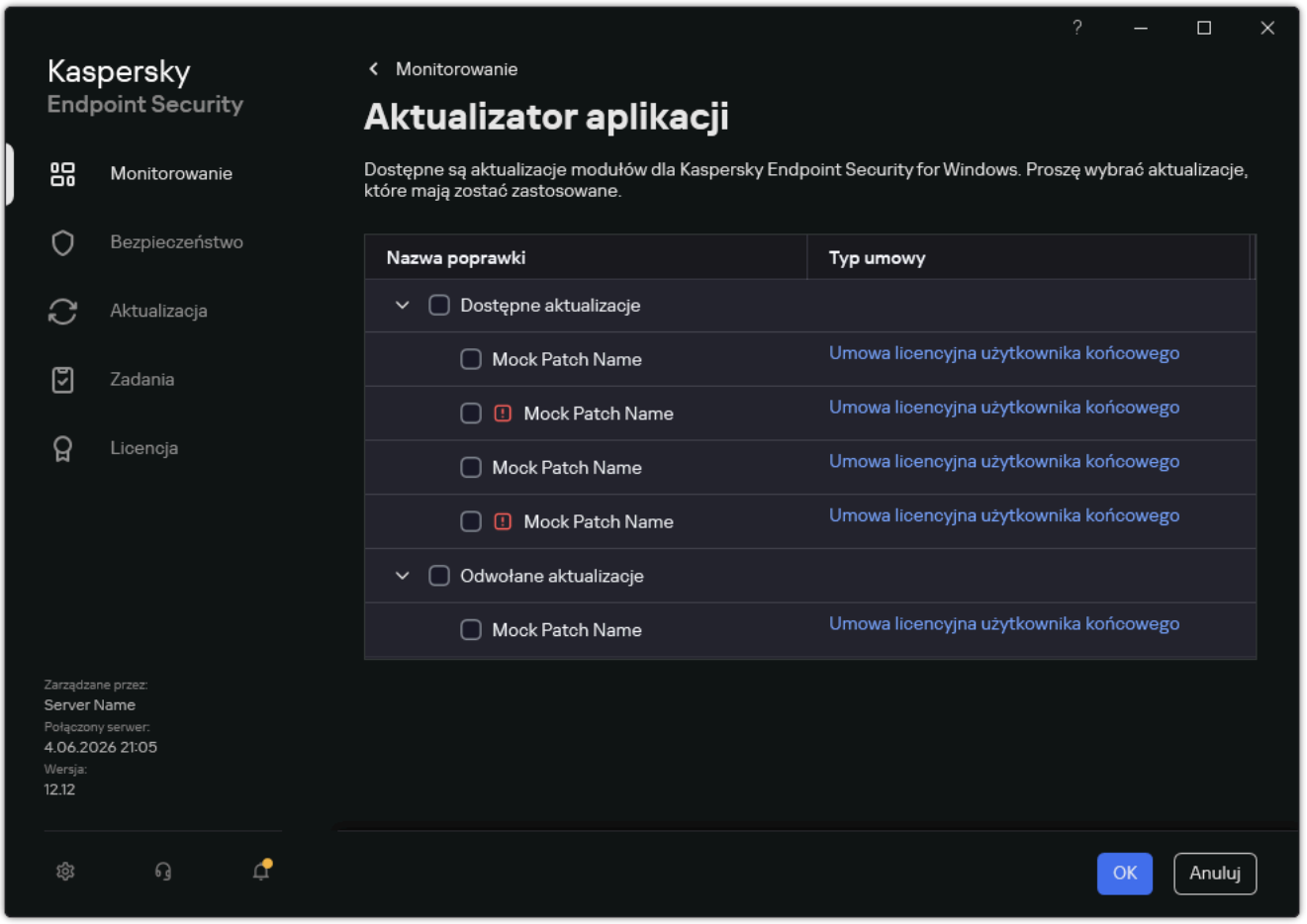
Etapy aktualizacji SMU aplikacji

1. **Po udostępnieniu nowej wersji aplikacji Kaspersky rozpocznie dystrybucję aktualizacji.**
2. **Użytkownik zatwierdza aktualizację aplikacji.**

   Jeżeli komputer jest podłączony do Kaspersky Security Center, aktualizacja jest dostępna w Kaspersky Security Center, w sekcji **Aktualizacja baz danych i modułów aplikacji Kaspersky**. Bardziej szczegółowe informacje na temat zatwierdzania aktualizacji można znaleźć w pomocy do Kaspersky Security Center.

   Jeżeli komputer nie jest połączony z Kaspersky Security Center, aktualizacja jest dostępna w sekcji powiadomień interfejsu aplikacji: . Aby zatwierdzić aktualizację, wybierz wersję aplikacji i zaakceptuj warunki umów (patrz poniższy rysunek).
3. **Kaspersky Endpoint Security uruchamia zadanie *Aktualizacja baz danych i modułów aplikacji* zgodnie ze skonfigurowanym harmonogramem.**

W rezultacie, Kaspersky Endpoint Security aktualizuje aplikację w trybie „cichym”.



Dostępne aktualizacje aplikacji

Dezinstalacja aplikacji

Usunięcie Kaspersky Endpoint Security pozostawi komputer i dane użytkownika bez ochrony przed zagrożeniami.

Podczas instalowania, aktualizacji lub odinstalowywania Kaspersky Endpoint Security mogą wystąpić błędy. Aby uzyskać więcej informacji na temat rozwiązywania tych błędów, zapoznaj się z Bazą wiedzy pomocy technicznej.

Zdalne usuwanie aplikacji za pośrednictwem Kaspersky Security Center

Możesz zdalnie odinstalować aplikację, korzystając z zadania *Zdalna dezinstalacja aplikacji*. Podczas wykonywania zadania program Kaspersky Endpoint Security pobiera narzędzie do usuwania aplikacji na komputer użytkownika. Po zakończeniu dezinstalacji aplikacji narzędzie zostanie automatycznie usunięte.

Jak usunąć aplikację za pomocą Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zadania**.

   Zostanie otwarta lista zadań.
3. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Serwer administracyjny Kaspersky Security Center → Zaawansowane → Zdalna dezinstalacja aplikacji**.

Krok 2. Wybieranie aplikacji do usunięcia

Wybierz **Odinstaluj aplikację obsługiwaną przez Kaspersky Security Center**.

Krok 3. Ustawienia zadania do odinstalowania aplikacji

Wybierz **Kaspersky Endpoint Security for Windows (14.1)**.

Krok 4. Ustawienia narzędzia do dezinstalacji

Skonfiguruj następujące dodatkowe ustawienia aplikacji:

- **Wymuś pobranie narzędzia dezinstalacyjnego**. Wybierz metodę dostarczenia narzędzia:
  - **Przy użyciu Agenta sieciowego**. Jeśli Agent sieciowy nie został zainstalowany na komputerze, w pierwszej kolejności Agent sieciowy zostanie zainstalowany przy użyciu narzędzi systemu operacyjnego. Następnie Kaspersky Endpoint Security zostanie odinstalowany przez narzędzia Agenta sieciowego.
  - **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**. Narzędzie zostanie dostarczone na komputery klienckie przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny. Możesz wybrać tę opcję, jeśli na komputerze klienckim nie ma zainstalowanego Agenta sieciowego, ale komputer kliencki jest w tej samej sieci co Serwer administracyjny.
  - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**. Narzędzie jest dostarczane na komputery klienckie przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny. Więcej informacji o punktach dystrybucji znajdziesz w pomocy do Kaspersky Security Center.
- **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**. W razie potrzeby odznacz to pole. Umożliwia to uniknięcie pobrania narzędzia do dezinstalacji, jeśli system operacyjny komputera nie spełni wymagań oprogramowania. Jeśli jesteś pewien, że system operacyjny komputera spełnia wymagania oprogramowania, możesz pominąć tę weryfikację.

Jeśli operacja dezinstalacji aplikacji jest chroniona hasłem, wykonaj następujące czynności:

1. Zaznacz pole **Użyj hasła dezinstalacyjnego**.
2. Kliknij przycisk **Edytuj**.
3. Wpisz hasło do konta KLAdmin.

Krok 5. Wybieranie ustawienia ponownego uruchomienia systemu operacyjnego

Po odinstalowaniu aplikacji wymagane jest ponowne uruchomienie. Wybierz akcję, która zostanie wykonana w celu ponownego uruchomienia komputera.

Krok 6. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 7. Wybieranie konta do uruchomienia zadania

Wybierz konto do zainstalowania Agenta sieciowego przy użyciu narzędzi systemu operacyjnego. W tym przypadku uprawnienia administratora są wymagane do uzyskania dostępu do komputera. Możesz dodać kilka kont. Jeśli konto nie posiada wystarczających uprawnień, Kreator instalacji użyje następnego konta. Jeśli usuwasz Kaspersky Endpoint Security przy użyciu narzędzi Agenta sieciowego, nie musisz wybierać konta.

Krok 8. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz uruchamiania zadania, na przykład, ręcznie lub gdy komputer jest w trybie bezczynności.

Krok 9. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład: *Usuń Kaspersky Endpoint Security 14.1*.

Krok 10. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Aplikacja zostanie odinstalowana w trybie cichym.

Jak usunąć aplikację za pomocą Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Security Center**.
2. Z listy rozwijalnej **Typ zadania** wybierz **Zdalna dezinstalacja aplikacji**.
3. W polu **Nazwa zadania** wpisz krótki opis, na przykład *Usuń Kaspersky Endpoint Security z komputerów pomocy technicznej*.
4. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

Krok 2. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Na przykład, wybierz oddzielną grupę administracyjną lub skompiluj wybór.

Krok 3. Konfigurowanie ustawień dezinstalacji aplikacji

W tym kroku skonfiguruj ustawienia dezinstalacji aplikacji:

1. Wybierz typ **Odinstaluj zarządzane aplikacje**.
2. Wybierz **Kaspersky Endpoint Security for Windows**.
3. **Wymuś pobranie narzędzia dezinstalacyjnego**. Wybierz metodę dostarczenia narzędzia:
   - **Przy użyciu Agenta sieciowego**. Jeśli Agent sieciowy nie został zainstalowany na komputerze, w pierwszej kolejności Agent sieciowy zostanie zainstalowany przy użyciu narzędzi systemu operacyjnego. Następnie Kaspersky Endpoint Security zostanie odinstalowany przez narzędzia Agenta sieciowego.
   - **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**. Narzędzie zostanie dostarczone na komputery klienckie przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny. Możesz wybrać tę opcję, jeśli na komputerze klienckim nie ma zainstalowanego Agenta sieciowego, ale komputer kliencki jest w tej samej sieci co Serwer administracyjny.
   - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**. Narzędzie jest dostarczane na komputery klienckie przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny. Więcej informacji o punktach dystrybucji znajdziesz w pomocy do Kaspersky Security Center.
4. W polu **Maksymalna liczba jednoczesnych pobierań** ustaw limit liczby żądań wysłanych do Serwera administracyjnego w celu pobrania narzędzia do odinstalowania aplikacji. Ograniczenie liczby żądań pomoże w ograniczeniu przeciążenia sieci.

5. W polu **Maksymalna liczba prób dezinstalacji** ustaw ograniczenie liczby prób odinstalowania aplikacji. Jeśli dezinstalacja Kaspersky Endpoint Security zakończy się błędem, zadanie automatycznie uruchomi ponownie dezinstalację.

6. Jeśli to konieczne, odznacz pole wyboru **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**. Umożliwia to uniknięcie pobrania narzędzia do dezinstalacji, jeśli system operacyjny komputera nie spełni wymagań oprogramowania. Jeśli jesteś pewien, że system operacyjny komputera spełnia wymagania oprogramowania, możesz pominąć tę weryfikację.

Krok 4. Wybieranie konta do uruchomienia zadania

Wybierz konto do zainstalowania Agenta sieciowego przy użyciu narzędzi systemu operacyjnego. W tym przypadku uprawnienia administratora są wymagane do uzyskania dostępu do komputera. Możesz dodać kilka kont. Jeśli konto nie posiada wystarczających uprawnień, Kreator instalacji użyje następnego konta. Jeśli usuwasz Kaspersky Endpoint Security przy użyciu narzędzi Agenta sieciowego, nie musisz wybierać konta.

Krok 5. Kończenie tworzenia zadania

Zakończ działanie kreatora, klikając przycisk **Zakończ**. Nowe zadanie zostanie wyświetlone na liście zadań.

Aby uruchomić zadanie, zaznacz pole obok zadania i kliknij przycisk **Uruchom**. Aplikacja zostanie odinstalowana w trybie cichym. Po zakończeniu dezinstalacji, Kaspersky Endpoint Security wyświetli pytanie o ponowne uruchomienie komputera.

> Jeśli działanie odinstalowania aplikacji jest chronione hasłem, we właściwościach zadania *Zdalna dezinstalacja aplikacji* wpisz hasło do konta KLAdmin. Bez hasła zadanie nie zostanie wykonane.

W celu użycia hasła do konta KLAdmin w zadaniu Zdalna dezinstalacja aplikacji:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie **Zdalna dezinstalacja aplikacji** w Kaspersky Security Center.

   Zostanie otwarte okno właściwości zadania.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Zaznacz pole **Użyj hasła dezinstalacyjnego**.

5. Wpisz hasło do konta KLAdmin.

6. Zapisz swoje zmiany.

Uruchom ponownie komputer, aby zakończyć dezinstalację. Aby to zrobić, Agent sieciowy wyświetla wyskakujące okno.

Zdalne usuwanie aplikacji za pomocą Active Directory

Możesz zdalnie odinstalować aplikację, używając zasad grupy systemu Microsoft Windows. Aby odinstalować aplikację, musisz otworzyć Konsolę zarządzania zasadami grupy (gpmc.msc) i użyć Edytora zasad grupy, aby utworzyć zadanie usunięcia aplikacji (więcej szczegółów znajdziesz na stronie wsparcia technicznego Microsoft).

Jeśli operacja dezinstalacji aplikacji jest chroniona hasłem, konieczne jest wykonanie następujących czynności:

1. Utwórz plik BAT o następującej zawartości:

```
msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
```

<GUID> jest unikatowym identyfikatorem aplikacji. Możesz znaleźć identyfikator GUID aplikacji w Bazie wiedzy pomocy technicznej lub za pomocą następującego polecenia:

```
wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
```

Na przykład

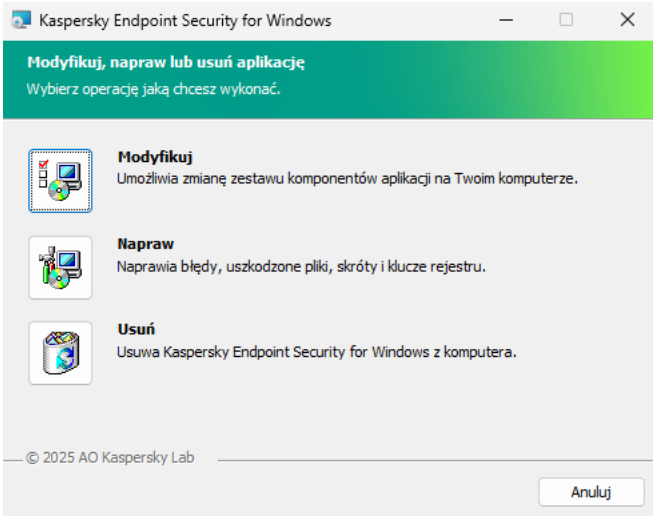
```
msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

2. W konsoli zarządzania zasadami grupy (gpmc.msc) utwórz nowe zasady systemu Microsoft Windows dla komputerów.

3. Użyj nowej zasady, aby uruchomić utworzony plik BAT na komputerach.

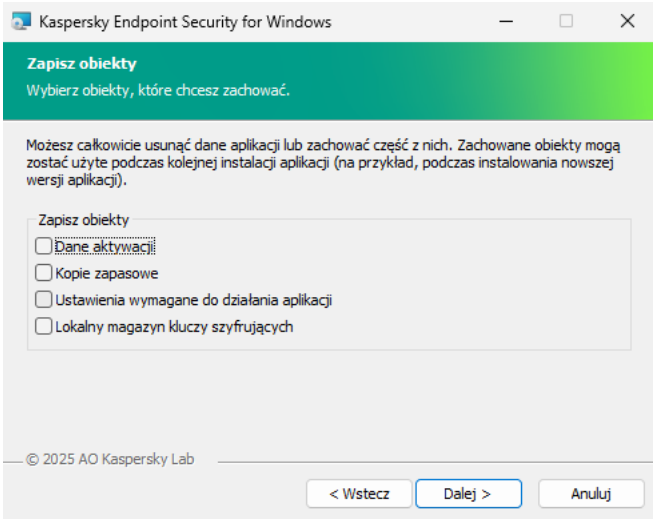
Lokalne usuwanie aplikacji

Aplikację możesz usunąć lokalnie, korzystając z Kreatora instalacji. Kaspersky Endpoint Security jest usuwany przy użyciu normalnej metody dla systemu operacyjnego Windows, czyli poprzez Panel sterowania. Zostanie uruchomiony Kreator instalacji. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.



Wybór operacji usuwania aplikacji

Możesz wskazać, które dane używane przez aplikację chcesz zachować do ponownego użycia podczas kolejnej instalacji programu (np. jego nowszej wersji). Jeśli nie określisz żadnych danych, aplikacja zostanie całkowicie usunięta (patrz rysunek poniżej).



Zapisanie danych po usunięciu

Możesz zapisać następujące dane:

- **Dane aktywacji**, które pozwalają uniknąć konieczności ponownego aktywowania aplikacji. Kaspersky Endpoint Security automatycznie dodaje klucz licencyjny, jeśli okres ważności licencji nie utracił ważności przed instalacją.
- **Kopie zapasowe** – pliki przeskanowane przez aplikację i umieszczone w Kopii zapasowej.

  Dostęp do plików Kopii zapasowej, które zostały zapisane po usunięciu aplikacji, można uzyskać tylko z poziomu tej samej wersji aplikacji, która została użyta do zapisania tych plików.

  Jeżeli zamierzasz użyć obiektów Kopii zapasowej po usunięciu aplikacji, przed usunięciem aplikacji musisz przywrócić te obiekty. Jednakże eksperci z Kaspersky nie zalecają przywracania obiektów z Kopii zapasowej, ponieważ może to doprowadzić do wyrządzenia szkód na komputerze.

- **Ustawienia wymagane do działania aplikacji** – wartości ustawień aplikacji wybrane podczas jej konfiguracji.
- **Lokalny magazyn kluczy szyfrujących** – dane umożliwiające dostęp do plików i dysków zaszyfrowanych przed usunięciem aplikacji. Aby zapewnić dostęp do zaszyfrowanych plików i dysków, upewnij się, że podczas ponownego instalowania Kaspersky Endpoint Security wybrałeś funkcjonalność szyfrowania danych. Do uzyskania dostępu do wcześniej zaszyfrowanych plików i dysków nie jest wymagane żadne dalsze działanie.

Kaspersky Endpoint Security zapisuje dane w folderze `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

Możesz także usunąć aplikację lokalnie przy użyciu wiersza polecenia.

Licencjonowanie aplikacji

Ta sekcja zawiera informacje o ogólnych pojęciach związanych z licencjonowaniem Kaspersky Endpoint Security.

Informacje o Umowie licencyjnej

Umowa licencyjna to wiążąca umowa prawna zawierana pomiędzy Tobą a firmą AO Kaspersky Lab, która określa zasady korzystania z zakupionej aplikacji.

Przed rozpoczęciem korzystania z aplikacji należy dokładnie przeczytać Umowę licencyjną.

Warunki Umowy licencyjnej możesz sprawdzić:

- Podczas instalowania Kaspersky Endpoint Security w trybie interaktywnym.
- W pliku license.txt. Ten dokument znajduje się w pakiecie dystrybucyjnym aplikacji i znajduje się również w folderze instalacyjnym aplikacji `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES`.

Potwierdzenie akceptacji treści Umowy licencyjnej podczas instalacji aplikacji jest równoznaczne z akceptacją warunków tejże umowy. Jeśli nie akceptujesz warunków Umowy licencyjnej, musisz przerwać instalację.

Informacje o licencji

Licencja to czasowo ograniczone prawo do korzystania z aplikacji nadane zgodnie z Umową licencyjną.

Licencja uprawnia Cię do korzystania z aplikacji zgodnie z warunkami Umowy licencyjnej użytkownika końcowego oraz do otrzymywania pomocy technicznej. Lista dostępnych funkcji oraz czas korzystania z aplikacji zależą od typu licencji użytej do aktywacji aplikacji.

Dostępne są następujące typy licencji:

- *Testowa* – jest to darmowa licencja udostępniana w celu zapoznania użytkowników z programem.

  Licencja testowa ma zazwyczaj krótki okres ważności. Po wygaśnięciu licencji testowej wszystkie funkcje programu Kaspersky Endpoint Security stają się niedostępne. Aby kontynuować korzystanie z aplikacji, musisz zakupić licencję komercyjną.

  Możesz aktywować aplikację przy użyciu licencji testowej tylko raz. Aplikacji nie można aktywować w ramach licencji próbnej po uprzedniej aktywacji za pomocą licencji komercyjnej.

- *Komercyjna* – płatna licencja oferowana podczas zakupu Kaspersky Endpoint Security.

  Funkcjonalność aplikacji, objęta licencją komercyjną, zależy od wyboru produktu. Wybrany produkt jest wyszczególniony w certyfikacie licencji. Informacje o dostępnych produktach można znaleźć na stronie internetowej firmy Kaspersky.

  Po wygaśnięciu licencji komercyjnej zostaną włączone kluczowe funkcje aplikacji. Aby kontynuować korzystanie z aplikacji, musisz odnowić licencję komercyjną. Jeśli nie planujesz odnowienia licencji, musisz usunąć aplikację z komputera.

Informacje o certyfikacie licencji

Certyfikat licencji to dokument przesyłany do użytkownika wraz z plikiem klucza lub kodem aktywacyjnym.

Certyfikat licencji zawiera następujące informacje o licencji:

- Identyfikator licencji lub numer zamówienia.
- Szczegóły dotyczące użytkownika, któremu udzielono licencji.
- Szczegóły dotyczące aplikacji, która może być aktywowana przy użyciu licencji.
- Ograniczenie dotyczące stanowisk objętych licencją (na przykład, liczba urządzeń, na których aplikacja może być używana z licencją).
- Data rozpoczęcia okresu ważności licencji.
- Data wygaśnięcia licencji lub okres licencjonowania.
- Typ licencji.

Informacje o subskrypcji

Subskrypcja dla Kaspersky Endpoint Security oznacza zamówienie aplikacji z określonymi parametrami (takimi, jak data wygaśnięcia subskrypcji i liczba chronionych urządzeń). Możesz zamówić subskrypcję dla Kaspersky Endpoint Security u swojego dostawcy usługi. Subskrypcja może zostać odnowiona ręcznie lub automatycznie, bądź też można ją anulować. Możesz zarządzać swoją subskrypcją na stronie internetowej dostawcy usługi.

Subskrypcja może być ograniczona (na przykład na jeden rok) lub nieograniczona (bez daty wygaśnięcia). Aby Kaspersky Endpoint Security działał po wygaśnięciu ograniczonej subskrypcji, należy ją odnowić. Nieograniczona subskrypcja jest odnawiana automatycznie, jeśli przedpłata została zrobiona w odpowiednim czasie.

Jeśli ograniczona subskrypcja wygaśnie, może zostać zaoferowany okres karencji na odnowienie subskrypcji, w trakcie którego aplikacja będzie dalej działać. Dostępność i czas trwania takiego okresu karencji jest ustalane przez dostawcę usługi.

Aby używać Kaspersky Endpoint Security z subskrypcją, należy użyć kodu aktywacyjnego, otrzymanego od dostawcy usługi. Po zastosowaniu kodu aktywacyjnego zostanie zainstalowany aktywny klucz. Aktywny klucz określa licencję do używania aplikacji z subskrypcją. Nie możesz aktywować aplikacji z subskrypcją przy użyciu pliku klucza. Dostawca usługi może dostarczyć tylko kod aktywacyjny. Nie można dodać zapasowego klucza w ramach subskrypcji.

Kody aktywacyjne zakupione dla subskrypcji nie mogą być użyte do aktywacji poprzednich wersji Kaspersky Endpoint Security.

Informacje o kluczu licencyjnym

Klucz licencyjny to sekwencja bitów, których można użyć do aktywacji, a następnie korzystania z aplikacji zgodnie z warunkami Umowy licencyjnej.

Certyfikat licencyjny nie jest udostępniany dla kluczy dodawanych z opcją subskrypcji.

Możesz dodać klucz licencyjny do aplikacji, stosując plik klucza lub wprowadzając kod aktywacyjny.

W przypadku naruszenia warunków Umowy licencyjnej, Kaspersky może zablokować klucz. Jeśli klucz został zablokowany, aby kontynuować korzystanie z aplikacji, należy dodać inny klucz.

Istnieją dwa typy kluczy: aktywny i zapasowy.

Aktywny klucz to klucz, który jest aktualnie używany przez aplikację. Jako aktywny klucz można dodać testowy lub komercyjny klucz licencyjny. Aplikacja może posiadać tylko jeden aktywny klucz.

Zapasowy klucz to klucz, który daje użytkownikowi prawo do korzystania z aplikacji, chociaż nie jest on aktualnie w użyciu. W momencie wygaśnięcia aktywnego klucza zapasowy klucz staje się automatycznie aktywny. Zapasowy klucz może zostać dodany tylko wtedy, gdy jest dostępny aktywny klucz.

Klucz dla licencji testowej może zostać dodany tylko jako klucz aktywny. Nie może być dodany jako klucz zapasowy. Klucz dla licencji testowej nie może zastąpić aktywnego klucza dla licencji komercyjnej.

Jeśli klucz został dodany do zablokowanych kluczy, funkcjonalność aplikacji zdefiniowana przez licencję użytą do aktywacji aplikacji pozostanie dostępna przez osiem dni. Aplikacja poinformuje użytkownika, że klucz został dodany do listy zabronionych kluczy. Po ośmiu dniach, funkcjonalność aplikacji zostaje ograniczona do poziomu funkcjonalności, który jest dostępny po wygaśnięciu licencji. Możesz korzystać z komponentów ochrony i kontroli oraz uruchamiać skanowanie z użyciem baz danych, które zostały zainstalowane przed wygaśnięciem licencji. Aplikacja będzie nadal szyfrować pliki, które zostały zmodyfikowane i zaszyfrowane przed wygaśnięciem licencji, ale nie będzie szyfrować nowych plików. Korzystanie z Kaspersky Security Network nie jest możliwe.

Informacje o kodzie aktywacyjnym

Kod aktywacyjny to unikatowa sekwencja 20 znaków alfanumerycznych. Wprowadź kod aktywacyjny, aby dodać klucz licencyjny, który aktywuje Kaspersky Endpoint Security. Kod aktywacyjny otrzymasz na adres e-mail podany po zakupie Kaspersky Endpoint Security.

Aby aktywować aplikację przy użyciu kodu aktywacyjnego, wymagane jest aktywne połączenie z internetem w celu nawiązania połączenia z serwerami aktywacji Kaspersky.

Podczas aktywacji aplikacji przy użyciu kodu aktywacyjnego, dodawany jest aktywny klucz. Zapasowy klucz można dodać tylko przy użyciu kodu aktywacyjnego i nie można go dodać przy użyciu pliku klucza.

Jeśli po aktywacji aplikacji utracono kod aktywacyjny, będzie można go odzyskać. Kod aktywacyjny jest niezbędny, na przykład, do rejestracji w Kaspersky CompanyAccount. Jeśli kod aktywacyjny został utracony po aktywacji aplikacji, skontaktuj się z partnerem firmy Kaspersky, u którego zakupiłeś licencję.

Informacje o pliku klucza

Plik klucza to plik z rozszerzeniem .key, który otrzymasz od Kaspersky. Przeznaczeniem pliku klucza jest dodanie klucza licencyjnego aktywującego aplikację.

Otrzymasz plik klucza na adres e-mail podany przy zakupie programu Kaspersky Endpoint Security lub zamówieniu wersji testowej programu Kaspersky Endpoint Security.

Aby aktywować aplikację przy użyciu pliku klucza, nie ma konieczności nawiązania połączenia z serwerami aktywacji Kaspersky.

Przypadkowo usunięty plik klucza można odzyskać. Plik klucza może być potrzebny, na przykład, do zarejestrowania się w usłudze CompanyAccount.

W celu odzyskania pliku klucza:

- Skontaktuj się ze sprzedawcą licencji.
- Uzyskaj plik klucza na stronie internetowej Kaspersky w oparciu o istniejący kod aktywacyjny.
- Pobierz plik klucza z innego Serwera administracyjnego.

Podczas aktywacji aplikacji przy użyciu pliku klucza, dodawany jest aktywny klucz. Zapasowy klucz można dodać tylko przy użyciu pliku klucza i nie można go dodać przy użyciu kodu aktywacyjnego.

Porównanie funkcjonalności aplikacji w zależności od typu licencji dla stacji roboczych

Zestaw funkcji Kaspersky Endpoint Security dostępnych na stacjach roboczych zależy od typu licencji (patrz tabela poniżej).

Zapoznaj się z porównaniem funkcji aplikacji dla serwerów

Porównanie funkcjonalności aplikacji w zależności od typu licencji Kaspersky Next znajduje się w części Pomoc Kaspersky Next.

Porównanie funkcji Kaspersky Endpoint Security

Funkcja	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Zaawansowana ochrona przed zagrożeniami								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓

Funkcja	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Wykrywanie zachowań	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona przed exploitami	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona przed włamaniami	✓	✓	✓	✓	✓	✓	✓	✓
Silnik korygujący	✓	✓	✓	✓	✓	✓	✓	✓
Podstawowa ochrona przed zagrożeniami								
Ochrona plików	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona WWW	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona poczty	✓	✓	✓	✓	✓	✓	✓	✓
Zapora sieciowa	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona sieci	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona przed atakami BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Kontrola zabezpieczeń								
Kontrola dziennika	–	–	–	–	–	–	–	–
Kontrola aplikacji	✓	✓	✓	✓	✓	✓	✓	✓
Kontrola urządzeń	✓	✓	✓	✓	✓	✓	✓	✓
Kontrola sieci	✓	✓	✓	✓	✓	✓	✓	✓
Adaptacyjna kontrola anomalii	–	✓	✓	✓	✓	✓	–	✓
Monitor integralności systemu	–	–	–	–	–	–	–	–
Szyfrowanie danych								
Kaspersky Disk Encryption	–	✓	✓	✓	✓	✓	–	✓
Szyfrowanie dysków funkcją BitLocker	–	✓	✓	✓	✓	✓	–	✓
Szyfrowanie plików	–	✓	✓	✓	✓	✓	–	✓
Szyfrowanie nośników wymiennych	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–

Funkcja	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Kaspersky Sandbox *(Licencję Kaspersky Sandbox należy zakupić osobno)*	✓	✓	✓	✓	✓	✓	✓	✓
Integracja z KUMA *(licencję na integrację KUMA należy zakupić osobno)*	✓	✓	✓	✓	✓	✓	✓	✓
Tryb Light Agent *(Aby aktywować aplikację, musisz dodać klucz licencyjny do maszyny SVM, z którą połączony jest klient Light Agent).*	–	–	–	–	–	–	✓	✓

Porównanie funkcjonalności aplikacji w zależności od typu licencji dla serwerów

Zestaw funkcji Kaspersky Endpoint Security dostępnych na serwerach zależy od typu licencji (patrz tabela poniżej).

Zapoznaj się z porównaniem funkcji aplikacji dla stacji roboczych

Porównanie funkcjonalności aplikacji w zależności od typu licencji Kaspersky Next znajduje się w części Pomoc Kaspersky Next.

Porównanie funkcji Kaspersky Endpoint Security

Funkcja	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Zaawansowana ochrona przed zagrożeniami								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Wykrywanie zachowań	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona przed exploitami	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona przed włamaniami	–	–	–	–	–	–	–	–
Silnik korygujący	✓	✓	✓	✓	✓	✓	✓	✓

Funkcja	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Podstawowa ochrona przed zagrożeniami								
Ochrona plików	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona WWW	–	✓	✓	✓	✓	✓	✓	✓
Ochrona poczty	–	✓	✓	✓	✓	✓	✓	✓
Zapora sieciowa	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona sieci	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona przed atakami BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Ochrona AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Kontrola zabezpieczeń								
Kontrola dziennika	–	–	–	–	–	–	–	✓
Kontrola aplikacji	–	✓	✓	✓	✓	✓	–	✓
Kontrola urządzeń	–	✓	✓	✓	✓	✓	✓	✓
Kontrola sieci	–	✓	✓	✓	✓	✓	✓	✓
Adaptacyjna kontrola anomalii	–	–	–	–	–	–	–	–
Monitor integralności systemu	–	–	–	–	–	–	–	✓
Szyfrowanie danych								
Kaspersky Disk Encryption	–	–	–	–	–	–	–	–
Szyfrowanie dysków funkcją BitLocker	–	✓	✓	✓	✓	✓	–	✓
Szyfrowanie plików	–	–	–	–	–	–	–	–
Szyfrowanie nośników wymiennych	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(Licencję Kaspersky Sandbox należy zakupić osobno)*	✓	✓	✓	✓	✓	✓	✓	✓

Funkcja	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Integracja z KUMA *(licencję na integrację KUMA należy zakupić osobno)*	✓	✓	✓	✓	✓	✓	✓	✓
Tryb Light Agent *(Aby aktywować aplikację, musisz dodać klucz licencyjny do maszyny SVM, z którą połączony jest klient Light Agent).*	–	–	–	–	–	–	✓	✓

Aktywowanie aplikacji

Aktywacja to procedura aktywacji licencji, która umożliwia wykorzystanie pełnej wersji aplikacji i wszystkich jej funkcji do momentu wygaśnięcia licencji. Aktywacja aplikacji wymaga dodania klucza licencyjnego.

Możesz aktywować aplikację na jeden z następujących sposobów:

- Lokalnie z interfejsu aplikacji za pomocą Kreatora aktywacji. W ten sposób możesz dodać aktywny i zapasowy klucz.
- Zdalnie przy użyciu pakietu oprogramowania Kaspersky Security Center.
  - Przy pomocy zadania *Dodaj klucz*.

    Ta metoda umożliwia dodanie klucza do określonego komputera lub do komputerów, które są częścią grupy administracyjnej. W ten sposób możesz dodać aktywny i zapasowy klucz.
  - Rozsyłając klucz, który jest przechowywany na Serwerze administracyjnym Kaspersky Security Center, na komputery.

    Ta metoda umożliwia automatyczne dodanie klucza do komputerów, które są już połączone z Kaspersky Security Center, oraz do nowych komputerów. Aby użyć tej metody, w pierwszej kolejności dodaj klucz do Serwera administracyjnego Kaspersky Security Center. Więcej informacji na temat dodawania kluczy do Serwera administracyjnego Kaspersky Security Center można znaleźć w pomocy do Kaspersky Security Center.

    W pierwszej kolejności rozsyłane są kody aktywacyjne z opcją subskrypcji.

- Dodając klucz do pakietu instalacyjnego Kaspersky Endpoint Security.

  Ta metoda umożliwia dodanie klucza we właściwościach pakietu instalacyjnego podczas wdrażania Kaspersky Endpoint Security. Aplikacja jest automatycznie aktywowana po instalacji.

- Korzystając z wiersza poleceń.

Aktywacja aplikacji przy pomocy kodu aktywacyjnego może zająć trochę czasu (podczas zdalnej i nieinteraktywnej instalacji) ze względu na obciążenie serwerów aktywacji Kaspersky. Jeśli chcesz aktywować aplikację od razu, możesz przerwać trwający proces aktywacji i uruchomić aktywację przy użyciu Kreatora aktywacji.

Jeśli rozwiązanie Kaspersky Endpoint Security jest używane w trybie Light Agent do ochrony środowisk wirtualnych, nie ma potrzeby oddzielnej aktywacji aplikacji.

Aktywowanie aplikacji

Jak aktywować aplikację w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Dodaj klucz**.

Krok 2. Dodawanie klucza

Wprowadź kod aktywacyjny lub wybierz plik klucza.

Więcej informacji na temat dodawania kluczy do repozytorium Kaspersky Security Center można znaleźć w pomocy do Kaspersky Security Center.

Krok 3. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 4. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz uruchamiania zadania, na przykład, ręcznie lub gdy komputer jest w trybie bezczynności.

Krok 5. Definiowanie nazwy zadania

Wprowadź nazwę zadania, np. *Aktywuj Kaspersky Endpoint Security for Windows*.

Krok 6. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania. W rezultacie Kaspersky Endpoint Security zostanie aktywowany na komputerach użytkowników w trybie cichym.

Jak aktywować aplikację w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.
2. Z listy rozwijalnej **Typ zadania** wybierz **Dodaj klucz**.
3. W polu **Nazwa zadania** wpisz krótki opis, na przykład, *Aktywacja Kaspersky Endpoint Security for Windows*.
4. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania. Przejdź do następnego kroku.

Krok 2. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 3. Wybieranie licencji

Wybierz licencję, której chcesz użyć do aktywacji aplikacji. Przejdź do następnego kroku.

Możesz dodać klucze do Web Console (**Operacje** → **Licencjonowanie**).

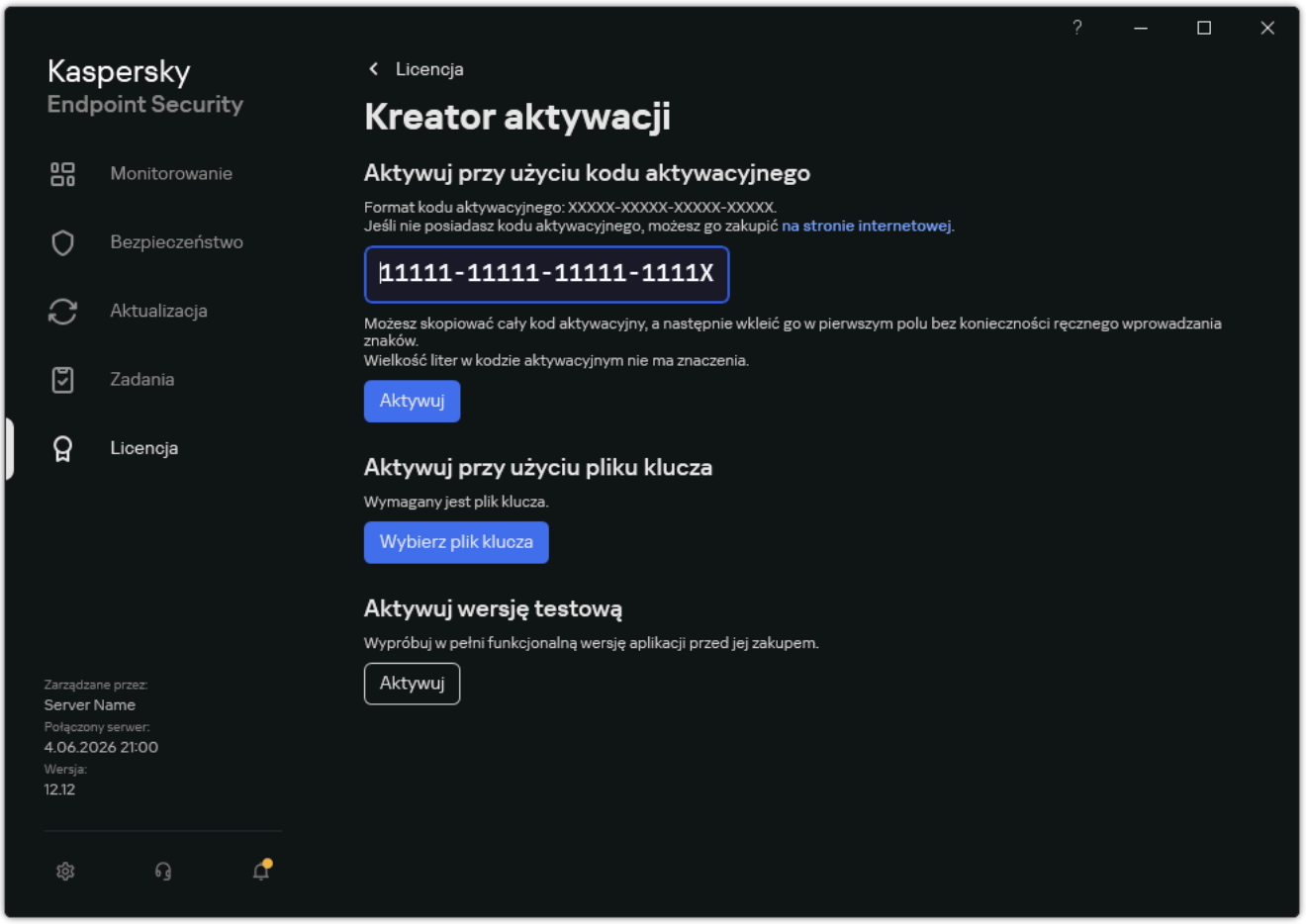
Krok 4. Kończenie tworzenia zadania

Zakończ działanie kreatora, klikając przycisk **Zakończ**. Nowe zadanie zostanie wyświetlone na liście zadań. Aby uruchomić zadanie, zaznacz pole obok zadania i kliknij przycisk **Uruchom**. W rezultacie Kaspersky Endpoint Security zostanie aktywowany na komputerach użytkowników w trybie cichym.

Jak aktywować aplikację w interfejsie aplikacji?

1. W oknie głównym aplikacji przejdź do sekcji **Licencja**.
2. Kliknij **Aktywuj aplikację przy użyciu nowej licencji**.

Zostanie uruchomiony Kreator aktywacji aplikacji. Postępuj zgodnie z instrukcjami Kreatora aktywacji.



Aktywowanie aplikacji

We właściwościach zadania *Dodaj klucz* możesz dodać klucz zapasowy do komputera. *Klucz rezerwowy* staje się aktywny, gdy aktywny klucz utraci ważność. Dostępność klucza zapasowego pozwala uniknąć ograniczeń funkcjonalności aplikacji po wygaśnięciu licencji.

Jak automatycznie dodać klucz licencyjny do komputerów za pomocą Konsoli administracyjnej (MMC)?

1. W Konsoli administracyjnej przejdź do folderu **Licencje Kaspersky**.

   Zostanie otwarta lista kluczy licencyjnych.

2. Otwórz właściwości klucza licencyjnego.

3. W sekcji **Ogólne** zaznacz pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**.

4. Zapisz swoje zmiany.

   Klucz zostanie automatycznie rozesłany na odpowiednie komputery. Podczas automatycznego rozsyłania klucza jako aktywnego lub zapasowego brane jest pod uwagę ograniczenie licencyjne dotyczące liczby komputerów (ustawione we właściwościach klucza). Jeśli ograniczenie licencji zostanie osiągnięte, rozesłanie tego klucza na komputery zostanie przerwane automatycznie. Możesz sprawdzić liczbę komputerów, do których klucz został dodany, oraz inne dane we właściwościach klucza, w sekcji **Urządzenia**.

Jak automatycznie dodać klucz licencyjny do komputerów za pośrednictwem Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Operacje** → **Licencjonowanie** → **Licencje**.

   Zostanie otwarta lista kluczy licencyjnych.

2. Otwórz właściwości klucza licencyjnego.

3. W zakładce **Ogólne** włącz przełącznik **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**.

4. Zapisz swoje zmiany.

   Klucz zostanie automatycznie rozesłany na odpowiednie komputery. Podczas automatycznego rozsyłania klucza jako aktywnego lub zapasowego brane jest pod uwagę ograniczenie licencyjne dotyczące liczby komputerów (ustawione we właściwościach klucza). Jeśli ograniczenie licencji zostanie osiągnięte, rozesłanie tego klucza na komputery zostanie przerwane automatycznie. Możesz sprawdzić liczbę komputerów, do których klucz został dodany, oraz innych danych we właściwościach klucza, na zakładce **Urządzenia**.

Jeśli aktywujesz aplikację przy użyciu *kodu aktywacyjnego*, potrzebujesz dostępu do Internetu w celu nawiązania połączenia z serwerami aktywacji Kaspersky. Jeśli aktywujesz aplikację za pomocą *pliku klucza*, dostęp do Internetu nie jest konieczny. Jeśli komputery znajdują się w izolowanym segmencie sieci bez dostępu do Internetu, aby aktywować aplikację za pomocą kodu, musisz zezwolić na używanie Serwera administracyjnego Kaspersky Security Center jako serwera proxy. Oznacza to, że aplikacja może uzyskać dostęp do serwerów aktywacji poprzez Serwer administracyjny, który ma dostęp do Internetu.

Jak zezwolić na używanie Serwera administracyjnego jako serwera proxy do aktywacji aplikacji w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.

4. Zaznacz pole **Użyj Kaspersky Security Center jako serwera proxy do aktywacji**.

5. Zapisz swoje zmiany.

Jak zezwolić na używanie Serwera administracyjnego jako serwera proxy do aktywacji aplikacji w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne** → **Integracja KSC**.

5. Zaznacz pole **Użyj Kaspersky Security Center jako serwera proxy do aktywacji**.

6. Zapisz swoje zmiany.

Jeśli nie możesz aktywować aplikacji za pomocą *kodu aktywacyjnego*, możesz spróbować uzyskać *plik klucza* za pomocą rozwiązania Kaspersky i próbując ponownie aktywować aplikację za pomocą innej metody.

Monitorowanie użycia licencji

Możesz monitorować użycie licencji na następujące sposoby:

- Zobacz *Raport o użyciu kluczy licencyjnych* dotyczący infrastruktury organizacji (**Monitorowanie** → **Raporty**).
- Przejrzyj stany komputerów na zakładce **Zarządzane urządzenia** → **Urządzenia**. Jeśli aplikacja nie została aktywowana, komputer będzie miał stan ⚠ *Aplikacja nie została aktywowana*.
- Przejrzyj informacje o licencji we właściwościach komputera.
- Przejrzyj właściwości klucza (**Operacje** → **Licencjonowanie**).

Specyfika aktywacji aplikacji w ramach Kaspersky Security Center Cloud Console

Dostępna jest wersja testowa dla konsoli Kaspersky Security Center Cloud Console. *Wersja testowa* to specjalna wersja konsoli Kaspersky Security Center Cloud Console, która ma na celu zapoznanie użytkownika z funkcjami aplikacji. W tej wersji możesz wykonywać działania w obszarze roboczym przez okres 30 dni. Wszystkie zarządzane aplikacje są automatycznie uruchamiane na podstawie licencji testowej dla Kaspersky Security Center Cloud Console, w tym Kaspersky Endpoint Security. Nie można jednak aktywować Kaspersky Endpoint Security przy użyciu własnej licencji testowej po wygaśnięciu licencji testowej dla Kaspersky Security Center Cloud Console. Szczegółowe informacje na temat licencjonowania Kaspersky Security Center można znaleźć w pomocy do Kaspersky Security Center Cloud Console.

> Wersja testowa konsoli Kaspersky Security Center Cloud Console nie pozwala na późniejsze przejście do wersji komercyjnej. Każdy testowy obszar roboczy zostanie automatycznie usunięty wraz z całą zawartością po upływie 30-dniowego okresu.

Usuwanie klucza licencyjnego

Aby usunąć klucz licencyjny, należy uruchomić na komputerze specjalne zadanie. Możesz usunąć klucz licencyjny, aby na przykład zmienić kolejność jednostek licencyjnych. Ponadto Kaspersky Endpoint Security powiadamia o wygaśnięciu licencji. Jeśli dodano klucz licencyjny z krótkim okresem ważności w celu wypróbowania aplikacji (na przykład dodatku EDR Optimum), możesz usunąć go, aby pozbyć się powiadomień i naprawić stan komputera.

Zadanie *Usuwanie klucza* pozwala usunąć wszelkie klucze licencyjne z komputera. Możesz usunąć aktywne klucze licencyjne, a także rezerwować klucze licencyjne. Oprócz klucza licencyjnego do aktywacji Kaspersky Endpoint Security możesz usunąć poszczególne klucze licencyjne rozwiązań Kaspersky Detection and Response (na przykład dodatek EDR Optimum).

Jak usunąć klucz licencyjny w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Usuwanie klucza**.

Krok 2. Wybieranie licencji

Wybierz klucze licencyjne, które chcesz usunąć. Klucz licencyjny można wybrać z magazynu kluczy Kaspersky Security Center lub wybrać plik klucza.

Krok 3. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 4. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz uruchamiania zadania, na przykład, ręcznie lub gdy komputer jest w trybie bezczynności.

Krok 5. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład *Usuwanie klucza do wersji beta*.

Krok 6. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Jak usunąć klucz licencyjny w Web Console

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.
2. Z listy rozwijalnej **Typ zadania** wybierz **Usuwanie klucza**.
3. W polu **Nazwa zadania** wpisz krótki opis, na przykład *Usuwanie klucza do wersji beta*.
4. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania. Przejdź do następnego kroku.

Krok 2. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 3. Wybieranie licencji

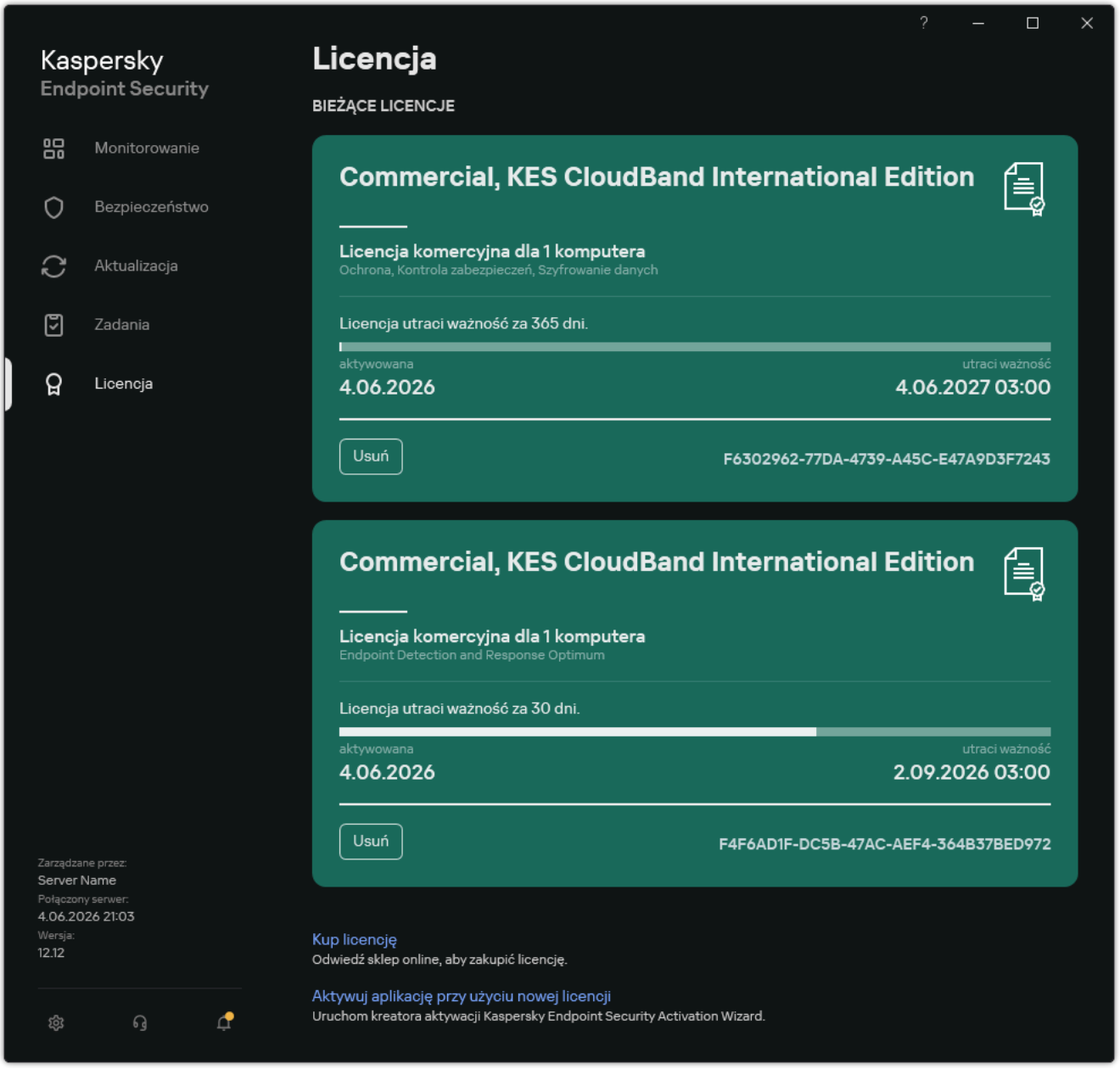
Wybierz klucze licencyjne, które chcesz usunąć. Klucz licencyjny można wybrać z magazynu kluczy Kaspersky Security Center lub wybrać plik klucza. Przejdź do następnego kroku.

Krok 4. Kończenie tworzenia zadania

Zakończ działanie kreatora, klikając przycisk **Zakończ**. Nowe zadanie zostanie wyświetlone na liście zadań. Aby uruchomić zadanie, zaznacz pole obok zadania i kliknij przycisk **Uruchom**.

Jak usunąć klucz licencyjny w interfejsie aplikacji

1. W oknie głównym aplikacji przejdź do sekcji **Licencja**.
2. Wybierz klucz, który chcesz usunąć i kliknij **Usuń**.



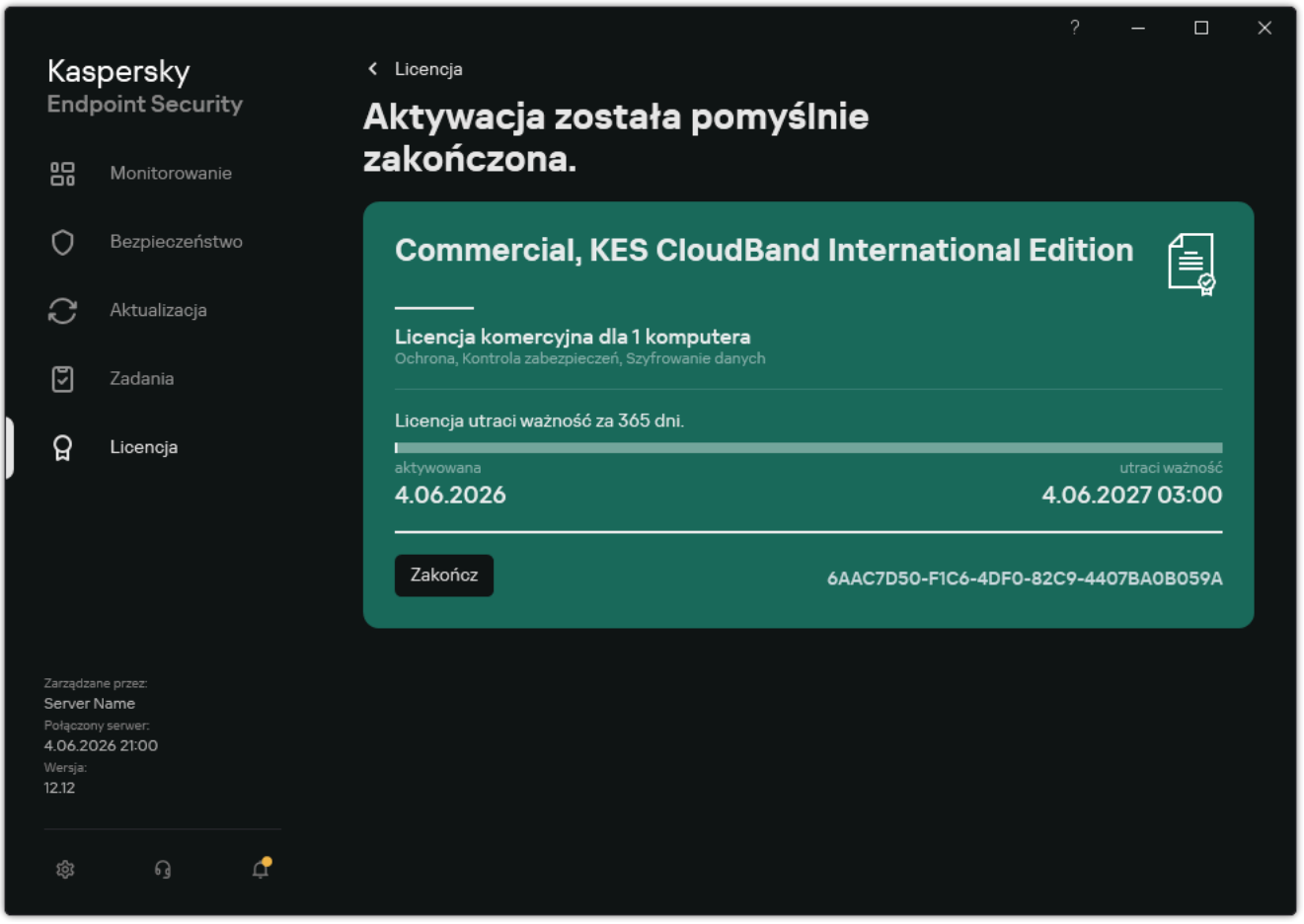
Okno Licencjonowanie

Możesz także usunąć klucz licencyjny w wierszu poleceń.

Przeglądanie informacji o licencji

W celu przejrzenia informacji o licencji:

W oknie głównym aplikacji przejdź do sekcji **Licencja** (patrz rysunek poniżej).



Okno Licencjonowanie

Sekcja wyświetla następujące szczegóły:

- *Stan klucza*. Na komputerze może być przechowywanych kilka kluczy. Istnieją dwa typy kluczy: aktywny i zapasowy. Aplikacja może posiadać tylko jeden aktywny klucz. Klucz zapasowy może stać się aktywny tylko wtedy, gdy aktywny klucz utraci ważność lub jeśli aktywny klucz został usunięty po kliknięciu przycisku **Usuń**.
- *Nazwa aplikacji*. Pełna nazwa zakupionej aplikacji firmy Kaspersky.
- *Typ licencji*. Dostępne są następujące typy licencji: testowa i komercyjna.
- *Funkcjonalność*. Funkcje aplikacji dostępne w posiadanej licencji. Funkcje mogą obejmować Ochronę, Kontrolę zabezpieczeń, Szyfrowanie danych i inne. Lista dostępnych funkcji znajduje się również w Certyfikacie licencji.

- *Dodatkowe informacje o licencji*. Data początkowa i data końcowa okresu ważności licencji (tylko dla klucza aktywnego), pozostały czas trwania okresu ważności.

  Godzina wygaśnięcia licencji jest wyświetlana zgodnie ze strefą czasową skonfigurowaną w systemie operacyjnym.

- *Klucz*. Klucz to unikatowa sekwencja znaków alfanumerycznych, wygenerowana z kodu aktywacyjnego lub pliku klucza.

W oknie Licencjonowanie wykonaj jedną z następujących czynności:

- **Kup licencję** / **Odnów licencję**. Otwiera stronę sklepu internetowego Kaspersky, w którym możesz zakupić lub odnowić licencję. W tym celu wprowadź informacje o swojej firmie i zapłać za zamówienie.

- **Aktywuj aplikację przy użyciu nowej licencji**. Spowoduje uruchomienie Kreatora aktywacji aplikacji. W tym kreatorze możesz dodać klucz, korzystając z kodu aktywacyjnego lub pliku klucza. Kreator aktywacji aplikacji umożliwia dodanie aktywnego klucza i tylko jednego klucza zapasowego.

Kupowanie licencji

Licencję można zakupić po zainstalowaniu aplikacji. Po zakupie licencji otrzymasz kod aktywacyjny lub plik klucza do aktywacji aplikacji.

W celu zakupienia licencji:

1. W oknie głównym aplikacji przejdź do sekcji **Licencja**.
2. Wykonaj jedną z poniższych czynności:

   - Jeśli nie dodano żadnego klucza lub dodano klucz dla licencji testowej, kliknij przycisk **Kup licencję**.
   - Jeżeli dodano klucz dla licencji komercyjnej, kliknij przycisk **Odnów licencję**.

   Zostanie otwarta strona sklepu internetowego Kaspersky, w którym można zakupić licencję.

Odnawianie subskrypcji

Jeśli korzystasz z aplikacji z subskrypcją, Kaspersky Endpoint Security automatycznie łączy się z serwerem aktywacji w określonych przedziałach czasu, aż do momentu wygaśnięcia Twojej subskrypcji.

Jeśli korzystasz z aplikacji z nieograniczoną subskrypcją, Kaspersky Endpoint Security automatycznie sprawdza, czy na serwerze aktywacji znajdują się odnowione klucze w sposób niezauważalny dla użytkownika. Jeżeli klucz jest dostępny na serwerze aktywacji, aplikacja doda go, zastępując poprzedni klucz. W ten sposób nieograniczona subskrypcja dla Kaspersky Endpoint Security jest odnawiana bez udziału użytkownika.

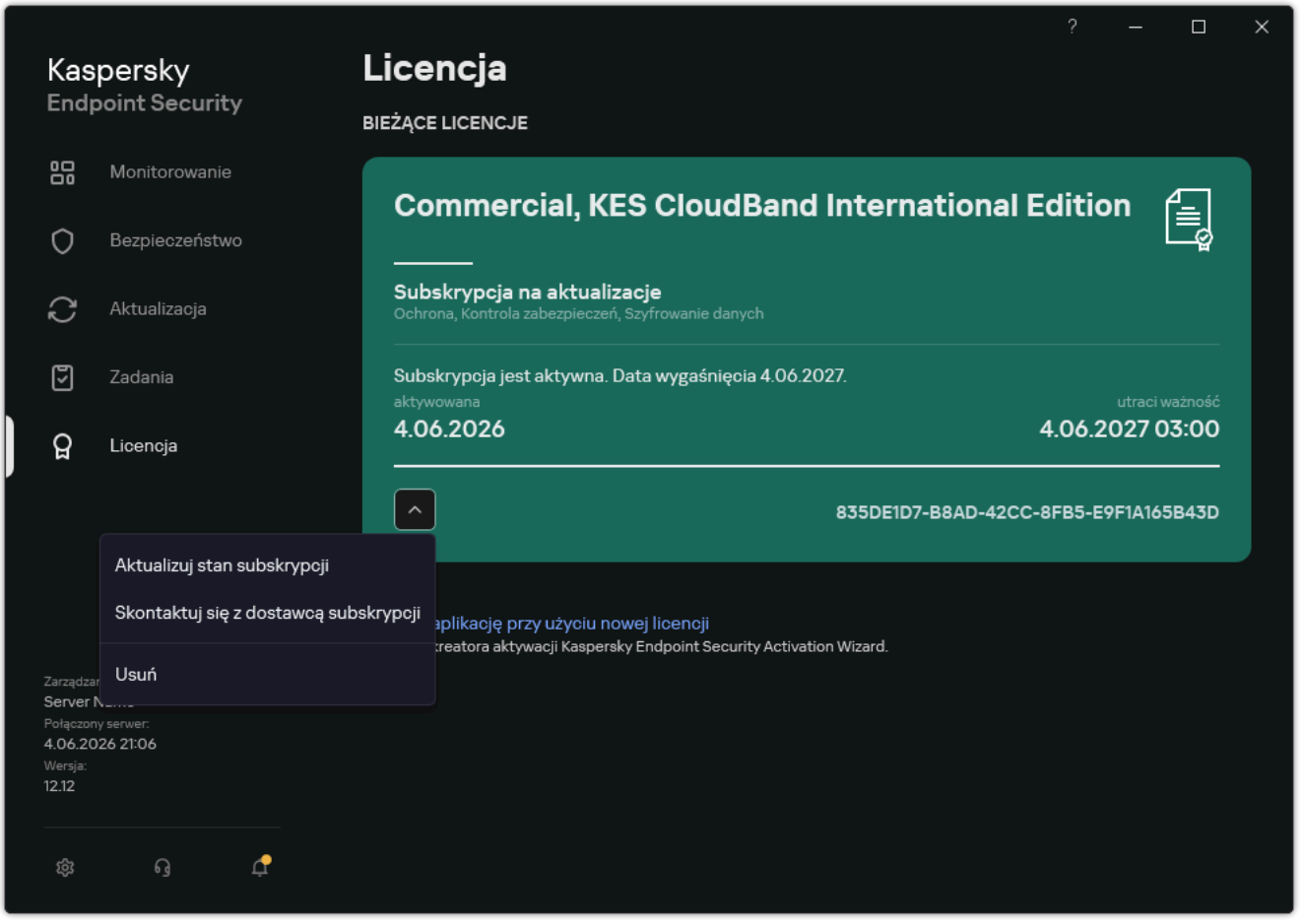
Jeśli korzystasz z aplikacji z ograniczoną subskrypcją, w dniu wygaśnięcia subskrypcji (lub w dniu wygaśnięcia okresu karencji na odnowienie subskrypcji) Kaspersky Endpoint Security powiadomi o tym fakcie i zaniecha próby automatycznego odnowienia subskrypcji. W tym przypadku program Kaspersky Endpoint Security zachowa się w ten sam sposób co przy wygaśnięciu licencji komercyjnej dla aplikacji – będzie działał bez możliwości aktualizacji i z niedostępną usługą Kaspersky Security Network.

Możesz odnowić subskrypcję na stronie internetowej dostawcy usługi.

W celu odwiedzenia strony dostawcy usługi z poziomu interfejsu aplikacji:

1. W oknie głównym aplikacji przejdź do sekcji **Licencja**.
2. Kliknij **Skontaktuj się z dostawcą subskrypcji**.

Możesz ręcznie zaktualizować stan subskrypcji. Może to być konieczne, gdy subskrypcja została odnowiona po wygaśnięciu okresu karencji, a aplikacja nie zaktualizowała automatycznie stanu subskrypcji.



Odnawianie subskrypcji

Rozpoczęcie pracy

Po zainstalowaniu Kaspersky Endpoint Security możesz zarządzać aplikacją za pomocą następujących interfejsów:

- Lokalny interfejs aplikacji.
- Serwer administracyjny Kaspersky Security Center.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Konsola administracyjna Kaspersky Security Center

Kaspersky Security Center umożliwia zdalne instalowanie i dezinstalowanie, uruchamianie i zatrzymywanie Kaspersky Endpoint Security, konfigurowanie ustawień aplikacji, zmienianie zestawu dostępnych komponentów aplikacji, dodawanie kluczy, a także uruchamianie i zatrzymywanie zadań aktualizacji i skanowania.

Aplikacją można zarządzać z poziomu Kaspersky Security Center przy użyciu wtyczki zarządzającej Kaspersky Endpoint Security.

Aby uzyskać więcej informacji na temat zarządzania aplikacją w Kaspersky Security Center, zapoznaj się z systemem pomocy Kaspersky Security Center.

Kaspersky Security Center Web Console i Kaspersky Security Center Cloud Console

Konsola Kaspersky Security Center Web Console (zwana dalej *Web Console*) to aplikacja webowa przeznaczona do scentralizowanego wykonywania głównych zadań zarządzania i utrzymania systemu ochrony sieci organizacji. Web Console to komponent Kaspersky Security Center, który zapewnia interfejs. Szczegółowe informacje na temat Kaspersky Security Center Web Console można znaleźć w pomocy do Kaspersky Security Center.

Kaspersky Security Center Cloud Console (zwana również „*Cloud Console*") to oparte na chmurze rozwiązanie do ochrony i zarządzania siecią organizacji. Szczegółowe informacje na temat Kaspersky Security Center Cloud Console można znaleźć w pomocy do Kaspersky Security Center Cloud Console.

Web Console i Cloud Console umożliwiają wykonywanie następujących czynności:

- Monitorowanie stanem systemu ochrony organizacji.
- Zainstalowanie aplikacji firmy Kaspersky na urządzeniach w obrębie Twojej sieci.
- Zarządzanie zainstalowanymi aplikacjami.
- Przeglądanie raportów dotyczących stanu systemu ochrony.

Zarządzanie programem Kaspersky Endpoint Security za pośrednictwem Web Console, Cloud Console i Konsoli administracyjnej Kaspersky Security Center zapewnia różne możliwości zarządzania. Dostępne komponenty i zadania różnią się również w zależności od konsoli.

Informacje o wtyczce zarządzającej Kaspersky Endpoint Security for Windows

Wtyczka zarządzająca Kaspersky Endpoint Security for Windows umożliwia interakcję między Kaspersky Endpoint Security a Kaspersky Security Center. Wtyczka zarządzająca umożliwia zarządzanie Kaspersky Endpoint Security przy użyciu zasad, zadań i lokalnych ustawień aplikacji. Interakcja z konsolą Kaspersky Security Center Web Console jest zapewniana przez wtyczkę internetową.

Wersja wtyczki zarządzającej może różnić się od wersji aplikacji Kaspersky Endpoint Security zainstalowanej na komputerze klienckim. Jeśli zainstalowana wersja wtyczki zarządzającej posiada mniej funkcji niż zainstalowana wersja Kaspersky Endpoint Security, ustawienia brakujących funkcji nie są kontrolowane przez wtyczkę zarządzającą. Te ustawienia mogą zostać zmodyfikowane przez użytkownika w lokalnym interfejsie Kaspersky Endpoint Security.

Wtyczka webowa nie jest instalowana domyślnie w Kaspersky Security Center Web Console. Wtyczkę internetową należy zainstalować na komputerze, na którym jest zainstalowana Kaspersky Security Center Web Console. Funkcjonalność wtyczki webowej jest dostępna dla wszystkich administratorów, którzy mają dostęp do konsoli Web Console w przeglądarce. Możesz przejrzeć listę zainstalowanych wtyczek webowych w interfejsie Web Console (**Ustawienia konsoli** → **Wtyczki webowa**). Więcej informacji na temat kompatybilności wersji wtyczek webowych z Web Console można znaleźć w pomocy do Kaspersky Security Center.

Jeśli używasz funkcji Kaspersky Endpoint Security w ramach rozwiązania Kaspersky Endpoint Detection and Response Optimum, musisz zainstalować wtyczkę zarządzającą Kaspersky Endpoint Detection and Response. Wyświetlanie szczegółów alertów wymaga wtyczki zarządzającej. *Szczegóły wykrycia* to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Do tworzenia zadań reagowania na zagrożenia potrzebna jest wtyczka zarządzająca Kaspersky Endpoint Security. Do przeglądania szczegółów alertów potrzebna jest wtyczka zarządzająca EDR.

Instalowanie wtyczki webowej

Wtyczkę webową możesz zainstalować w następujący sposób:

- Zainstaluj wtyczkę webową przy pomocy Kreatora wstępnej konfiguracji konsoli Kaspersky Security Center Web Console.

  Web Console automatycznie wyświetla pytanie o uruchomienie Kreatora wstępnej konfiguracji podczas podłączania Web Console do Serwera administracyjnego po raz pierwszy. Możesz również uruchomić Kreatora szybkiego startu w interfejsie Web Console (**WYKRYWANIE I WDRAŻANIE** → **Wdrażanie i przypisywanie** → **Kreator wstępnej konfiguracji**). Kreator wstępnej konfiguracji sprawdza także, czy zainstalowane wtyczki webowe są aktualne i pobiera niezbędne aktualizacje. Więcej informacji na temat Kreatora wstępnej konfiguracji Kaspersky Security Center Web Console znajdziesz w pomocy do Kaspersky Security Center.

- Zainstaluj wtyczkę webową przy użyciu listy dostępnych pakietów dystrybucyjnych w Web Console.

  Aby zainstalować wtyczkę webową, wybierz pakiet dystrybucyjny wtyczki webowej Kaspersky Endpoint Security w interfejsie Web Console (**Ustawienia konsoli → Wtyczki webowa**). Lista dostępnych pakietów dystrybucyjnych jest aktualizowana automatycznie po publikacji nowych wersji aplikacji firmy Kaspersky.

- Pobierz pakiet dystrybucyjny do Web Console z zewnętrznego źródła.

  Aby zainstalować wtyczkę webową, dodaj archiwum ZIP pakietu dystrybucyjnego dla wtyczki webowej Kaspersky Endpoint Security w interfejsie Web Console (**Ustawienia konsoli → Wtyczki webowa**). Pakiet dystrybucyjny wtyczki webowej może zostać pobrany, na przykład, ze strony internetowej Kaspersky.

Procedura instalacji wtyczki internetowej uległa zmianie w wersji Kaspersky Endpoint Security 12.11 for Windows. Pakiet dystrybucyjny zawiera teraz dwie wtyczki internetowe: *Kaspersky Endpoint Security for Windows 14.2.0* i *Unified Protection and Management Plug-in*. Wynika to z przejścia na ujednoliconą wtyczkę internetową do zarządzania aplikacjami Kaspersky. Ujednolicona wtyczka internetowa umożliwia utworzenie pojedynczej zasady do zarządzania wieloma aplikacjami Kaspersky (na przykład Kaspersky Endpoint Security w wersjach dla systemu Windows, macOS i Linux). Proces przejścia na ujednoliconą wtyczkę internetową może objąć kilka wersji. Po jego zakończeniu pakiet dystrybucyjny będzie zawierał wyłącznie wtyczkę *Unified Protection and Management Plug-in*.

Aktualizowanie wtyczki zarządzającej

Aby zaktualizować wtyczkę zarządzającą Kaspersky Endpoint Security for Windows, pobierz najnowszą wersję wtyczki (zawartej w pakiecie dystrybucyjnym) i uruchom kreatora instalacji wtyczki.

Jeśli nowa wersja wtyczki webowej stanie się dostępna, konsola Web Console wyświetli komunikat *Dla używanych wtyczek dostępne są aktualizacje*. Możesz przejść do aktualizacji wersji wtyczki webowej z tego komunikatu konsoli Web Console. Możesz także ręcznie sprawdzić dostępność nowych aktualizacji wtyczki webowej w interfejsie konsoli Web Console (**Ustawienia konsoli → Wtyczki webowe**). Poprzednia wersja wtyczki webowej zostanie automatycznie usunięta podczas aktualizacji.

> Jeśli wtyczka webowa zostanie zaktualizowana, już istniejące elementy (na przykład, zasady lub zadania) zostaną zapisane. Nowe ustawienia elementów implementujących nowe funkcje Kaspersky Endpoint Security pojawią się w istniejących elementach i będą posiadać domyślne wartości.

Wtyczkę webową możesz zaktualizować w następujący sposób:

- Zaktualizuj wtyczkę webową na liście wtyczek webowych w trybie online.

  Aby zaktualizować wtyczkę webową, wybierz pakiet dystrybucyjny wtyczki webowej Kaspersky Endpoint Security w interfejsie Web Console (**Ustawienia konsoli → Wtyczki webowe**). Konsola Web Console sprawdza dostępność aktualizacji na serwerach Kaspersky i pobiera odpowiednie aktualizacje.

- Zaktualizuj wtyczkę webową z pliku.

  Aby zaktualizować wtyczkę webową, wybierz archiwum ZIP pakietu dystrybucyjnego dla wtyczki webowej Kaspersky Endpoint Security w interfejsie Web Console (**Ustawienia konsoli → Wtyczki webowe**). Pakiet dystrybucyjny wtyczki webowej może zostać pobrany, na przykład, ze strony internetowej Kaspersky. Możesz zaktualizować wtyczkę webową Kaspersky Endpoint Security tylko do najnowszej wersji. Wtyczka webowa nie może zostać zaktualizowana do starszej wersji.

Jeśli otwarty jest jakikolwiek element (taki, jak zasada lub zadanie), wtyczka webowa sprawdzi informacje dotyczące jego kompatybilności. Jeśli wersja wtyczki webowej jest równa lub nowsza niż wersja określona w informacjach dotyczących kompatybilności, możesz zmienić ustawienia tego elementu. W przeciwnym razie nie będziesz mógł używać wtyczki webowej do zmiany ustawień wybranego elementu. Zalecane jest zaktualizowanie wtyczki webowej.

Kwestie specjalne dotyczące pracy z różnymi wersjami wtyczek zarządzających

Możesz zarządzać Kaspersky Endpoint Security za pośrednictwem Kaspersky Security Center tylko wtedy, gdy posiadasz Wtyczkę zarządzającą, której wersja jest równa lub nowsza niż wersja określona w informacjach dotyczących kompatybilności Kaspersky Endpoint Security z Wtyczką zarządzającą. Możesz sprawdzić minimalną wymaganą wersję Wtyczki zarządzającej w pliku installer.ini, znajdującym się w pakiecie dystrybucyjnym.

Jeśli otwarty jest jakikolwiek element (taki, jak zasada lub zadanie), wtyczka zarządzająca sprawdzi informacje dotyczące jego kompatybilności. Jeśli wersja wtyczki zarządzającej jest równa lub nowsza niż wersja określona w informacjach dotyczących kompatybilności, możesz zmienić ustawienia tego komponentu. W przeciwnym razie nie będziesz mógł używać wtyczki zarządzającej do zmiany ustawień wybranego elementu. Zalecane jest zaktualizowanie wtyczki zarządzającej.

Jeśli wtyczka zarządzająca Kaspersky Endpoint Security jest zainstalowana w Konsoli administracyjnej, podczas instalowania nowej wersji wtyczki zarządzającej należy wziąć pod uwagę następujące kwestie:

- Poprzednia wersja wtyczki zarządzającej Kaspersky Endpoint Security zostanie usunięta.
- Nowa wersja wtyczki zarządzającej Kaspersky Endpoint Security obsługuje zarządzanie poprzednią wersją Kaspersky Endpoint Security for Windows na komputerach użytkowników.
- Możesz użyć nowej wersji wtyczki zarządzającej, aby zmienić ustawienia w zasadach, zadaniach i innych elementach utworzonych przez poprzednią wersję wtyczki zarządzającej.
- W przypadku nowych ustawień nowsza wersja wtyczki zarządzającej stosuje domyślne wartości, gdy profil, profil zasad lub zadanie jest zapisywane po raz pierwszy.

  Po zaktualizowaniu wtyczki zarządzającej zalecane jest sprawdzenie i zapisanie wartości nowych ustawień w zasadach i profilach zasad. Jeśli tego nie zrobisz, nowe grupy ustawień Kaspersky Endpoint Security na komputerze użytkownika przyjmą domyślne wartości i mogą być edytowane (atrybut ). Zalecane jest sprawdzenie ustawień, zaczynając od zasad i profili zasad na najwyższym poziomie hierarchii. Zalecane jest także użycie konta użytkownika, które posiada uprawnienia dostępu do wszystkich obszarów funkcyjnych Kaspersky Security Center.

  Aby poznać nowe możliwości aplikacji, zapoznaj się z Informacjami o kompilacji lub systemem pomocy aplikacji.

- Jeśli nowy parametr został dodany do grupy ustawień w nowej wersji wtyczki zarządzającej, poprzednio zdefiniowany stan atrybutu  /  dla tej grupy ustawień nie zostanie zmieniony.

Kwestie specjalne podczas używania zaszyfrowanych protokołów do interakcji z zewnętrznymi usługami

Kaspersky Endpoint Security i Kaspersky Security Center używają zaszyfrowanego kanału komunikacji za pośrednictwem protokołu TLS (Transport Layer Security) do pracy z zewnętrznymi usługami Kaspersky. Kaspersky Endpoint Security używa zewnętrznych usług dla następujących funkcji:

- aktualizowanie baz danych i modułów aplikacji;
- aktywowanie aplikacji przy użyciu kodu aktywacyjnego (aktywacja 2.0);
- korzystanie z Kaspersky Security Network.

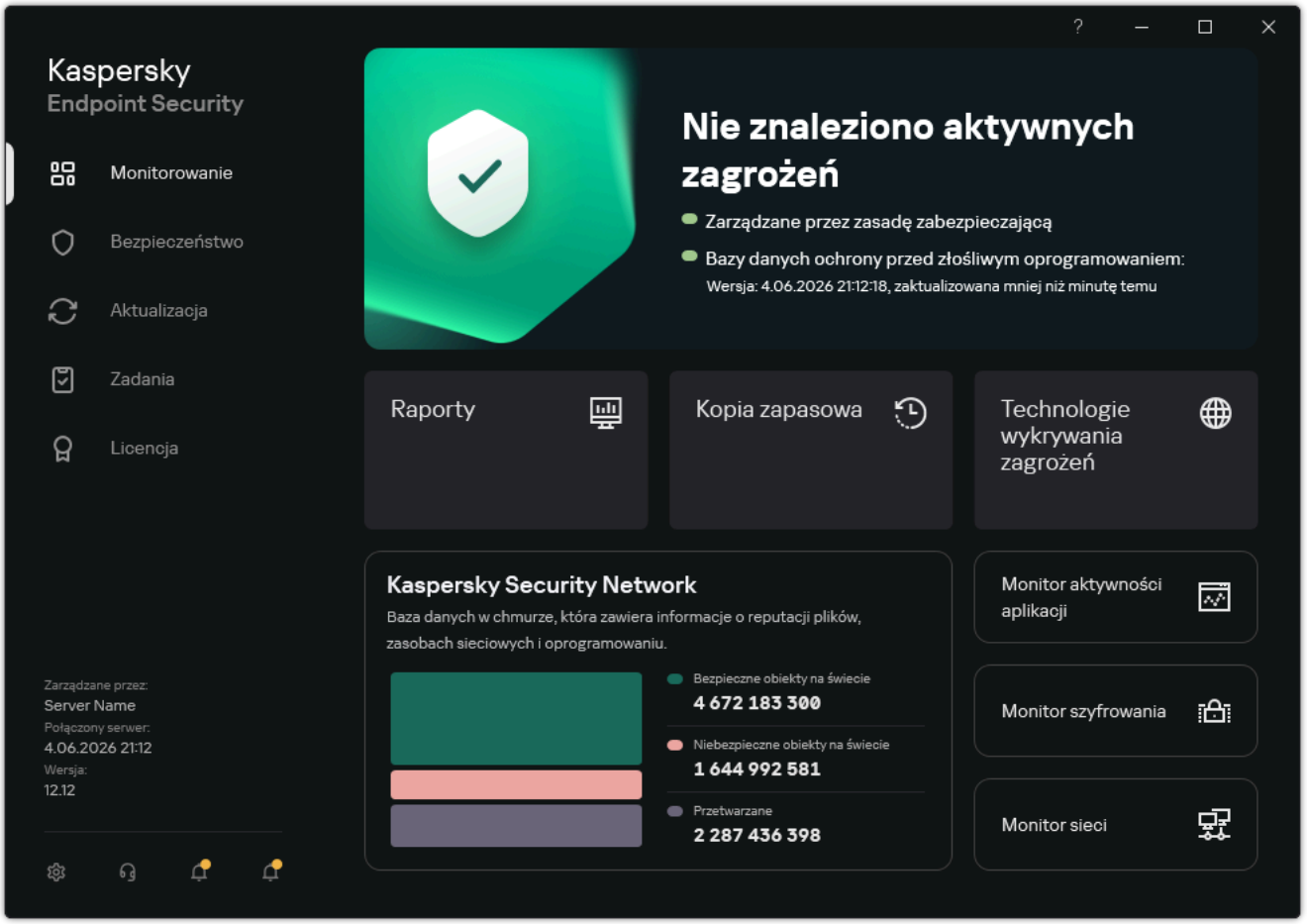
Korzystanie z TLS zabezpiecza aplikację poprzez dostarczenie następujących funkcji:

- Szyfrowanie. Zawartość wiadomości jest poufna i nie zostanie ujawniona innym użytkownikom.
- Integralność. Odbiorca wiadomości jest pewny, że zawartość wiadomości nie została zmodyfikowana od momentu przekazania wiadomości przez nadawcę.
- Autoryzacja. Odbiorca jest pewny, że ta komunikacja została nawiązana tylko z zaufanym serwerem Kaspersky.

Kaspersky Endpoint Security używa certyfikatów kluczy publicznych do autoryzacji na serwerze. Public Key Infrastructure (PKI) jest wymagana do pracy z certyfikatami. Urząd certyfikacji jest częścią PKI. Kaspersky używa swojego własnego Urzędu certyfikacji, ponieważ usługi Kaspersky są czysto publiczne, a nie techniczne. W tym przypadku, jeśli certyfikaty główne Thawte, VeriSign, GlobalTrust i inne zostaną wycofane, Kaspersky PKI będzie działać bez problemów.

Środowiska, które zawierają MITM (narzędzia programowe i sprzętowe, które obsługują analizowanie protokołu HTTPS), są uznawane za niebezpieczne przez Kaspersky Endpoint Security. Podczas pracy z usługami Kaspersky mogą wystąpić błędy. Na przykład, mogą wystąpić błędy dotyczące korzystania z certyfikatu typu Self-Signed Certificate. Te błędy mogą występować, ponieważ narzędzie HTTPS Inspection z Twojego środowiska nie rozpoznaje Kaspersky PKI. Aby rozwiązać te problemy, musisz skonfigurować wykluczenia do interakcji z usługami zewnętrznymi.

Interfejs aplikacji



Okno główne aplikacji

Monitorowanie	• **Raporty**. Przeglądaj zdarzenia, które wystąpiły podczas działania aplikacji, pojedynczych modułów i zadań. • **Kopia zapasowa**. Przeglądaj listę zapisanych kopii zainfekowanych plików, które zostały usunięte przez aplikację. • **Technologie wykrywania zagrożeń**. Przeglądaj informacje o technologiach wykrywania zagrożeń oraz liczbie zagrożeń wykrytych przez te technologie. • **Kaspersky Security Network**. Stan połączenia nawiązanego między Kaspersky Endpoint Security a Kaspersky Security Network oraz globalnych statystyk KSN. *Kaspersky Security Network (KSN)* jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobów sieciowych oraz oprogramowania. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi programu Kaspersky Endpoint Security na nowe zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów. Jeśli uczestniczysz w Kaspersky Security Network, usługi KSN zapewniają Kaspersky Endpoint Security informacje o reputacji przeskanowanych adresów internetowych, a także informacje o kategorii i reputacji przeskanowanych plików. • **Monitor aktywności aplikacji**. Przeglądaj informacje o działaniu zainstalowanych aplikacji. Monitor aktywności aplikacji śledzi pliki, rejestr i zdarzenia systemu operacyjnego związane z aplikacją. • **Monitor sieci**. Przeglądaj informacje o aktywności sieciowej komputera w czasie rzeczywistym. • **Monitor szyfrowania**. Monitoruje proces szyfrowania lub deszyfrowania dysku w czasie rzeczywistym. Monitor szyfrowania jest dostępny, jeśli komponent Kaspersky Disk Encryption lub komponent Szyfrowanie dysków funkcją BitLocker Drive Encryption jest zainstalowany.
Bezpieczeństwo	Stan działania zainstalowanych komponentów. Możesz także przejść do konfigurowania komponentów lub przeglądania raportów.
Aktualizacja	Zarządzaj zadaniami aktualizacji Kaspersky Endpoint Security. Możesz aktualizować antywirusowe bazy danych i moduły aplikacji oraz wycofać ostatnią aktualizację. Administrator może ukryć sekcję przed użytkownikiem lub ograniczyć zarządzanie zadaniem.
Zadania	Zarządzaj zadaniami skanowania Kaspersky Endpoint Security. Możesz uruchomić skanowanie w poszukiwaniu złośliwego oprogramowania i sprawdzanie integralności aplikacji. Administrator może ukrywać zadania przed użytkownikiem lub ograniczyć zarządzanie zadaniami.

Licencja	Licencjonowanie aplikacji. Możesz kupić licencję, aktywować aplikację lub odnowić subskrypcję. Możesz także przejrzeć informacje o bieżącej licencji.
	Konfigurowanie ustawień aplikacji. Administrator może zabronić wprowadzenia zmian w ustawieniach w Kaspersky Security Center.
	Informacje o aplikacji: bieżąca wersja Kaspersky Endpoint Security, data publikacji baz danych, klucz i inne informacje. Możesz przejrzeć zasoby z informacjami firmy Kaspersky, które zawierają przydatne informacje, zalecenia i odpowiedzi na najczęściej zadawane pytania dotyczące zakupu, instalacji i korzystania z aplikacji.
	Wiadomości zawierające informacje o dostępnych aktualizacjach i prośby o dostęp do zaszyfrowanych plików i urządzeń.

Ikona aplikacji w obszarze powiadomień paska zadań

Po zainstalowaniu aplikacji Kaspersky Endpoint Security, w obszarze powiadomień paska zadań Microsoft Windows pojawi się jej ikona.

Jeśli ikona aplikacji w obszarze powiadomień paska zadań jest ukryta, administrator wyłączył wyświetlanie interfejsu aplikacji w zasadzie.

Ikona posiada następujące funkcje:

- Wskazuje aktywność aplikacji.
- Służy jako skrót do menu kontekstowego i okna głównego aplikacji.

Do wyświetlania informacji o działaniu aplikacji dostępne są następujące stany ikony aplikacji:

- Ikona oznacza, że krytycznie ważne składniki ochrony aplikacji są włączone. Kaspersky Endpoint Security wyświetli ostrzeżenie , jeśli użytkownik jest zobowiązany do wykonania akcji, na przykład, uruchomienia ponownie komputera po zaktualizowaniu aplikacji.
- Ikona oznacza, że krytycznie ważne składniki ochrony aplikacji są wyłączone lub działają nieprawidłowo. Składniki ochrony mogą działać nieprawidłowo, na przykład, w przypadku wygaśnięcia licencji lub w wyniku błędu aplikacji. Kaspersky Endpoint Security wyświetli ostrzeżenie z opisem problemu w ochronie komputera.

Menu kontekstowe ikony aplikacji zawiera następujące elementy:

- **Kaspersky Endpoint Security for Windows**. Otwiera okno główne aplikacji. W tym oknie możesz dostosować działania składników i zadań aplikacji oraz przejrzeć statystyki przetworzonych plików i wykrytych zagrożeń.
- **Wstrzymaj ochronę** / **Wznów ochronę**. Wstrzymuje działanie wszystkich składników ochrony i kontroli, które nie są oznaczone kłódką () w profilu. Przed wykonaniem tego działania, zalecane jest wyłączenie profilu Kaspersky Security Center.

  Przed wstrzymaniem działania składników ochrony i kontroli, aplikacja żąda podania hasła dostępu do Kaspersky Endpoint Security (hasło do konta lub hasło tymczasowe). Następnie możesz wybrać czas, na jaki zostanie wstrzymane działanie: dla określonej ilości czasu, aż do ponownego uruchomienia lub na żądanie użytkownika.

  Ten element menu kontekstowego jest dostępny, jeśli ochrona hasłem jest włączona. Aby wznowić działanie składników ochrony i kontroli, w menu kontekstowym aplikacji kliknij **Wznów ochronę**.

  Wstrzymanie działania składników ochrony i kontroli nie wpływa na wydajność zadań aktualizacji i skanowania w poszukiwaniu złośliwego oprogramowania. Aplikacja będzie też dalej korzystała z Kaspersky Security Network.

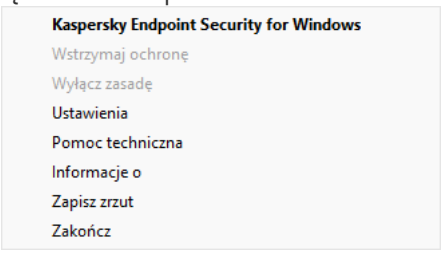
- **Wyłącz zasadę** / **Włącz zasadę**. Wyłączanie zasady Kaspersky Security Center na komputerze. Wszystkie ustawienia Kaspersky Endpoint Security są dostępne do konfiguracji, włącznie z ustawieniami, które mają zamkniętą kłódkę w profilu (). Jeśli zasada jest wyłączona, aplikacja żąda podania hasła dostępu do Kaspersky Endpoint Security (hasło do konta lub hasło tymczasowe). Ten element menu kontekstowego jest dostępny, jeśli ochrona hasłem jest włączona. Aby włączyć zasadę, w menu kontekstowym aplikacji wybierz **Włącz zasadę**.

- **Ustawienia**. Otwiera okno ustawień aplikacji.

- **Pomoc techniczna**. To powoduje otwarcie okna zawierającego informacje niezbędne do skontaktowania się z pomocą techniczną Kaspersky.

- **Informacje o**. Element ten otwiera okno informacyjne zawierające szczegółowe dane o aplikacji.

- **Zakończ**. Element ten zamyka Kaspersky Endpoint Security. Kliknięcie tego elementu menu kontekstowego powoduje wyładowanie aplikacji z pamięci RAM komputera.



Menu kontekstowe ikony aplikacji

Uproszczony interfejs aplikacji

Jeśli profil Kaspersky Security Center skonfigurowany do wyświetlania uproszczonego interfejsu aplikacji jest stosowany na komputerze klienckim, na którym jest zainstalowany Kaspersky Endpoint Security, okno główne aplikacji nie jest dostępne na tym komputerze klienckim. Kliknij ikonę Kaspersky Endpoint Security (patrz rysunek poniżej) prawym klawiszem myszy, aby otworzyć menu kontekstowe zawierające następujące elementy:

- **Wyłącz zasadę** / **Włącz zasadę**. Wyłączanie zasady Kaspersky Security Center na komputerze. Wszystkie ustawienia Kaspersky Endpoint Security są dostępne do konfiguracji, włącznie z ustawieniami, które mają zamkniętą kłódkę w profilu (). Jeśli zasada jest wyłączona, aplikacja żąda podania hasła dostępu do Kaspersky Endpoint Security (hasło do konta lub hasło tymczasowe). Ten element menu kontekstowego jest dostępny, jeśli ochrona hasłem jest włączona. Aby włączyć zasadę, w menu kontekstowym aplikacji wybierz **Włącz zasadę**.

- **Zadania**. Lista rozwijalna zawierająca następujące elementy:

  - **Sprawdzanie integralności aplikacji**.

  - **Wycofywanie baz danych do ich poprzedniej wersji**.

  - **Pełne skanowanie**.

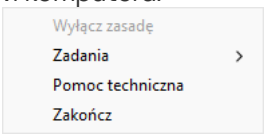
  - **Skanowanie niestandardowe**.

  - **Skanowanie obszarów krytycznych**.

  - **Aktualizacja**.

- **Pomoc techniczna**. To powoduje otwarcie okna zawierającego informacje niezbędne do skontaktowania się z pomocą techniczną Kaspersky.

- **Zakończ**. Element ten zamyka Kaspersky Endpoint Security. Kliknięcie tego elementu menu kontekstowego powoduje wyładowanie aplikacji z pamięci RAM komputera.



Menu kontekstowe ikony aplikacji podczas wyświetlania uproszczonego interfejsu

Konfigurowanie wyświetlania interfejsu aplikacji

Możesz skonfigurować tryb wyświetlania interfejsu aplikacji dla użytkownika. Użytkownik może wchodzić w interakcje z aplikacją na następujące sposoby:

- **Wyświetl uproszczony interfejs**. Na komputerze klienckim okno główne aplikacji jest niedostępne, a dostępna jest tylko ikona w obszarze powiadomień systemu Windows. W menu kontekstowym ikony użytkownik może przeprowadzić ograniczoną liczbę operacji na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetla nad ikoną aplikacji tylko powiadomienia wymagające podjęcia działania przez użytkownika.

- **Wyświetl interfejs użytkownika**. Na komputerze klienckim dostępne są: okno główne Kaspersky Endpoint Security oraz ikona w obszarze powiadomień systemu Windows. W menu kontekstowym ikony użytkownik może przeprowadzić operacje na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetli także powiadomienia nad ikoną aplikacji.

- **Nie wyświetlaj interfejsu użytkownika**. Na komputerze klienckim nie są wyświetlane żadne działania Kaspersky Endpoint Security. Ikona w obszarze powiadomień systemu Windows oraz powiadomienia nie są dostępne.

Jak skonfigurować tryb wyświetlania interfejsu aplikacji w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Ustawienia ogólne** → **Interfejs**.

4. W sekcji **Interakcja z użytkownikiem** skonfiguruj sposób wyświetlania interfejsu aplikacji:

   - **Wyświetl interfejs użytkownika**. Na komputerze klienckim dostępne są: okno główne Kaspersky Endpoint Security oraz ikona w obszarze powiadomień systemu Windows. W menu kontekstowym ikony użytkownik może przeprowadzić operacje na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetli także powiadomienia nad ikoną aplikacji. W razie potrzeby możesz włączyć funkcjonalność **Ukryj sekcję Monitor aktywności aplikacji**, aby ukryć dane dotyczące aktywności aplikacji na komputerze, co ograniczy dostęp użytkownika do narzędzia Monitor aktywności aplikacji.

   - **Wyświetl uproszczony interfejs**. Na komputerze klienckim okno główne aplikacji jest niedostępne, a dostępna jest tylko ikona w obszarze powiadomień systemu Windows. W menu kontekstowym ikony użytkownik może przeprowadzić ograniczoną liczbę operacji na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetla nad ikoną aplikacji tylko powiadomienia wymagające podjęcia działania przez użytkownika.

   - **Nie wyświetlaj interfejsu użytkownika**. Na komputerze klienckim nie są wyświetlane żadne działania Kaspersky Endpoint Security. Ikona w obszarze powiadomień systemu Windows oraz powiadomienia nie są dostępne.

5. Zapisz swoje zmiany.

Jak skonfigurować tryb wyświetlania interfejsu aplikacji w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Interakcja użytkownika**.
5. W sekcji **Widoczność dla użytkowników** skonfiguruj sposób wyświetlania interfejsu aplikacji:

   - **Wyświetl interfejs użytkownika**. Gdy ta funkcjonalność jest wyłączona, na komputerze klienckim nie są wyświetlane żadne oznaki działania programu Kaspersky Endpoint Security. Ikona w obszarze powiadomień systemu Windows oraz powiadomienia nie są dostępne.
   - **Uproszczone**. Na komputerze klienckim okno główne aplikacji jest niedostępne, a dostępna jest tylko ikona w obszarze powiadomień systemu Windows. W menu kontekstowym ikony użytkownik może przeprowadzić ograniczoną liczbę operacji na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetla nad ikoną aplikacji tylko powiadomienia wymagające podjęcia działania przez użytkownika.
   - **Pełne**. Na komputerze klienckim dostępne są: okno główne Kaspersky Endpoint Security oraz ikona w obszarze powiadomień systemu Windows. W menu kontekstowym ikony użytkownik może przeprowadzić operacje na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetli także powiadomienia nad ikoną aplikacji.
   - **Ukryj sekcję Monitor aktywności aplikacji**. Jeśli chcesz ukryć informacje o aktywności aplikacji na komputerze użytkownika, możesz ograniczyć dostęp użytkownika do narzędzia Monitor aktywności aplikacji.
6. Zapisz swoje zmiany.

Przygotowanie aplikacji do użytku

Po zainstalowaniu aplikacji na komputerach klienckich, aby pracować z Kaspersky Endpoint Security z poziomu Kaspersky Security Center Web Console należy wykonać następujące czynności:

- Utworzyć i skonfigurować profil.

  Istnieje możliwość wykorzystania profili do wprowadzenia identycznych ustawień programu Kaspersky Endpoint Security na wszystkich komputerach klienckich należących do grupy administracyjnej. Kreator wstępnej konfiguracji programu Kaspersky Security Center automatycznie tworzy zasadę dla Kaspersky Endpoint Security.
- Utwórz zadania *Aktualizacja baz danych i modułów aplikacji* oraz *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

  Zadanie *Aktualizacja baz danych i modułów aplikacji* jest wymagane do zapewnienia aktualnej ochrony komputera. Podczas wykonywania zadania Kaspersky Endpoint Security aktualizuje antywirusowe bazy danych i moduły. Zadanie *Aktualizacja baz danych i modułów aplikacji* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja baz danych i modułów aplikacji*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

  Zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* jest wymagane do natychmiastowego wykrywania wirusów i innych szkodliwych programów. Należy ręcznie utworzyć zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

Jak utworzyć zadanie Skanowanie w poszukiwaniu złośliwego oprogramowania w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Skanowanie w poszukiwaniu złośliwego oprogramowania**.

Krok 2. Obszar skanowania

Utwórz listę obiektów, które będą skanowane przez Kaspersky Endpoint Security podczas uruchamiania zadania skanowania.

Krok 3. Działanie Kaspersky Endpoint Security

Wybierz akcję po wykryciu zagrożenia:

- **Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik.

- **Wylecz; poinformuj, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeśli leczenie się nie powiedzie, Kaspersky Endpoint Security doda informacje o wykrytych zainfekowanych plikach do listy aktywnych zagrożeń.

- **Poinformuj**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików.

- **Uruchom natychmiast Zaawansowane leczenie**. Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security wykorzystuje technologię zaawansowanego leczenia do leczenia aktywnych zagrożeń podczas skanowania.

  Technologia zaawansowanego leczenia służy do usuwania z systemu operacyjnego szkodliwych aplikacji, które już uruchomiły swoje procesy w pamięci RAM i nie pozwalają aplikacji Kaspersky Endpoint Security na usunięcie ich przy pomocy innych metod. W rezultacie zagrożenie zostanie zneutralizowane. W trakcie działania Zaawansowanego leczenia zaleca się nie uruchamiać nowych procesów ani nie modyfikować rejestru systemu operacyjnego. Technologia zaawansowanego leczenia wykorzystuje dużą ilość zasobów systemu operacyjnego, co może spowolnić inne aplikacje. Po zakończeniu zaawansowanego leczenia, Kaspersky Endpoint Security uruchomi ponownie komputer bez pytania użytkownika o potwierdzenie.

- **Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności**. Odroczono uruchomienie zadania, gdy zasoby komputera są zajęte. Kaspersky Endpoint Security uruchamia zadanie skanowania, jeśli komputer jest zablokowany lub wygaszacz ekranu jest włączony. Jeśli przerwałeś wykonywanie zadania, na przykład, poprzez odblokowanie komputera, Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane. Ta opcja terminarza umożliwia zaoszczędzenie zasobów komputera w trakcie korzystania z komputera.

Krok 4. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.

- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 5. Wybieranie konta do uruchomienia zadania

Wybierz konto, aby uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika. Jeśli obszar skanowania obejmuje dyski sieciowe lub inne obiekty z ograniczonym dostępem, wybierz konto użytkownika z wystarczającymi uprawnieniami dostępu.

Krok 6. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz uruchamiania zadania, na przykład, ręcznie lub po pobraniu antywirusowych baz danych do repozytorium.

Krok 7. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład *Codzienne pełne skanowanie*.

Krok 8. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania. W wyniku tego działania zadanie Skanowanie antywirusowe zostanie wykonane na komputerach użytkowników zgodnie z określonym terminarzem.

Jak utworzyć zadanie Skanowanie w poszukiwaniu złośliwego oprogramowania w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Skanowanie w poszukiwaniu złośliwego oprogramowania**.

   c. W polu **Nazwa zadania** wpisz krótki opis, na przykład *Cotygodniowe skanowanie*.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.

5. Wybierz konto do uruchomienia zadania. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika.

6. Zakończ działanie Kreatora.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Aby skonfigurować terminarz zadania, przejdź do właściwości zadania.

   Zalecane jest skonfigurowanie terminarza uruchamiania zadania przynajmniej raz w tygodniu.

8. Zaznacz pole obok zadania.

9. Kliknij **Uruchom**.

   Możesz monitorować stan zadania oraz liczbę urządzeń, na których to zadanie zostało wykonane pomyślnie lub zakończyło się błędem.

W wyniku tego działania zadanie Skanowanie antywirusowe zostanie wykonane na komputerach użytkowników zgodnie z określonym terminarzem.

- Zoptymalizuj wydajność Kaspersky Endpoint Security.

Zarządzanie profilami

Profil to zbiór ustawień aplikacji określonych dla grupy administracyjnej. Możesz skonfigurować kilka profili z różnymi wartościami dla jednej aplikacji. Aplikacja może działać z różnymi ustawieniami dla różnych grup administracyjnych. Każda grupa administracyjna może posiadać swój własny profil dla aplikacji.

Każde ustawienie zasad ma atrybut („kłódka"). Status tego atrybutu decyduje o tym, czy ustawienie zostanie przekazane do zarządzanych urządzeń w grupie administracyjnej:

- Jeżeli „kłódka" jest otwarta ( ), wartość tego ustawienia nie zostanie przekazana do zarządzanych urządzeń. Ustawienie to będzie można modyfikować w lokalnym interfejsie aplikacji. Takie ustawienia są określane jako *odblokowane*.

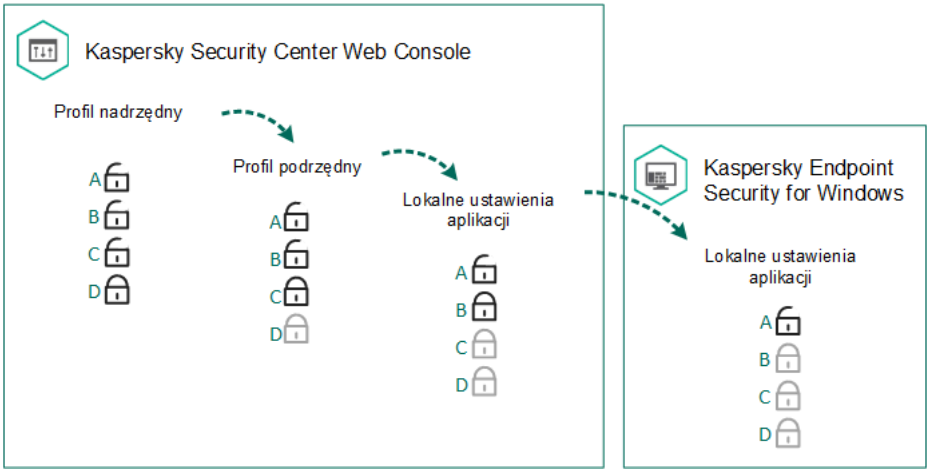
- Jeżeli „kłódka" jest zamknięta ( ), wartość tego ustawienia zostanie przekazana i zastosowana do zarządzanych urządzeń. Takie ustawienia są określane jako *zablokowane*. Ustawień zablokowanych nie można modyfikować w lokalnym interfejsie aplikacji.

Ustawienia profilu są wysyłane na komputery kliencki przez Agenta sieciowego podczas *synchronizacji*. Domyślnie, Serwer administracyjny przeprowadza synchronizację natychmiast po zmianie ustawień profilu. Port UDP o numerze 15000 na komputerze klienckim jest używany do synchronizacji. Domyślnie, Serwer administracyjny przeprowadza synchronizację co każde 15 minut. Jeśli po zmianie ustawień profilu synchronizacja się nie powiedzie, kolejna próba synchronizacji zostanie podjęta zgodnie ze skonfigurowanym terminarzem.

Dziedziczenie ustawień

Zasady, podobnie jak grupy administracyjne, są ułożone w hierarchię. *Zasada potomna* to zasada dla zagnieżdżonych poziomów hierarchii, czyli zasada dla zagnieżdżonych grup administracyjnych i podrzędnych Serwerów administracyjnych.

Domyślnie zasada potomna dziedziczy ustawienia z zasady nadrzędnej. Jeśli ustawienie w zasadzie nadrzędnej ma atrybut („kłódka" zamknięta), wówczas w zasadach potomnych i lokalnych ustawieniach aplikacji wartość tego ustawienia zostanie zastąpiona zgodnie z zasadą nadrzędną, a ustawienie zostanie zablokowane. W razie potrzeby można wyłączyć dziedziczenie ustawień z zasady nadrzędnej. Profile użytkowników mobilnych nie oddziałują na inne profile poprzez hierarchię grup administracyjnych.



Dziedziczenie ustawień

Uprawnienia dostępu do ustawień profilu (odczyt, zapis, wykonanie) są definiowane dla każdego użytkownika, który posiada dostęp do Serwera administracyjnego Kaspersky Security Center, oraz oddzielnie dla każdego obszaru funkcyjnego Kaspersky Endpoint Security. Aby skonfigurować prawa dostępu do ustawień zasad, przejdź do sekcji **Zabezpieczenia** okna właściwości serwera administracyjnego Kaspersky Security Center (domyślnie ta sekcja jest ukryta w interfejsie konsoli).

Korekty zasad

Kaspersky Security Center śledzi zmiany w zasadach i tworzy korekty. *Korekta* jest zbiorem zmodyfikowanych parametrów zapisanych przez użytkownika. Korekty umożliwiają porównywanie i cofanie zmian w parametrach zasad. Oprócz zestawu zmodyfikowanych parametrów korekta obejmuje informacje o użytkowniku, który wprowadził zmiany, a także czas, adres IP, komentarz użytkownika i inne istotne dane.

Aby wyświetlić dziennik korekt, otwórz właściwości zasady i przejdź do sekcji **Historia rewizji**. Więcej informacji o pracy z korektami znajdziesz w pomocy do Kaspersky Security Center.

Tworzenie profilu

Podczas tworzenia zasad kreator sugeruje ustawienia istotne dla wybranego trybu. Na przykład w przypadku trybu Light Agent należy dodać serwer ochrony (SVM). Używając aplikacji do ochrony serwera SQL, musisz dodać wstępnie zdefiniowane wykluczenia ze skanowania, aby mieć pewność, że działanie serwera nie zostanie zakłócone. Po wybraniu trybu kreator proponuje odpowiednie ustawienia zasad. Następnie możesz edytować te ustawienia we właściwościach zasad.

Jak utworzyć zasadę w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej wybierz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Zasady**.
4. Kliknij **Nowa zasada**.

   Zostanie uruchomiony Kreator tworzenia profilu
5. Postępuj zgodnie z instrukcjami Kreatora tworzenia profilu.

Krok 1. Wybieranie aplikacji w celu utworzenia zasad grupy

Wybierz aplikację **Kaspersky Endpoint Security for Windows (14.1)**.

Krok 2. Nadawanie nazwy zasadom grupy

Wprowadź nazwę zasad grupy, na przykład: *Zasady dla biura*.

Przy użyciu kreatora zasad można również tworzyć nowe zasady na podstawie istniejących. Aby to zrobić, podczas określania nazwy zasad grupy zaznacz pole **Użyj ustawień zasady dla wcześniejszej wersji aplikacji**. Kreator umożliwia również utworzenie zasad Kaspersky Endpoint Security (KES) na podstawie zasad innego rozwiązania, np. Kaspersky Security for Windows Server (KSWS) lub Kaspersky Security for Virtualization Light Agent for Windows.

Krok 3. Uczestnictwo w Kaspersky Security Network

Przeczytaj i zaakceptuj warunki Oświadczenia Kaspersky Security Network (KSN).

Krok 4. Wybieranie trybu użytkowania aplikacji na komputerach

Możesz skonfigurować zasady dla następujących trybów aplikacji Kaspersky Endpoint Security w zależności od jej przeznaczenia:

- Standardowy tryb ochrony hostów

  W tym trybie możesz wybrać sposób konfiguracji zasad:

  - **Utwórz zasadę z ustawieniami domyślnymi**. Domyślne ustawienia są uznawane za optymalne. Te ustawienia są zalecane przez ekspertów z Kaspersky. Domyślne ustawienia zawierają zalecany poziom ochrony i optymalne zużycie zasobów.

  - **Zmień ustawienia zasady w kreatorze**. Ta metoda umożliwia zarządzanie ustawieniami zasad krok po kroku w kreatorze. Możesz również zarządzać ustawieniami zasad za pomocą pliku konfiguracyjnego aplikacji (patrz następny krok).

- Endpoint Detection and Response Agent do ochrony przed zaawansowanymi zagrożeniami i atakami ukierunkowanymi.

  Endpoint Detection and Response Agent to aplikacja instalowana na poszczególnych stacjach roboczych i serwerach w infrastrukturze informatycznej organizacji w celu obsługi rozwiązań Detection and Response firmy Kaspersky. W następnym kroku musisz wybrać rozwiązanie do integracji EDR Agent.

- Klient Light Agent do ochrony środowisk wirtualnych.

  Aby korzystać z aplikacji w trybie Light Agent, należy skonfigurować połączenie z maszyną wirtualną SVM. Ustawienia te są wymagane, aby aplikacja mogła działać w trybie Light Agent.

Kaspersky Endpoint Security zapewnia wspólną zasadę dla wszystkich trybów aplikacji i typów systemów operacyjnych. Oznacza to, że dana zasada obejmuje cały zestaw ustawień. Aplikacja może jednak ignorować niektóre ustawienia zasad, ponieważ rozwiązanie Kaspersky Endpoint Security zostało wdrożone w trybie, w którym pewne funkcje są niedostępne. Na przykład podczas korzystania z aplikacji w trybie Endpoint Detection and Response Agent dostępne są tylko ustawienia istotne dla integracji z rozwiązaniami Kaspersky Detection and Response oraz integracji z platformą KUMA.

Zalecamy używanie różnych zasad do różnych trybów i typów systemów operacyjnych.

Krok 5. Importowanie ustawień

Ten krok będzie dostępny, jeśli w kroku 4 wybrano ręczną konfigurację zasady.

Możesz utworzyć zasadę na podstawie ustawień Kaspersky Endpoint Security z pliku konfiguracyjnego CFG. Kreator nie ma dostępu do wszystkich ustawień zasady podczas importowania pliku konfiguracji aplikacji. W ustawieniach aplikacji brakuje na przykład profili zasad. Jeśli chcesz przenieść wszystkie ustawienia i profile do zasady, możesz zaimportować inną zasadę z pliku KLP.

Podczas importowania pliku konfiguracyjnego Kaspersky Endpoint Security nie przesyła haseł do kontenerów kryptograficznych. Jeśli łączysz się z serwerami za pomocą uwierzytelniania dwukierunkowego, musisz od podstaw określić hasła do kontenerów kryptograficznych.

Krok 6-10. Konfiguracja ustawień zasad

Ten krok będzie dostępny, jeśli w kroku 4 wybrano ręczną konfigurację zasady.

Wykonaj poniższe kroki, aby zarządzać ustawieniami zasad.

Krok 11. Konfigurowanie strefy zaufanej

Skonfiguruj strefę zaufaną. Możesz dodać predefiniowane wykluczenia ze skanowania i zaufane aplikacje. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach. Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje mogą także pomóc w szybkiej konfiguracji Kaspersky Endpoint Security w trybie Light Agent w środowiskach wirtualnych Citrix i VMware.

Krok 12. Wybór statusu zasady

- **Aktywny**. Po kolejnej synchronizacji, profil zostanie uzyty jako profil aktywny.

  Ustawienia aktywnego profilu zostaną zapisane na komputerach klienckich podczas synchronizacji. Nie możesz stosować jednocześnie kilku profili na jednym komputerze, dlatego tylko jeden profil może być aktywny w każdej grupie.

- **Nieaktywny**. Profil Kopii zapasowej. Jeśli to konieczne, profil nieaktywny może zostać przełączony w stan aktywny.

  Możesz utworzyć nieograniczoną liczbę nieaktywnych profili. Profil nieaktywny nie wpływa na ustawienia aplikacji na komputerach w sieci. Profile nieaktywne są przeznaczone do sytuacji wyjątkowych, takich jak atak wirusa. Jeśli dojdzie do ataku za pośrednictwem dysków flash, możesz aktywować profil, który blokuje dostęp do dysków flash. W tym przypadku profil aktywny automatycznie staje się nieaktywny.

- **Użytkownik mobilny**. Profil jest aktywowany, gdy komputer opuści sieć obwodową organizacji.

Zakończ działanie kreatora.

Jak utworzyć zasadę w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia profilu
3. Wybierz Kaspersky Endpoint Security i kliknij **Dalej**.
4. Przeczytaj i zaakceptuj warunki Oświadczenia Kaspersky Security Network (KSN) i kliknij **Dalej**.
5. Wybierz tryb działania aplikacji:

   - Tryb standardowy do ochrony stacji roboczych i serwerów
   - Endpoint Detection and Response Agent do ochrony przed zaawansowanymi zagrożeniami i atakami ukierunkowanymi.

     Wybierając ten tryb, możesz utworzyć zasady na potrzeby integracji komputera z rozwiązaniami Kaspersky Detection and Response. Kreator poprosi o skonfigurowanie integracji z Kaspersky Managed Detection and Response, a następnie z Kaspersky Anti Targeted Attack Platform (EDR).
   - Light Agent do ochrony środowisk wirtualnych.

     Jeśli wybierzesz ten tryb, w następnym kroku trzeba będzie skonfigurować połączenie z serwerem ochrony (SVM). Ustawienia te są wymagane, aby aplikacja mogła działać w trybie Light Agent.

   Kaspersky Endpoint Security zapewnia wspólną zasadę dla wszystkich trybów aplikacji i typów systemów operacyjnych. Oznacza to, że dana zasada obejmuje cały zestaw ustawień. Aplikacja może jednak ignorować niektóre ustawienia zasad, ponieważ rozwiązanie Kaspersky Endpoint Security zostało wdrożone w trybie, w którym pewne funkcje są niedostępne. Na przykład podczas korzystania z aplikacji w trybie Endpoint Detection and Response Agent dostępne są tylko ustawienia istotne dla integracji z rozwiązaniami Kaspersky Detection and Response oraz integracji z platformą KUMA.

   > Zalecamy używanie różnych zasad do różnych trybów i typów systemów operacyjnych.
6. Skonfiguruj strefę zaufaną. Możesz dodać predefiniowane wykluczenia ze skanowania i zaufane aplikacje. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach. Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje mogą także pomóc w szybkiej konfiguracji Kaspersky Endpoint Security w trybie Light Agent w środowiskach wirtualnych Citrix i VMware.

7. Na zakładce **Ogólne** możesz wykonać następujące działania:

- Zmień nazwę profilu.
- Wybierz stan profilu:
  - **Aktywny**. Po kolejnej synchronizacji, profil zostanie uzyty jako profil aktywny.

    Ustawienia aktywnego profilu zostaną zapisane na komputerach klienckich podczas synchronizacji. Nie możesz stosować jednocześnie kilku profili na jednym komputerze, dlatego tylko jeden profil może być aktywny w każdej grupie.
  - **Nieaktywny**. Profil Kopii zapasowej. Jeśli to konieczne, profil nieaktywny może zostać przełączony w stan aktywny.

    Możesz utworzyć nieograniczoną liczbę nieaktywnych profili. Profil nieaktywny nie wpływa na ustawienia aplikacji na komputerach w sieci. Profile nieaktywne są przeznaczone do sytuacji wyjątkowych, takich jak atak wirusa. Jeśli dojdzie do ataku za pośrednictwem dysków flash, możesz aktywować profil, który blokuje dostęp do dysków flash. W tym przypadku profil aktywny automatycznie staje się nieaktywny.
  - **Użytkownik mobilny**. Profil jest aktywowany, gdy komputer opuści sieć obwodową organizacji.
- Skonfiguruj dziedziczenie ustawień:
  - **Dziedzicz ustawienia z zasady nadrzędnej**. Jeśli ten przełącznik zostanie ustawiony w pozycji włączenia, wartości ustawień profilu będą dziedziczone z profilu najwyższego poziomu hierarchii. Ustawienia profilu nie mogą być edytowane, jeśli dla profilu nadrzędnego ustawiono .
  - **Wymuś dziedziczenie ustawień w zasadach podrzędnych**. Jeśli przełącznik jest ustawiony w pozycji włączenia, wartości ustawień profilu zostaną przeniesione do profili potomnych. We właściwościach zasady podrzędnej przycisk przełączania **Dziedzicz ustawienia z zasady nadrzędnej** zostanie automatycznie włączony i nie można go wyłączyć. Ustawienia profilu potomnego są dziedziczone z profilu nadrzędnego, za wyjątkiem ustawień oznaczonych . Ustawienia profilu potomnego nie mogą być edytowane, jeśli dla profilu nadrzędnego ustawiono .

8. Na zakładce **Ustawienia aplikacji** możesz skonfigurować ustawienia zasad Kaspersky Endpoint Security.

9. Zakończ działanie kreatora.

W wyniku tego działania ustawienia programu Kaspersky Endpoint Security zostaną skonfigurowane na komputerach klienckich podczas kolejnej synchronizacji. Możesz wyświetlić informacje o zasadzie stosowanej na komputerze w interfejsie Kaspersky Endpoint Security, klikając przycisk w oknie głównym (na przykład, nazwę zasady). Aby to zrobić, w ustawieniach zasady Agenta sieciowego należy włączyć odbiór rozszerzonych danych zasad. Więcej informacji na temat zasady Agenta sieciowego można znaleźć w pomocy do Kaspersky Security Center.

Eksportowanie i importowanie zasad

Kaspersky Endpoint Security umożliwia eksportowanie zasad wraz z ustawieniami i profilami do pliku KLP. Następnie można użyć funkcji eksportowania/importowania zasad, aby utworzyć ich kopię zapasową, przenieść je na inny serwer lub, na przykład, przenieść zasady z Kaspersky Security Center Windows do Kaspersky Security Center Linux. Szczegółowe informacje na temat zarządzania zasadami znajdują się w pomocy Kaspersky Security Center.

Jak eksportować i importować zasady w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Zasady**.
4. Aby wyeksportować zasadę:
   a. Kliknij zasadę, którą chcesz wyeksportować.
   b. Kliknij łącze **Eksportuj zasadę do pliku** znajdujące się w prawej części okna.
   c. W otwartym oknie określ nazwę pliku KLP, do którego chcesz wyeksportować zasadę, i wybierz folder, w którym chcesz zapisać ten plik.
   d. Zapisz plik.
5. Aby zaimportować zasadę:
   a. Kliknij **Importuj zasadę z pliku**.
   b. W otworzonym oknie wybierz plik KLP zasady, którą chcesz zaimportować.
   c. Otwórz plik.

   To działanie dodaje nową zasadę o statusie *Zasada nieaktywna*.

Eksportowanie i importowanie zasad w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Aby wyeksportować zasadę:
   a. Zaznacz pole wyboru obok zasady, którą chcesz wyeksportować.
   b. Kliknij przycisk **Eksportuj**.
   c. W otwartym oknie określ nazwę pliku KLP, do którego chcesz wyeksportować zasadę, i wybierz folder, w którym chcesz zapisać ten plik.
   d. Zapisz plik.
3. Aby zaimportować zasadę:
   a. Kliknij **Importuj**.
   b. Wybierz plik KLP zasady, którą chcesz zaimportować.
   c. Po pomyślnym przetworzeniu zasady wybierz grupę administracyjną, do której chcesz ją zastosować.
   d. Kliknij przycisk **Zakończone**, aby zakończyć importowanie zasady.

   To działanie dodaje nową zasadę o statusie *Nieaktywny*.

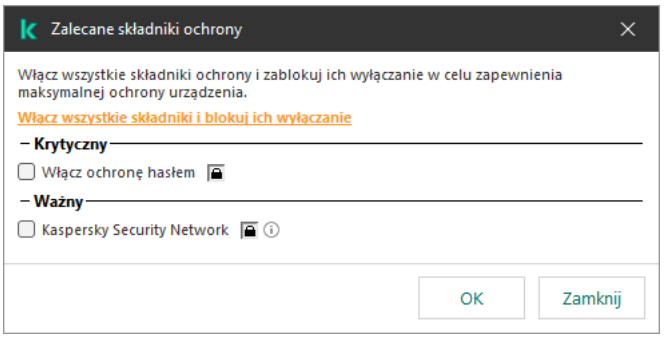
Wskaźnik poziomu ochrony

Wskaźnik poziomu ochrony jest wyświetlany w górnej części okna właściwości zasady. Wskaźnik może przyjąć jedną z następujących wartości:

- **Wysoki poziom ochrony**. Wskaźnik przyjmuje tę wartość oraz kolor zielony, jeśli włączone są wszystkie komponenty z następujących kategorii:
  - **Krytyczny**. Ta kategoria zawiera następujące komponenty:
    - Ochrona plików.
    - Wykrywanie zachowań.
    - Ochrona przed exploitami.
    - Silnik korygujący.
    - Ochrona usług aplikacji przed zewnętrznym zarządzaniem.
  - **Ważny**. Ta kategoria zawiera następujące komponenty:
    - Kaspersky Security Network.
    - Ochrona WWW.
    - Ochrona poczty.
    - Ochrona przed włamaniami.
    - Ochrona hasłem.
- **Średni poziom ochrony**. Wskaźnik przyjmuje tę wartość i staje się żółty, jeśli wyłączony jest jeden z ważnych komponentów.
- **Niski poziom ochrony**. Wskaźnik przyjmuje tę wartość i staje się czerwony w jednej z następujących sytuacji:
  - Wyłączony jest jeden lub kilka krytycznych komponentów.
  - Wyłączony jest jeden lub kilka ważnych komponentów.

Jeśli wskaźnik jest wyświetlany z wartością **Średni poziom ochrony** lub **Niski poziom ochrony**, po prawej stronie wskaźnika pojawi się odnośnik, który otwiera okno **Zalecane składniki ochrony**. W tym oknie możesz włączyć dowolne z zalecanych składników ochrony.

Po uaktualnieniu aplikacji wskaźnik poziomu ochrony może wskazywać niższy poziom ochrony niż przed uaktualnieniem. Dzieje się tak, ponieważ nowsza wersja aplikacji wprowadza nowe komponenty lub funkcje, które są ważne dla bezpieczeństwa komputera. Po uaktualnieniu aplikacji należy zarządzać nowymi ustawieniami, aby mieć pewność, że poziom ochrony pozostanie wysoki.



Wskaźnik poziomu ochrony zasad

Zarządzanie zadaniami

Możesz utworzyć następujące typy zadań do zarządzania Kaspersky Endpoint Security poprzez Kaspersky Security Center:

- Zadania lokalne konfigurowane dla każdego komputera klienckiego oddzielnie.
- Zadania grupowe konfigurowane dla komputerów klienckich w grupach administracyjnych.
- Zdania dla wyboru komputerów.

Można utworzyć dowolną liczbę zadań grupowych, zadań dla wyborów komputerów oraz zadań lokalnych. Szczegółowe informacje na temat pracy z grupami administracyjnymi i wyborami komputerów można znaleźć w pomocy do Kaspersky Security Center.

Kaspersky Endpoint Security obsługuje następujące zadania:

- **Skanowanie w poszukiwaniu złośliwego oprogramowania**. Kaspersky Endpoint Security skanuje obszary komputera, określone w ustawieniach zadania, w poszukiwaniu wirusów i innych zagrożeń. Zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* jest wymagane do działania Kaspersky Endpoint Security i jest tworzone podczas działania Kreatora wstępnej konfiguracji. Zalecane jest skonfigurowanie terminarza uruchamiania zadania przynajmniej raz w tygodniu.
- **Dodaj klucz**. Kaspersky Endpoint Security dodaje klucz do aktywowania aplikacji, w tym klucz dodatkowy. Przed uruchomieniem zadania upewnij się, że liczba komputerów, na których zadanie ma zostać wykonane, nie przekracza liczby komputerów dozwolonych przez licencję.
- **Zmiana składników aplikacji**. Kaspersky Endpoint Security instaluje lub usuwa komponenty na komputerach klienckich zgodnie z listą komponentów określonych w ustawieniach zadania. Moduł Ochrona plików nie może zostać usunięty. Optymalny zestaw komponentów Kaspersky Endpoint Security pomaga oszczędzić zasoby komputera.
- **Inwentaryzacja**. Kaspersky Endpoint Security zbiera informacje o wszystkich plikach wykonywalnych aplikacji, które są przechowywane na komputerach. Zadanie *Inwentaryzacja* jest wykonywane przez komponent Kontrola aplikacji. Jeśli komponent Kontrola aplikacji nie jest zainstalowany, zadanie zakończy się błędem.
- **Aktualizacja baz danych i modułów aplikacji**. Kaspersky Endpoint Security zaktualizuje bazy danych i moduły aplikacji. Zadanie *Aktualizacja baz danych i modułów aplikacji* jest wymagane do działania Kaspersky Endpoint Security i jest tworzone podczas działania Kreatora wstępnej konfiguracji. Zalecane jest skonfigurowanie terminarza, który uruchamia zadanie przynajmniej raz dziennie.

- **Wyczyść dane**. Kaspersky Endpoint Security usuwa pliki i foldery z komputerów użytkowników od razu lub jeśli nie ma połączenia z Kaspersky Security Center przez dłuższy czas.
- **Wycofywanie aktualizacji**. Kaspersky Endpoint Security wycofuje ostatnią aktualizację baz danych i modułów aplikacji. Może to być konieczne, jeśli, na przykład, nowe bazy danych zawierają niepoprawne dane, które mogłyby spowodować, że Kaspersky Endpoint Security zablokuje bezpieczną aplikację.
- **Sprawdzanie integralności aplikacji**. Kaspersky Endpoint Security analizuje pliki aplikacji, sprawdza pliki pod kątem uszkodzeń i modyfikacji, a także sprawdza podpisy cyfrowe plików aplikacji.
- **Zarządzanie kontami Agenta autoryzacji**. Kaspersky Endpoint Security konfiguruje ustawienia konta Agenta autoryzacji. Agent autoryzacji jest potrzebny do pracy z zaszyfrowanymi dyskami. Przed załadowaniem systemu operacyjnego użytkownik musi zakończyć uwierzytelnianie za pomocą Agenta.

Jeżeli aplikacja działa jako część rozwiązania Endpoint Detection and Response firmy Kaspersky możesz uruchomić dodatkowe zadania jako akcje reagowania na wykrycie (responses). Na przykład możesz zdalnie zakończyć działanie procesu, korzystając z zadania *Zakończ proces*.

Zadania są uruchamiane na komputerze tylko wtedy, gdy program Kaspersky Endpoint Security jest uruchomiony.

Tworzenie zadania

Jak utworzyć zadanie w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz **Zadania**.
3. Kliknij **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia zadania.
4. Postępuj zgodnie z instrukcjami Kreatora tworzenia zadania.

Jak utworzyć zadanie w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.
3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz zadanie, które chcesz uruchomić na komputerach użytkownika.

   c. W polu **Nazwa zadania** wpisz krótki opis.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.

5. Wybierz konto do uruchomienia zadania. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika.

6. Zakończ działanie kreatora.

Nowe zadanie zostanie wyświetlone na liście zadań. Zadanie będzie miało domyślne ustawienia. Aby skonfigurować ustawienia zadania, przejdź do właściwości zadania. Aby uruchomić zadanie, należy zaznaczyć pole obok zadania i kliknąć przycisk **Uruchom**. Po uruchomieniu zadania możesz je zatrzymać i wznowić później.

Na liście zadań możesz monitorować wyniki zadania, które zawierają stan zadania i statystyki wykonania zadania na komputerach. Możesz także utworzyć wybór zdarzeń do monitorowania zakończenia wykonywania zadań (**Monitorowanie → Wybory zdarzeń**). Bardziej szczegółowe informacje na temat wyboru zdarzeń można znaleźć w pomocy do Kaspersky Security Center. Wyniki wykonania zadania są także zapisywanie lokalnie w dzienniku zdarzeń systemu Windows oraz w raportach Kaspersky Endpoint Security.

Zarządzanie dostępem do zadań

Uprawnienia dostępu do zadań Kaspersky Endpoint Security (odczyt, zapis, wykonanie) są definiowane dla każdego użytkownika, który posiada dostęp do Serwera administracyjnego Kaspersky Security Center, poprzez ustawienia dostępu do obszarów funkcyjnych Kaspersky Endpoint Security. Aby skonfigurować dostęp do obszarów funkcyjnych Kaspersky Endpoint Security, przejdź do sekcji **Bezpieczeństwo** okna właściwości Serwera administracyjnego Kaspersky Security Center. Aby uzyskać więcej informacji na temat zarządzania zadaniami w Kaspersky Security Center, zapoznaj się z systemem pomocy Kaspersky Security Center.

Możesz skonfigurować uprawnienia użytkowników do uzyskiwania dostępu do zadań za pomocą zasady (*tryb zarządzania zadaniami*). Na przykład możesz ukryć zadania grupowe w interfejsie Kaspersky Endpoint Security.

Jak skonfigurować tryb zarządzania zadaniami w interfejsie Kaspersky Endpoint Security poprzez Konsolę administracyjną (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Zadania lokalne → Zarządzanie zadaniami**.

4. Skonfiguruj tryb zarządzania zadaniami (patrz tabela poniżej).

5. Zapisz swoje zmiany.

Jak skonfigurować tryb zarządzania zadaniami w interfejsie Kaspersky Endpoint Security za pośrednictwem Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne → Interakcja użytkownika**.

5. W obszarze **Dozwolone akcje** skonfiguruj tryb zarządzania zadaniami (patrz tabela poniżej).

6. Zapisz swoje zmiany.

Ustawienia Zarządzania zadaniami

Parametr	Opis
Dostęp do zadań lokalnych	Jeśli pole jest zaznaczone, zadania lokalne są wyświetlane w interfejsie lokalnym Kaspersky Endpoint Security. Jeżeli nie ma dodatkowych ograniczeń profilu, użytkownik może konfigurować i uruchamiać zadania. Jednakże konfigurowanie terminarza uruchamiania zadania pozostaje niedostępne dla użytkowania. Użytkownik może uruchamiać zadania tylko ręcznie. Jeśli pole jest odznaczone, korzystanie z zadań lokalnych zostaje zatrzymane. W tym trybie zadania lokalne nie są uruchamiane zgodnie z terminarzem. Zadania nie mogą być uruchamiane anie konfigurowane w lokalnym interfejsie Kaspersky Endpoint Security lub podczas pracy z wierszem poleceń. Użytkownik może uruchomić skanowanie pliku lub folderu, wybierając opcję **Szukaj wirusów** w menu kontekstowym pliku lub folderu. Zadanie skanowania jest uruchamiane z domyślnymi wartościami ustawień zadania skanowania obiektów.
Zobacz zadania grupowe	Jeśli pole jest zaznaczone, zadania grupowe są wyświetlane w interfejsie lokalnym Kaspersky Endpoint Security. Użytkownik może wyświetlić listę wszystkich zadań w interfejsie aplikacji. Jeśli pole nie jest odznaczone, Kaspersky Endpoint Security wyświetla pustą listę zadań.
Zarządzaj zadaniami grupowymi	Jeśli to pole jest zaznaczone, użytkownicy mogą uruchamiać i zatrzymywać zadania grupowe określone w konsoli Kaspersky Security Center. Użytkownicy mogą uruchamiać i zatrzymywać zadania w interfejsie aplikacji lub w uproszczonym interfejsie aplikacji. Jeśli pole jest odznaczone, Kaspersky Endpoint Security automatycznie uruchamia zaplanowane zadania lub administrator uruchamia zadania ręcznie w konsoli Kaspersky Security Center.

Konfigurowanie lokalnych ustawień aplikacji

W Kaspersky Security Center możesz skonfigurować ustawienia Kaspersky Endpoint Security na określonym komputerze. Są to *lokalne ustawienia aplikacji*. Niektóre ustawienia mogą być niedostępne do edycji. Te ustawienia są zablokowane przez atrybut we właściwościach profilu.

Jak skonfigurować lokalne ustawienia aplikacji w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.

3. W obszarze roboczym wybierz zakładkę **Urządzenia**.

4. Kliknij dwukrotnie komputer, aby otworzyć okno właściwości komputera.

5. W oknie ustawień komputera wybierz sekcję **Aplikacje**.

6. Na liście aplikacji Kaspersky zainstalowanych na komputerze wybierz **Kaspersky Endpoint Security for Windows (14.1)** i kliknij ją dwukrotnie, aby otworzyć właściwości aplikacji.

7. W sekcji **Ustawienia ogólne** skonfiguruj Kaspersky Endpoint Security, a także Raporty i pliki danych.

   Pozostałe sekcje w oknie właściwości aplikacji są standardowe dla Kaspersky Security Center. Opis tych sekcji można znaleźć w systemie pomocy programu Kaspersky Security Center.

   > Jeśli aplikacja podlega zasadzie, która blokuje wprowadzanie zmian w określonych ustawieniach, nie będziesz mógł ich zmodyfikować w trakcie konfiguracji ustawień aplikacji w sekcji **Ustawienia ogólne**.

8. Zapisz swoje zmiany.

Jak skonfigurować lokalne ustawienia aplikacji w konsoli Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Wybierz komputer, dla którego chcesz skonfigurować lokalne ustawienia aplikacji.

   Spowoduje to otwarcie właściwości komputera.
3. Wybierz zakładkę **Aplikacje**.
4. Kliknij **Kaspersky Endpoint Security for Windows**.

   Spowoduje to otwarcie lokalnych ustawień aplikacji.
5. Wybierz zakładkę **Ustawienia aplikacji**.
6. Skonfiguruj lokalne ustawienia aplikacji.
7. Zapisz swoje zmiany.

Lokalne ustawienia aplikacji są takie same, jak ustawienia profilu, za wyjątkiem ustawień szyfrowania.

Uruchamianie i zatrzymywanie Kaspersky Endpoint Security

Po zainstalowaniu Kaspersky Endpoint Security na komputerze użytkownika, aplikacja jest uruchamiana automatycznie. Domyślnie, Kaspersky Endpoint Security jest uruchamiany po załadowaniu systemu operacyjnego. Nie można skonfigurować automatycznego uruchamiania aplikacji w ustawieniach systemu operacyjnego.

Pobieranie antywirusowych baz danych Kaspersky Endpoint Security po uruchomieniu systemu operacyjnego może zająć do dwóch minut w zależności od możliwości komputera. W tym czasie poziom ochrony zostanie zredukowany. Pobieranie antywirusowych baz danych, gdy Kaspersky Endpoint Security jest uruchomiony na już załadowanym systemie operacyjnym, nie spowoduje zredukowania poziomu ochrony komputera.

Jak skonfigurować uruchamianie Kaspersky Endpoint Security w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.
4. Użyj pola **Uruchom aplikację przy uruchomieniu komputera (zalecane)**, aby skonfigurować uruchamianie aplikacji.
5. Zapisz swoje zmiany.

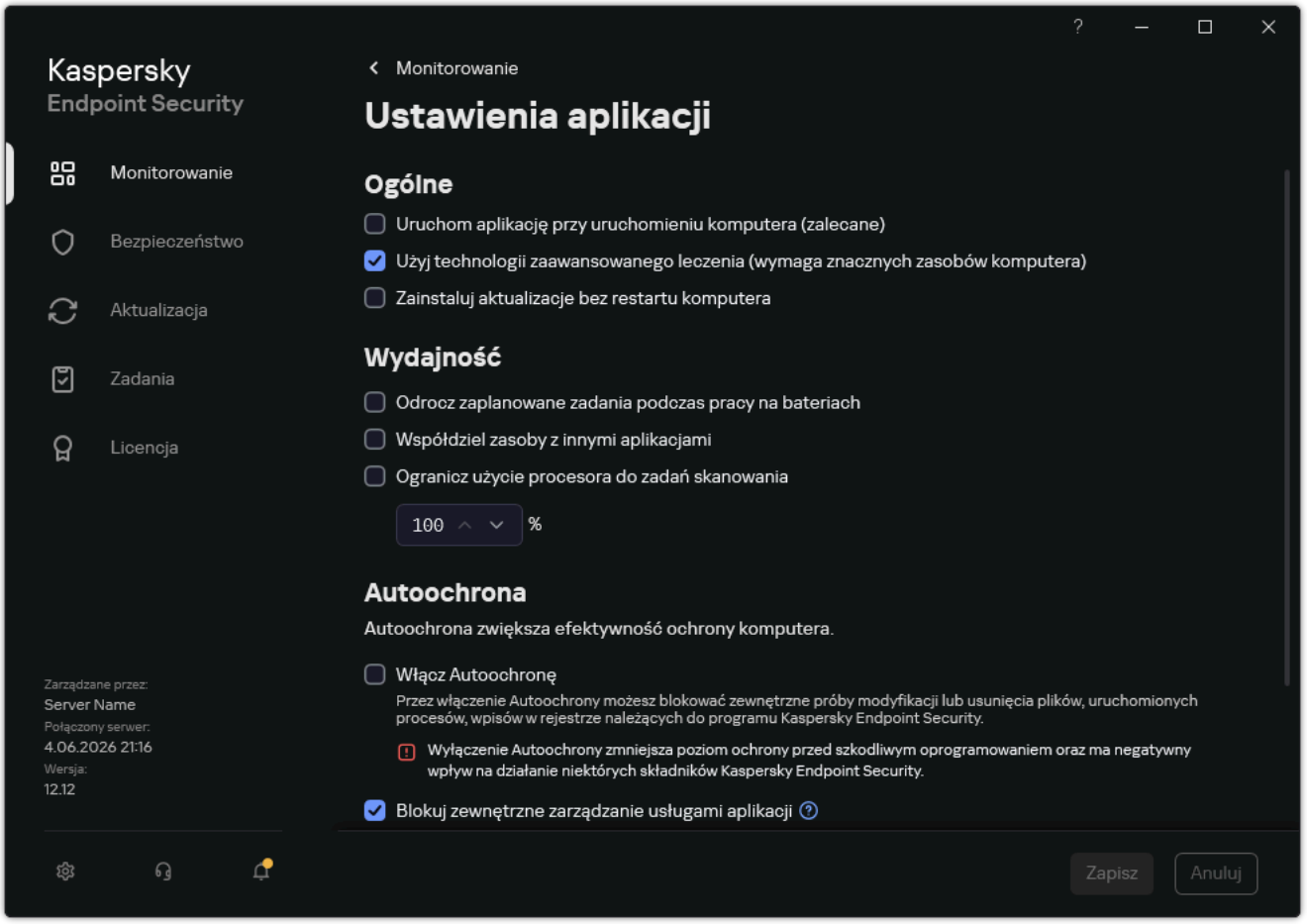
Jak skonfigurować uruchamianie Kaspersky Endpoint Security w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Interakcja użytkownika**.
5. Użyj pola **Uruchom Kaspersky Endpoint Security przy włączaniu komputera (zalecane)**, aby skonfigurować uruchamianie aplikacji.
6. Zapisz swoje zmiany.

Jak skonfigurować uruchamianie Kaspersky Endpoint Security w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.



Ustawienia Kaspersky Endpoint Security for Windows

3. Użyj pola **Uruchom aplikację przy uruchomieniu komputera (zalecane)**, aby skonfigurować uruchamianie aplikacji.

4. Zapisz swoje zmiany.

Eksperci z Kaspersky nie zalecają ręcznego wyłączania Kaspersky Endpoint Security, ponieważ narazi to komputer i dane osobowe na zagrożenia. W razie konieczności możesz wstrzymać ochronę komputera na tak długo jak potrzebujesz, bez wyłączania aplikacji.

Możesz monitorować stan aplikacji za pomocą widżetu **Stan ochrony**.

Jak uruchomić lub zatrzymać Kaspersky Endpoint Security w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.

3. W obszarze roboczym wybierz zakładkę **Urządzenia**.

4. Kliknij dwukrotnie komputer, aby otworzyć okno właściwości komputera.

5. W oknie ustawień komputera wybierz sekcję **Aplikacje**.

6. Na liście aplikacji Kaspersky zainstalowanych na komputerze wybierz **Kaspersky Endpoint Security for Windows (14.1)** i kliknij ją dwukrotnie, aby otworzyć właściwości aplikacji.

7. Wykonaj jedną z poniższych czynności:

   - W celu uruchomienia aplikacji kliknij przycisk  na prawo od listy aplikacji Kaspersky.

   - W celu zatrzymania aplikacji kliknij przycisk  na prawo od listy aplikacji Kaspersky.

Jak uruchomić lub zatrzymać Kaspersky Endpoint Security w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

2. Kliknij nazwę tego komputera, na którym chcesz uruchomić lub zatrzymać działanie Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości komputera.

3. Wybierz zakładkę **Aplikacje**.

4. Zaznacz pole obok **Kaspersky Endpoint Security for Windows**.

5. Kliknij przycisk **Uruchom** lub **Zatrzymaj**.

Jak uruchomić lub zatrzymać Kaspersky Endpoint Security z poziomu wiersza poleceń?

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.

2. Przejdź do folderu, w którym znajduje się plik wykonywalny klpsm.exe.

3. Aby uruchomić aplikację z poziomu wiersza polecenia, wpisz `klpsm.exe start_avp_service`.

4. Aby zatrzymać aplikację z poziomu wiersza polecenia, wpisz `klpsm.exe stop_avp_service`.

Aby zatrzymać aplikację z poziomu wiersza poleceń, włącz możliwość zewnętrznego zarządzania usługami systemowymi.



Uruchamianie i zatrzymywanie aplikacji z poziomu wiersza poleceń

Wstrzymywanie i wznawianie kontroli i ochrony komputera

Pojęcie wstrzymywania kontroli i ochrony komputera oznacza wyłączenie na pewien czas wszystkich składników kontroli i ochrony programu Kaspersky Endpoint Security.

Stan aplikacji jest wyświetlany przy pomocy ikony aplikacji w obszarze powiadomień paska zadań.

- Ikona oznacza, że kontrola i ochrona komputera zostały wstrzymane.
- Ikona oznacza, że kontrola i ochrona komputera zostały włączone.

Wstrzymywanie lub wznawianie kontroli i ochrony komputera nie ma wpływu na zadania skanowania i aktualizacji.

Jeżeli podczas wstrzymywania lub wznawiania kontroli i ochrony komputera nawiązane są jakiekolwiek połączenia sieciowe, wówczas zostanie wyświetlone powiadomienie o zerwaniu tych połączeń.

W celu wstrzymania kontroli i ochrony komputera:

1. Kliknij prawym przyciskiem myszy ikonę aplikacji znajdującą się w obszarze powiadomień paska zadań.
2. Z otwartego menu kontekstowego wybierz **Wstrzymaj ochronę** (patrz rysunek poniżej).

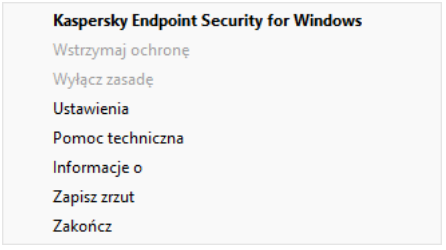
   Ten element menu kontekstowego jest dostępny, jeśli ochrona hasłem jest włączona.

3. Wybierz jedną z następujących opcji:

   - **Wstrzymaj na <określony czas>** – kontrola i ochrona komputera zostaną wznowione po upływie czasu wybranego z listy rozwijalnej dostępnej poniżej.
   - **Wstrzymaj do restartu aplikacji** – kontrola i ochrona komputera zostaną wznowione po ponownym uruchomieniu aplikacji lub systemu operacyjnego. Aby użyć tej opcji, należy włączyć automatyczne uruchamianie aplikacji.
   - **Wstrzymaj** – kontrola i ochrona komputera zostaną wznowione na Twoje żądanie.

4. Kliknij **Wstrzymaj ochronę**.

   Kaspersky Endpoint Security wstrzymuje działanie wszystkich składników ochrony i kontroli, które nie są oznaczone kłódką (🔒) w profilu. Przed wykonaniem tego działania, zalecane jest wyłączenie profilu Kaspersky Security Center.



Menu kontekstowe ikony aplikacji

W celu wznowienia kontroli i ochrony komputera:

1. Kliknij prawym przyciskiem myszy ikonę aplikacji znajdującą się w obszarze powiadomień paska zadań.
2. Z otwartego menu kontekstowego wybierz **Wznów ochronę**.

Możesz wznowić kontrolę i ochronę komputera w dowolnym momencie, niezależnie od wybranej opcji wstrzymania kontroli i ochrony komputera.

Tworzenie i korzystanie z pliku konfiguracyjnego

Plik konfiguracyjny z ustawieniami Kaspersky Endpoint Security umożliwia wykonanie następujących zadań:

- Lokalnej instalacji Kaspersky Endpoint Security z predefiniowanymi ustawieniami z poziomu wiersza poleceń.
- Zdalnej instalacji Kaspersky Endpoint Security z predefiniowanymi ustawieniami z poziomu Kaspersky Security Center.
- Przenieś ustawienia aplikacji do zasady.
- Przeniesienia ustawień Kaspersky Endpoint Security z jednego komputera na drugi (zapoznaj się z poniższymi instrukcjami).

Eksportowanie pliku konfiguracyjnego

W celu utworzenia pliku konfiguracyjnego:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Zarządzaj ustawieniami**.
3. Kliknij **Eksportuj**.
4. W otwartym oknie wskaż miejsce, w którym chcesz zapisać plik konfiguracyjny, i wprowadź nazwę pliku.

   Aby użyć pliku konfiguracyjnego dla lokalnej lub zdalnej instalacji Kaspersky Endpoint Security, należy nadać mu nazwę install.cfg.

5. W razie potrzeby wprowadź hasło, aby wyeksportować konfigurację aplikacji do pliku.

   Aby zapisać plik konfiguracyjny, komponent Ochrona hasłem musi być włączony. Użytkownik musi mieć uprawnienie **Eksportuj ustawienia**.

6. Zapisz plik.

W rezultacie aplikacja tworzy plik konfiguracyjny. Plik konfiguracyjny może zawierać szczegóły konta użytkownika, dlatego Kaspersky Endpoint Security szyfruje plik. Nie można edytować pliku konfiguracyjnego. Wszelkie próby modyfikacji pliku konfiguracyjnego spowodują jego uszkodzenie.

Importowanie pliku konfiguracyjnego

Plik konfiguracyjny może zawierać szczegóły kont użytkowników dodanych do aplikacji. Jeśli importujesz plik na tym samym komputerze, na którym został utworzony, Kaspersky Endpoint Security importuje hasła kont użytkowników. Jeśli importujesz plik na inny komputer, musisz wprowadzić hasła ręcznie.

Podczas importowania pliku konfiguracyjnego Kaspersky Endpoint Security nie przesyła haseł do kontenerów kryptograficznych. Jeśli łączysz się z serwerami za pomocą uwierzytelniania dwukierunkowego, musisz od podstaw określić hasła do kontenerów kryptograficznych.

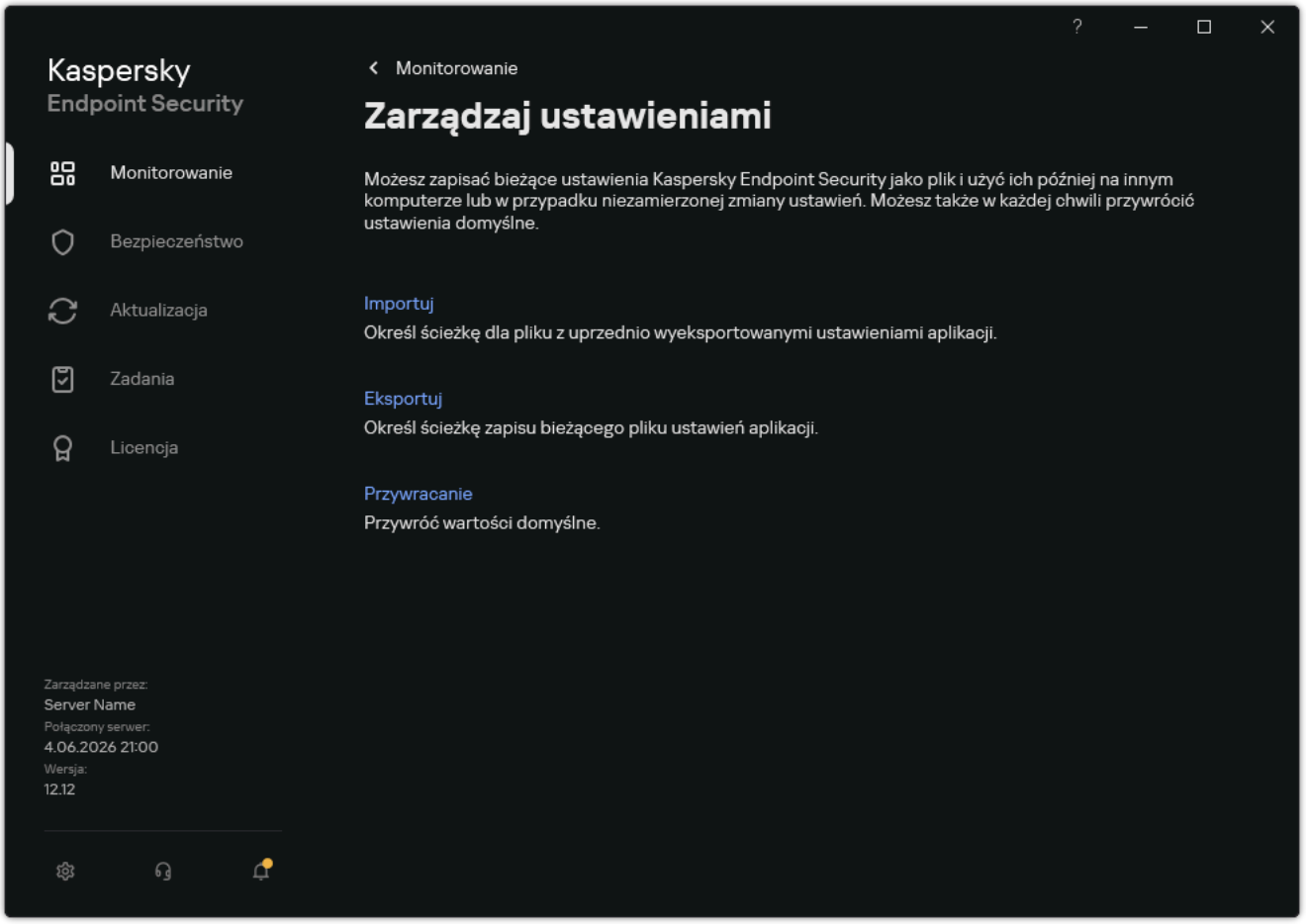
W celu zaimportowania ustawień Kaspersky Endpoint Security z pliku konfiguracyjnego:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Zarządzaj ustawieniami**.
3. Kliknij **Importuj**.

4. W otwartym oknie wprowadź ścieżkę dostępu do pliku konfiguracyjnego.

5. Otwórz plik.

Wszystkie wartości ustawień Kaspersky Endpoint Security zostaną ustawione zgodnie z wybranym plikiem konfiguracyjnym.



Zarządzanie ustawieniami aplikacji

Przywracanie ustawień domyślnych aplikacji

W każdej chwili można przywrócić ustawienia aplikacji zalecane przez Kaspersky. Po przywróceniu ustawień, poziom ochrony wszystkich modułów zostaje ustawiony na **Zalecany**.

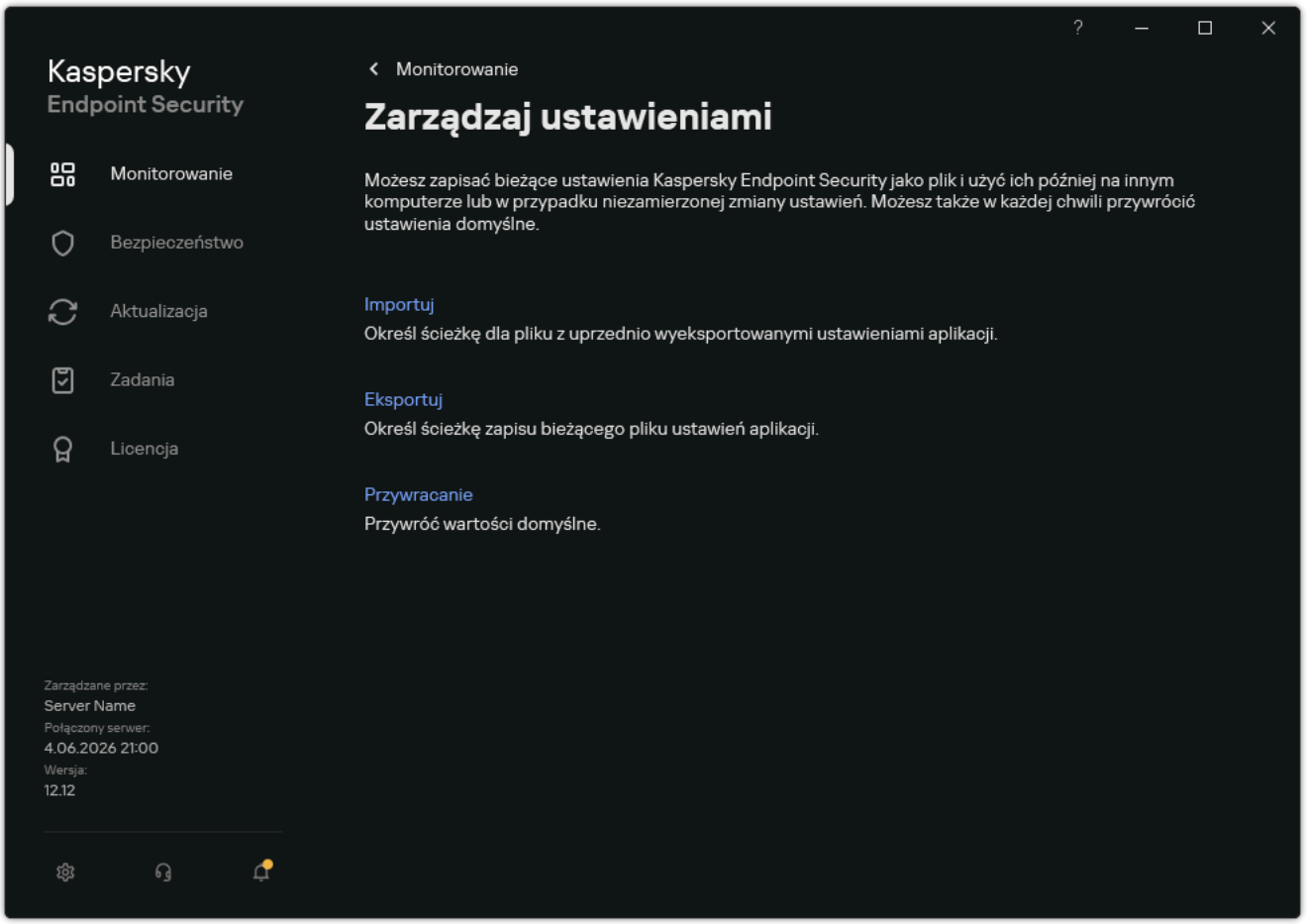
W celu przywrócenia domyślnych ustawień aplikacji:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Zarządzaj ustawieniami**.

3. Kliknij **Przywracanie**.

4. Zapisz swoje zmiany.



Zarządzanie ustawieniami aplikacji

Działanie Kaspersky Endpoint Security i kompatybilność z innymi aplikacjami

Wydajność Kaspersky Endpoint Security wiąże się z liczbą typów wykrywanych szkodliwych obiektów, zużyciem energii i wykorzystaniem zasobów komputera.

Wybieranie typów wykrywanych obiektów

Kaspersky Endpoint Security umożliwia dostosowanie ochrony komputera i wybranie typów obiektów wykrywanych przez aplikację podczas działania. Kaspersky Endpoint Security zawsze skanuje system operacyjny w poszukiwaniu wirusów, robaków i trojanów. Nie możesz wyłączyć skanowania tych typów obiektów. Takie szkodliwe oprogramowanie może wyrządzić znaczne szkody w komputerze. Aby zwiększyć ochronę komputera, możesz poszerzyć zakres wykrywanych typów obiektów, włączając monitorowanie legalnych aplikacji, które cyberprzestępca może przejąć w celu wyrządzenia szkód lub kradzieży danych.

Korzystanie z trybu oszczędzania energii

Zużycie energii przez aplikację jest kluczowe dla komputerów przenośnych. Zaplanowane zadania z Kaspersky Endpoint Security zazwyczaj wykorzystują dużą ilość zasobów. Aby oszczędzać energię w trakcie pracy na baterii, możesz użyć trybu oszczędzania energii.

W trybie oszczędzania energii automatycznie odraczane są następujące zadania:

- Zadanie Pełne skanowanie;
- Zadanie Skanowanie obszarów krytycznych;
- Zadanie Skanowanie obiektów;
- Zadanie Sprawdzanie integralności.

Niezależnie od tego, czy tryb oszczędzania energii jest włączony, Kaspersky Endpoint Security wstrzymuje zadania szyfrowania po przejściu komputera przenośnego do trybu pracy na bateriach. Aplikacja wznawia zadania szyfrowania po przejściu komputera przenośnego z trybu pracy na bateriach do trybu głównego.

Udostępnianie zasobów komputera innym aplikacjom

Zużycie zasobów komputera podczas skanowania komputera może zwiększyć obciążenie podsystemów procesora i dysku twardego. Aby rozwiązać problem równoczesnego wykonywania działań w trakcie dużego obciążenia procesora i podsystemów dysku, Kaspersky Endpoint Security może udostępnić zasoby innym aplikacjom.

Używanie zaawansowanej technologii leczenia

Obecnie szkodliwe aplikacje mogą wnikać do najniższych poziomów systemu operacyjnego, co praktycznie uniemożliwia jego usunięcie. Po wykryciu szkodliwej aktywności w systemie operacyjnym, Kaspersky Endpoint Security wykonuje zaawansowaną procedurę leczenia, która korzysta ze specjalnej technologii zaawansowanego leczenia. *Technologia zaawansowanego leczenia* służy do usuwania z systemu operacyjnego szkodliwych aplikacji, które już uruchomiły swoje procesy w pamięci RAM i nie pozwalają aplikacji Kaspersky Endpoint Security na usunięcie ich przy pomocy innych metod. W rezultacie zagrożenie zostanie zneutralizowane. W trakcie działania Zaawansowanego leczenia zaleca się nie uruchamiać nowych procesów ani nie modyfikować rejestru systemu operacyjnego. Technologia zaawansowanego leczenia wykorzystuje dużą ilość zasobów systemu operacyjnego, co może spowolnić inne aplikacje.

Po zakończeniu procesu Zaawansowanego leczenia na komputerze działającym pod kontrolą Microsoft Windows dla stacji roboczych, Kaspersky Endpoint Security poprosi użytkownika o pozwolenie na ponowne uruchomienie komputera. Po ponownym uruchomieniu systemu Kaspersky Endpoint Security wykryje pliki szkodliwego oprogramowania i rozpocznie „lekkie" pełne skanowanie komputera.

Ponowne uruchomienie nie jest możliwe na komputerze działającym pod kontrolą Microsoft Windows dla serwerów z powodu specyfiki Kaspersky Endpoint Security. Nieplanowane ponowne uruchomienie serwera plików może doprowadzić do tymczasowej niedostępności danych serwera plików lub utraty niezapisanych danych. Zaleca się uruchamiać serwer plików trzymając się ściśle ustalonego terminarza. Z tego powodu technologia zaawansowanego leczenia jest domyślnie wyłączona dla serwerów plików.

Jeśli aktywna infekcja zostanie wykryta na serwerze plików, zdarzenie zostanie przesłane do Kaspersky Security Center wraz z informacją, że konieczne jest zaawansowane leczenie. Aby wyleczyć aktywną infekcję na serwerze, włącz technologię zaawansowanego leczenia dla serwerów i uruchom grupowe zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* w momencie wygodnym dla użytkowników serwera.

Włączanie i wyłączanie trybu oszczędzania energii

Tryb oszczędzania energii jest funkcjonalnością, która zmniejsza obciążenie zasobów laptopa i wydłuża czas pracy na baterii, nie obniżając znacząco poziomu bezpieczeństwa. W trybie oszczędzania energii aplikacja ogranicza uruchamianie zaplanowanych zadań. W ten sposób tryb oszczędzania energii zapewnia równowagę między poziomem bezpieczeństwa i czasem pracy baterii laptopa.

Gdy tryb oszczędzania energii jest włączony, a komputer działa na bateriach, następujące zadania nie są uruchamiane, nawet jeśli zostały zaplanowane:

- *Pełne skanowanie*.
- *Skanowanie obszarów krytycznych*.
- *Skanowanie niestandardowe*.
- *Sprawdzanie integralności aplikacji*.
- *Skanowanie IOC*.
- *Aktualizacja baz danych i modułów aplikacji* (tylko poprawki)

Aplikacja pomija zaplanowane aktualizacje bazy danych tylko wtedy, gdy laptop jest zasilany z baterii, a poziom naładowania baterii wynosi poniżej 30%. We wszystkich pozostałych przypadkach Kaspersky Endpoint Security aktualizuje bazy danych zgodnie z harmonogramem, niezależnie od tego, czy laptop jest podłączony do zasilania, czy działa na zasilaniu bateryjnym, a także czy aplikacja działa w trybie oszczędzania energii.

Jak włączyć lub wyłączyć tryb oszczędzania energii w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.
5. W sekcji **Wydajność** użyj pola **Odrocz zaplanowane zadania podczas pracy na bateriach**, aby włączyć lub wyłączyć tryb oszczędzania energii.
6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

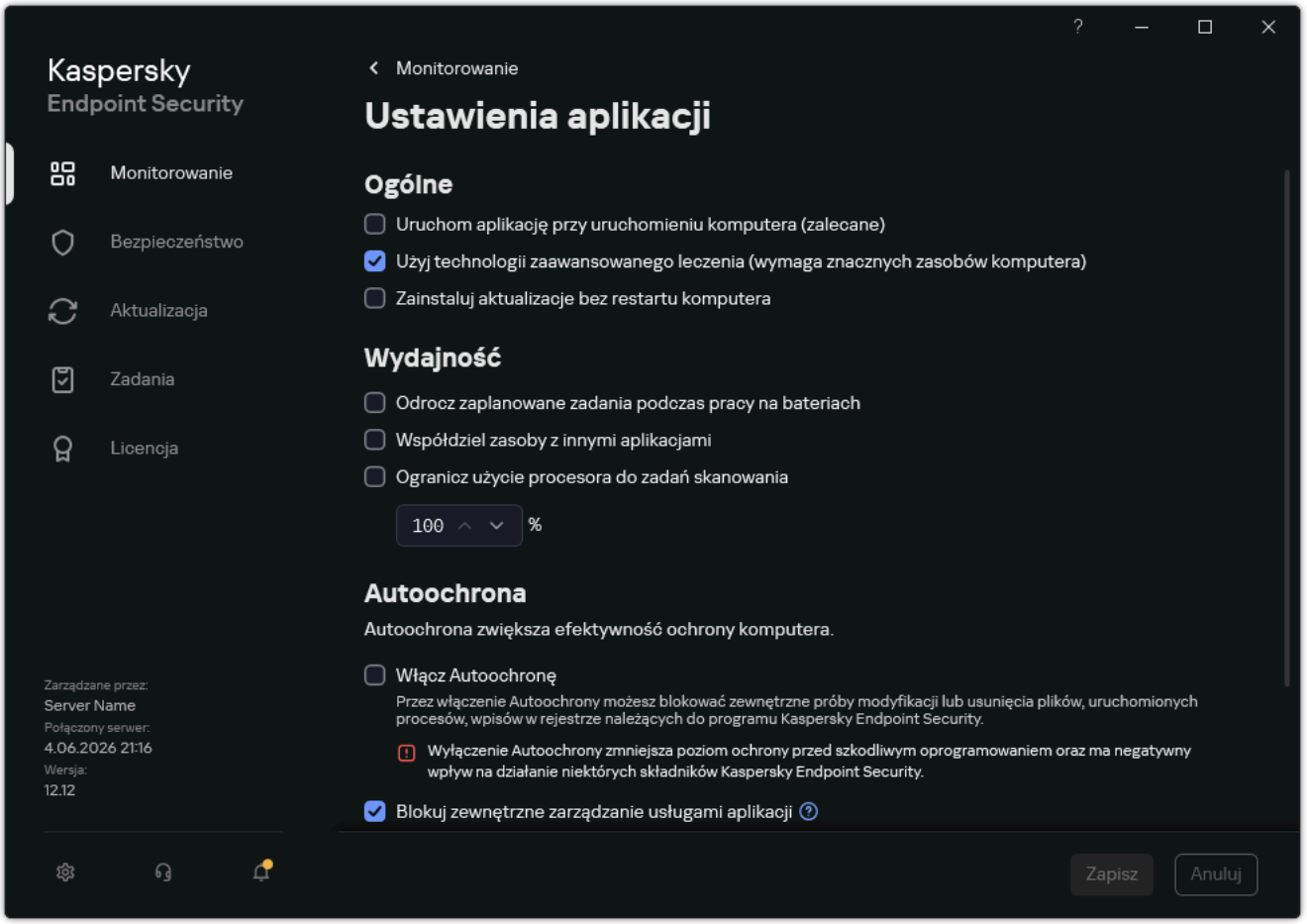
Jak włączyć lub wyłączyć tryb oszczędzania energii w Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Wydajność**.
5. W sekcji **Odrocz lub pomiń zaplanowane zadania podczas pracy na bateriach** użyj pola **Odraczanie lub pomijanie zaplanowanych zadań podczas pracy na bateriach (zależy od systemu)**, aby włączyć lub wyłączyć tryb oszczędzania energii.
6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć tryb oszczędzania energii w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.



Ustawienia Kaspersky Endpoint Security for Windows

3. W sekcji **Wydajność** użyj pola **Odrocz zaplanowane zadania podczas pracy na bateriach**, aby włączyć lub wyłączyć tryb oszczędzania energii.
4. Zapisz swoje zmiany.

Włączanie i wyłączanie udostępniania zasobów innym aplikacjom

Zużycie zasobów komputera przez Kaspersky Endpoint Security podczas skanowania komputera może zwiększyć obciążenie podsystemów procesora i dysku twardego. Może to spowolnić działanie innych aplikacji. Aby zoptymalizować wydajność, Kaspersky Endpoint Security zapewnia *tryb przenoszenia zasobów do innych aplikacji*. W tym trybie system operacyjny może zmniejszyć priorytet wątków zadania skanowania Kaspersky Endpoint Security, gdy obciążenie procesora jest wysokie. Pozwala to na redystrybucję zasobów systemu operacyjnego do innych aplikacji. W ten sposób zadania skanowania otrzymają mniej czasu pracy procesora. W rezultacie Kaspersky Endpoint Security będzie potrzebował więcej czasu na przeskanowanie komputera. Domyślnie aplikacja udostępnia zasoby innym aplikacjom.

Jak włączyć lub wyłączyć udostępnianie zasobów innym aplikacjom w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.
4. W sekcji **Wydajność** użyj pola **Udostępniaj zasoby innym aplikacjom**, aby włączyć lub wyłączyć współdzielenie zasobów z innymi aplikacjami.
5. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć udostępnianie zasobów innym aplikacjom w Web Console i Cloud Console?

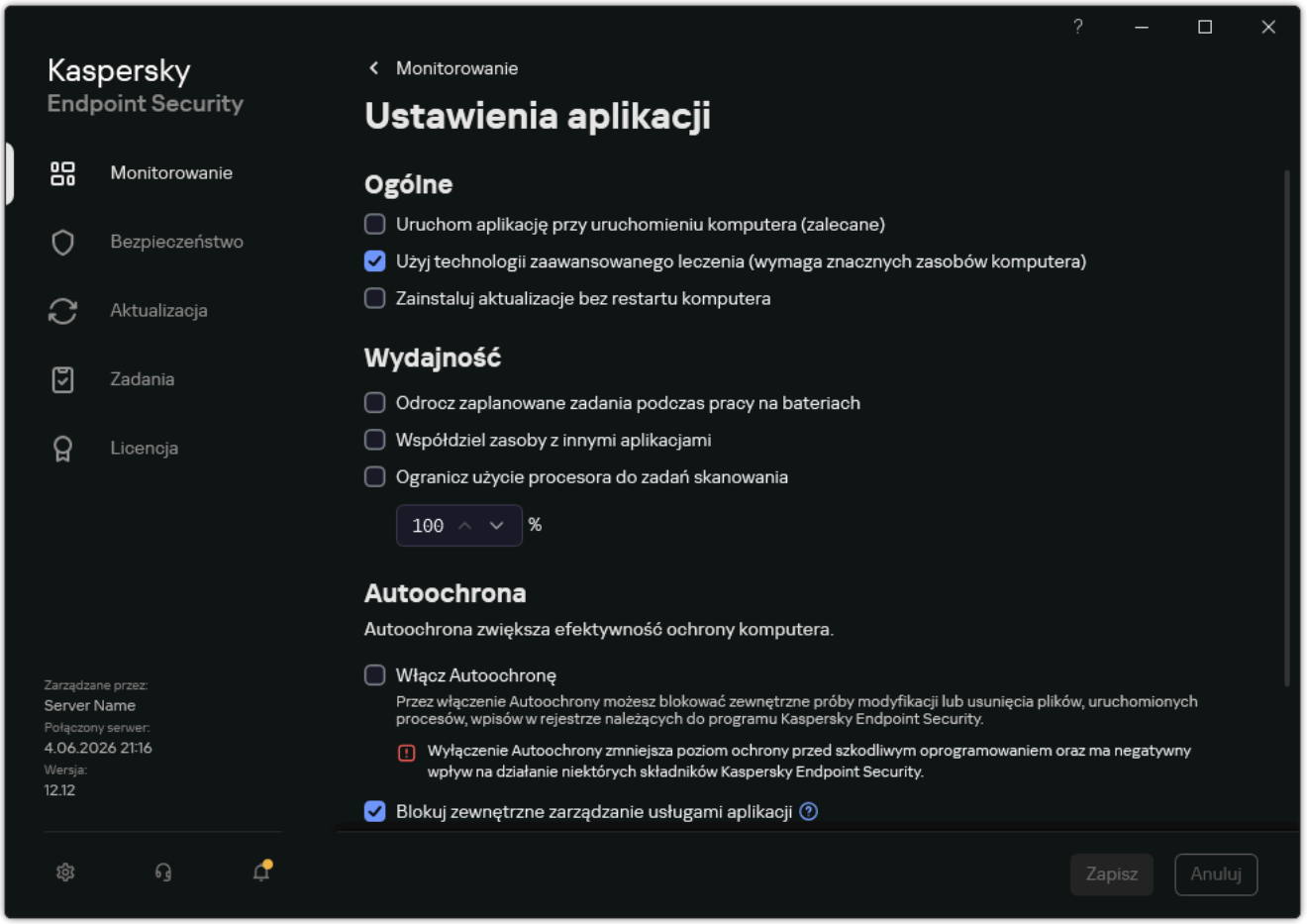
1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Wydajność**.
5. W sekcji **Współdziel zasoby z innymi aplikacjami** użyj przełącznika **Współdziel zasoby z innymi aplikacjami**, aby włączyć lub wyłączyć udostępnianie zasobów innym aplikacjom.
6. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć udostępnianie zasobów innym aplikacjom w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.



Ustawienia Kaspersky Endpoint Security for Windows

3. W sekcji **Wydajność** użyj pola **Udostępniaj zasoby innym aplikacjom**, aby włączyć lub wyłączyć współdzielenie zasobów z innymi aplikacjami.

4. Zapisz swoje zmiany.

Praktyczne zastosowanie aplikacji do optymalizowania wydajności Kaspersky Endpoint Security

Podczas wdrażania Kaspersky Endpoint Security for Windows możesz użyć następujących zaleceń w celu skonfigurowania ochrony komputera i zoptymalizowania wydajności. Aby uzyskać więcej informacji na temat rozwiązywania problemów z wydajnością komputera, zapoznaj się z Bazą wiedzy pomocy technicznej.

Ogólne

Skonfiguruj ogólne ustawienia aplikacji zgodnie z następującymi zaleceniami:

1. Zaktualizuj Kaspersky Endpoint Security do najnowszej wersji.

   Nowsze wersje aplikacji zawierają naprawione błędy, udoskonaloną stabilność oraz zoptymalizowaną wydajność.

2. Włącz składniki ochrony z domyślnymi ustawieniami.

   Domyślne ustawienia są uznawane za optymalne. Te ustawienia są zalecane przez ekspertów z Kaspersky. Domyślne ustawienia zawierają zalecany poziom ochrony i optymalne zużycie zasobów. Jeśli to konieczne, możesz przywrócić domyślne ustawienia aplikacji.

3. Włącz funkcje optymalizacji działania aplikacji.

   Aplikacja zawiera funkcje optymalizacji działania: tryb oszczędzania energii oraz współdzielenie zasobów do innych aplikacji. Upewnij się, że te opcje są włączone.

Skanowanie w poszukiwaniu złośliwego oprogramowania na stacjach roboczych

Włączenie Skanowania w tle jest zalecane dla Skanowania w poszukiwaniu złośliwego oprogramowania stacji roboczych. *Skanowanie w tle* to tryb skanowania programu Kaspersky Endpoint Security, który nie wyświetla powiadomień. Skanowanie w tle wymaga mniej zasobów komputera niż inne typy skanowań (takie jak pełne skanowanie). W tym trybie Kaspersky Endpoint Security skanuje obiekty startowe, sektory startowe, pamięć systemową i partycje systemowe. Ustawienia skanowania w tle są uznawane za optymalne. Te ustawienia są zalecane przez ekspertów z Kaspersky. Dlatego też dla wykonania Skanowania w poszukiwaniu złośliwego oprogramowania komputera możesz użyć tylko trybu skanowania w tle bez użycia innych zadań skanowania.

Jeśli skanowanie w tle nie odpowiada Twoim potrzebom, skonfiguruj zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* zgodnie z następującymi zaleceniami:

1. Ustaw limit zużycia zasobów procesora podczas skanowania komputera.

   Możesz ograniczyć użycie procesora przez zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Aby to zrobić, w ustawieniach aplikacji określ maksymalny procent obciążenia procesora dla wszystkich rdzeni, który może być wykorzystany podczas skanowania komputera. Może to wydłużyć czas skanowania komputera.

2. Skonfiguruj optymalny terminarz skanowania komputera.

   Możesz skonfigurować zadanie do uruchamiania, gdy komputer działa z minimalnym obciążeniem. Na przykład, możesz skonfigurować zadanie do uruchamiania w nocy lub w weekendy.

   Jeśli użytkownicy wyłączą komputer poza godzinami pracy, możesz włączyć funkcję Wake-on-LAN. Funkcja Wake-on-LAN umożliwia zdalne włączenie komputera poprzez wysłanie specjalnego sygnału przez sieć lokalną. Aby użyć tej funkcji, musisz włączyć Wake-on-LAN w ustawieniach BIOS-u. Możesz także skonfigurować automatyczne wyłączanie komputera po zakończeniu skanowania.

   Jeśli nie mogłeś skonfigurować optymalnego terminarza skanowania, skonfiguruj zadania tak, aby były uruchamiane tylko wtedy, gdy komputer jest w trybie bezczynności. Kaspersky Endpoint Security uruchamia zadanie skanowania, jeśli komputer jest zablokowany lub wygaszacz ekranu jest włączony. Jeśli przerwałeś wykonywanie zadania, na przykład, poprzez odblokowanie komputera, Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane.

3. Określ obszar skanowania.

Wybierz następujące obiekty do skanowania (minimalny zestaw obszarów skanowania):

- Pamięć jądra
- Uruchomione procesy i obiekty startowe
- Sektory startowe
- %systemroot% (bez podfolderów)
- %systemroot%\System (bez podfolderów)
- %systemroot%\System32 (bez podfolderów)
- %systemroot%\System32\drivers (bez podfolderów)
- %systemroot%\SysWOW64 (bez podfolderów)
- %systemroot%\SysWOW64\drivers (bez podfolderów)

4. Włącz technologie iSwift i iChecker.

   - Technologia iSwift.

     Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.

   - Technologia iChecker.

     Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).

   Możesz tylko włączyć technologie iSwift i iChecker w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security. Nie możesz włączyć tych technologii w konsoli Kaspersky Security Center Web Console.

5. Wyłącz skanowanie archiwów chronionych hasłem.

   Jeśli skanowanie archiwów chronionych hasłem jest włączone, pytanie o hasło jest wyświetlane przed skanowaniem archiwów. Ponieważ zalecane jest skonfigurowanie terminarza uruchamiania zadania poza godzinami pracy, użytkownik nie może wprowadzić hasła. Możesz ręcznie skanować archiwa chronione hasłem.

6. Wyłącz jednoczesne uruchamianie kilku zadań skanowania.

   Kaspersky Endpoint Security będzie wysyłał nowe zadania skanowania, jeśli bieżące skanowanie będzie kontynuowane. Pomaga to zoptymalizować obciążenie komputera.

Skanowanie w poszukiwaniu złośliwego oprogramowania na serwerach

Skonfiguruj zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* zgodnie z następującymi zaleceniami:

1. Ustaw limit zużycia zasobów procesora podczas skanowania komputera.

   Możesz ograniczyć użycie procesora przez zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Aby to zrobić, w ustawieniach aplikacji określ maksymalny procent obciążenia procesora dla wszystkich rdzeni, który może być wykorzystany podczas skanowania komputera. Może to wydłużyć czas skanowania komputera.

2. Skonfiguruj optymalny terminarz skanowania komputera.

   Możesz skonfigurować zadanie do uruchamiania, gdy komputer działa z minimalnym obciążeniem. Na przykład, możesz skonfigurować zadanie do uruchamiania w nocy lub w weekendy.

3. Włącz technologie iSwift i iChecker.

   - Technologia iSwift.

     Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.

   - Technologia iChecker.

     Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).

   Możesz tylko włączyć technologie iSwift i iChecker w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security. Nie możesz włączyć tych technologii w konsoli Kaspersky Security Center Web Console.

4. Wyłącz skanowanie archiwów chronionych hasłem.

   Jeśli skanowanie archiwów chronionych hasłem jest włączone, pytanie o hasło jest wyświetlane przed skanowaniem archiwów. Ponieważ zalecane jest skonfigurowanie terminarza uruchamiania zadania poza godzinami pracy, użytkownik nie może wprowadzić hasła. Możesz ręcznie skanować archiwa chronione hasłem.

5. Wyłącz jednoczesne uruchamianie kilku zadań skanowania.

   Kaspersky Endpoint Security będzie wysyłał nowe zadania skanowania, jeśli bieżące skanowanie będzie kontynuowane. Pomaga to zoptymalizować obciążenie komputera.

Kaspersky Security Network

Aby lepiej chronić Twój komputer, Kaspersky Endpoint Security wykorzystuje dane otrzymane od użytkowników z całego świata. Usługa Kaspersky Security Network została zaprojektowana do gromadzenia tych danych.

Kaspersky Security Network (KSN) jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobów sieciowych oraz oprogramowania. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi programu Kaspersky Endpoint Security na nowe zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów. Jeśli uczestniczysz w Kaspersky Security Network, usługi KSN zapewniają Kaspersky Endpoint Security informacje o reputacji przeskanowanych adresów internetowych, a także informacje o kategorii i reputacji przeskanowanych plików.

Edytuj ustawienia Kaspersky Security Network zgodnie z następującymi zaleceniami:

1. Wyłącz rozszerzony tryb KSN.

   Rozszerzony tryb KSN to tryb, w którym Kaspersky Endpoint Security wysyła dodatkowe dane do Kaspersky.

2. Konfiguruj Kaspersky Private Security Network.

   Kaspersky Private Security Network (KPSN) to rozwiązanie, które umożliwia użytkownikom komputerów z zainstalowanym programem Kaspersky Endpoint Security lub innymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów.

3. Włącz tryb chmury.

   Tryb chmury odnosi się do trybu działania aplikacji, w którym Kaspersky Endpoint Security używa lekkiej wersji antywirusowych baz danych. Kaspersky Security Network obsługuje działanie aplikacji, gdy używana jest lekka wersja antywirusowych baz danych. Lekka wersja antywirusowych baz danych umożliwia korzystanie z około połowy pamięci RAM komputera, która inaczej zostałaby użyta ze zwykłymi bazami danych. Jeśli nie uczestniczysz w Kaspersky Security Network lub jeśli tryb chmury jest wyłączony, Kaspersky Endpoint Security pobierze pełną wersję antywirusowych baz danych z serwerów Kaspersky.

Skanowanie w poszukiwaniu złośliwego oprogramowania

Skanowanie w poszukiwaniu złośliwego oprogramowania jest niezwykle ważne dla bezpieczeństwa komputera. Regularne uruchamianie skanowania antywirusowego pozwala wyeliminować możliwość rozpowszechniania się szkodliwego oprogramowania, które nie jest wykrywane przez moduły ochrony z powodu ustawienia niskiego poziomu ochrony lub z innych powodów.

Kaspersky Endpoint Security nie skanuje plików, których zawartość znajduje się w magazynie w chmurze OneDrive, i tworzy wpisy dziennika informujące, że pliki te nie zostały przeskanowane.

Pełne skanowanie

Szczegółowe skanowanie całego komputera. Kaspersky Endpoint Security skanuje następujące obiekty:

- Pamięć jądra
- Obiekty uruchamiane wraz ze startem systemu operacyjnego
- Sektory startowe
- Kopię zapasową systemu operacyjnego
- Wszystkie dyski twarde i wymienne

Eksperci z Kaspersky zalecają, aby nie zmieniać obszaru skanowania zadania *Pełne skanowanie*.

Aby zachować zasoby komputera, zalecane jest użycie zadania skanowania w tle zamiast zadania pełnego skanowania. Nie wpłynie to na poziom ochrony komputera.

Skanowanie obszarów krytycznych

Domyślnie, Kaspersky Endpoint Security skanuje pamięć jądra, uruchomione procesy i sektory startowe dysku.

Eksperci z Kaspersky zalecają, aby nie zmieniać obszaru skanowania zadania *Skanowanie obszarów krytycznych*.

Skanowanie niestandardowe

Kaspersky Endpoint Security skanuje obiekty wybrane przez użytkownika. Możesz skanować każdy obiekt z poniższej listy:

- Pamięć systemowa
- Obiekty uruchamiane wraz ze startem systemu operacyjnego
- Kopię zapasową systemu operacyjnego
- Dyski twarde, wymienne i sieciowe
- Dowolny wybrany plik

Skanowanie w tle

Skanowanie w tle to tryb skanowania programu Kaspersky Endpoint Security, który nie wyświetla powiadomień. Skanowanie w tle wymaga mniej zasobów komputera niż inne typy skanowań (takie jak pełne skanowanie). W tym trybie Kaspersky Endpoint Security skanuje obiekty startowe, sektory startowe, pamięć systemową i partycje systemowe.

Sprawdzanie integralności aplikacji

Kaspersky Endpoint Security sprawdza, czy moduły aplikacji nie są uszkodzone lub zmodyfikowane.

Skanowanie komputera

Skanowanie jest niezwykle ważne dla bezpieczeństwa komputera. Regularne uruchamianie skanowania antywirusowego pozwala wyeliminować możliwość rozpowszechniania się szkodliwego oprogramowania, które nie jest wykrywane przez moduły ochrony z powodu ustawienia niskiego poziomu ochrony lub z innych powodów. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej.

W Kaspersky Endpoint Security występują następujące predefiniowane standardowe zadania: *Pełne skanowanie*, *Skanowanie obszarów krytycznych*, *Skanowanie niestandardowe*. Jeśli w Twojej organizacji wdrożono system administracyjny Kaspersky Security Center, możesz utworzyć zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* i skonfigurować skanowanie.

Jak w Konsoli administracyjnej (MMC) uruchomić zadanie skanowania?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zadania**.

3. Wybierz zadanie skanowania i kliknij je dwukrotnie, aby otworzyć właściwości zadania.

   W razie konieczności utworzyć zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

4. W oknie właściwości zadania wybierz sekcję **Ustawienia**.

5. Skonfiguruj zadanie skanowanie (patrz tabela poniżej).

   Jeśli to konieczne, skonfiguruj terminarz zadania skanowania.

6. Zapisz swoje zmiany.

7. Uruchom zadanie skanowania.

Kaspersky Endpoint Security uruchomi skanowanie komputera. Jeśli użytkownik przerwał wykonywanie zadania (na przykład, poprzez wyłączenie komputera), Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane.

Jak w konsoli Web Console i Cloud Console uruchomić zadanie skanowania?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie skanowania.

   Zostanie otwarte okno właściwości zadania.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Skonfiguruj zadanie skanowanie (patrz tabela poniżej).

   Jeśli to konieczne, skonfiguruj terminarz zadania skanowania.

5. Zapisz swoje zmiany.

6. Uruchom zadanie skanowania.

Kaspersky Endpoint Security uruchomi skanowanie komputera. Jeśli użytkownik przerwał wykonywanie zadania (na przykład, poprzez wyłączenie komputera), Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane.

Jak w interfejsie aplikacji uruchomić zadanie skanowania?

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.

2. Na liście zadań wybierz zadanie skanowania i kliknij ⚙.

3. Skonfiguruj zadanie skanowanie (patrz tabela poniżej).

   Jeśli to konieczne, skonfiguruj terminarz zadania skanowania.

4. Zapisz swoje zmiany.

5. Uruchom zadanie skanowania.

Kaspersky Endpoint Security uruchomi skanowanie komputera. Aplikacja wyświetli postęp skanowania, liczbę przeskanowanych plików oraz czas pozostały do skanowania. Kliknij przycisk **Zatrzymaj**, aby zatrzymać zadanie w dowolnym momencie. Jeśli zadanie skanowania nie jest wyświetlane, oznacza to, że administrator zabronił użycia zadań lokalnych w zasadzie.

Aby zoptymalizować wydajność Kaspersky Endpoint Security podczas skanowania komputera, możesz zarządzać zaawansowanymi ustawieniami zadania *Pełne skanowanie* i ograniczyć użycie zasobów procesora.

W Kaspersky Security Center możesz również użyć zadania *Skanowanie w tle* zamiast *Pełne skanowanie*, aby zoptymalizować wydajność aplikacji. Nie wpłynie to na poziom ochrony komputera. Skanowania w tle nie można skonfigurować.

W rezultacie Kaspersky Endpoint Security skanuje komputer i w przypadku wykrycia zagrożenia wykonuje działanie skonfigurowane w ustawieniach aplikacji. Zwykle aplikacja próbuje wyleczyć zainfekowane pliki. W rezultacie zainfekowane pliki mogą otrzymać następujące stany:

- **Odroczony**. Zainfekowany plik nie mógł zostać wyleczony. Aplikacja usuwa zainfekowany plik po ponownym uruchomieniu komputera.
- **Zapisano w raporcie**. Zainfekowany plik nie mógł zostać wyleczony. Aplikacja dodaje informacje o wykrytych zainfekowanych plikach do listy aktywnych zagrożeń.
- **Zapis nie jest obsługiwany** lub **Błąd zapisu**. Zainfekowany plik nie mógł zostać wyleczony. Aplikacja nie ma uprawnień do zapisu.
- **Już przetworzono**. Aplikacja wcześniej wykryła zainfekowany plik. Aplikacja leczy lub usuwa zainfekowany plik po ponownym uruchomieniu komputera.

Ustawienia skanowania

Parametr	Opis
Poziom ochrony	Kaspersky Endpoint Security może używać różnych grup ustawień uruchamiania skanowania. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane *poziomami ochrony*. • **Wysoki**. Kaspersky Endpoint Security skanuje wszystkie typy plików. Podczas skanowania plików złożonych aplikacja skanuje archiwa, pakiety dystrybucyjne i pliki w formatach biurowych, ale nie skanuje archiwów chronionych hasłem. Po ustawieniu tego poziomu bezpieczeństwa aplikacja korzysta z analizy heurystycznej z poziomem szczegółowości **Poziom szczegółowy**. • **Zalecany**. Kaspersky Endpoint Security skanuje wszystkie typy plików. Podczas skanowania plików złożonych aplikacja skanuje archiwa, pakiety dystrybucyjne i pliki w formatach biurowych, ale nie skanuje archiwów chronionych hasłem. Po ustawieniu tego poziomu bezpieczeństwa aplikacja korzysta z analizy heurystycznej z poziomem szczegółowości **Poziom średni**. • **Niski**. Kaspersky Endpoint Security skanuje tylko określone formaty plików. Podczas skanowania plików złożonych aplikacja skanuje archiwa, pakiety dystrybucyjne i pliki w formatach biurowych, ale nie skanuje archiwów chronionych hasłem. Po ustawieniu tego poziomu bezpieczeństwa aplikacja korzysta z analizy heurystycznej z poziomem szczegółowości **Poziom niski**. Możesz wybrać jeden z predefiniowanych poziomów ochrony lub ręcznie skonfigurować ustawienia poziomu ochrony. Jeśli zmieniłeś ustawienia poziomu ochrony, możesz zawsze powrócić do zalecanych ustawień poziomu ochrony.

Parametr	Opis
Działanie po wykryciu zagrożenia	**Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik. **Wylecz; poinformuj, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeśli leczenie się nie powiedzie, Kaspersky Endpoint Security doda informacje o wykrytych zainfekowanych plikach do listy aktywnych zagrożeń. **Poinformuj**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików. Przed próbą wyleczenia lub usunięcia zainfekowanego pliku, aplikacja utworzy kopię zapasową pliku w przypadku, gdy potrzebujesz przywrócić plik lub jeśli może zostać wyleczony w przyszłości. Po wykryciu zainfekowanych plików, które są częścią aplikacji Sklep Windows, Kaspersky Endpoint Security spróbuje usunąć plik.
Uruchom natychmiast Zaawansowane leczenie *(dostępny tylko w Kaspersky Security Center Console)*	Zaawansowane leczenie podczas wykonywania zadania skanowania antywirusowego na komputerze jest wykonywane tylko wtedy, gdy funkcja Zaawansowane leczenie jest włączona we właściwościach zasady zastosowanej do tego komputera. Jeśli pole zostało zaznaczone, Kaspersky Endpoint Security wyleczy aktywną infekcję od razu po jej wykryciu podczas wykonywania zadania skanowania antywirusowego. Po wyleczeniu aktywnej infekcji, Kaspersky Endpoint Security uruchamia komputer ponownie bez pytania użytkownika. Jeśli pole zostało odznaczone, Kaspersky Endpoint Security nie wyleczy aktywnej infekcji od razu po jej wykryciu podczas wykonywania zadania skanowania antywirusowego. Kaspersky Endpoint Security generuje zdarzenia aktywnej infekcji w lokalnych raportach aplikacji i po stronie Kaspersky Security Center. Aktywna infekcja może zostać wyleczona, gdy zadanie skanowania antywirusowego jest uruchamiane z włączoną funkcją Zaawansowanego leczenia. W ten sposób administrator systemu może wybrać odpowiedni czas na przeprowadzenie Zaawansowanego leczenia i następnie automatyczne ponowne uruchomienie komputera.
Obszar skanowania	Lista obiektów, które są skanowane przez Kaspersky Endpoint Security podczas wykonywania zadania skanowania. Obiekty z obszaru skanowania mogą zawierać pamięć jądra, uruchomione procesy, sektory startowe, miejsce przechowywania kopii zapasowej systemu, dyski twarde lub sieciowe, nośniki wymienne, foldery lub pliki. W programie Kaspersky Endpoint Security for Windows 12.12 poczta e-mail jest wykluczona z zakresu skanowania aplikacji. Skanowanie przychodzących i wychodzących wiadomości e-mail odbywa się za pomocą komponentu Ochrona poczty. Jeśli używasz starszej wersji wtyczki zarządzającej, aplikacja wyklucza pocztę e-mail z zakresu skanowania, nawet jeśli zasady je uwzględniają.
Terminarz skanowania	**Ręcznie**. Tryb uruchamiania, w którym możesz ręcznie uruchomić skanowanie w wygodnym dla siebie momencie. **Zgodnie z terminarzem**. W tym trybie aplikacja uruchamia zadanie skanowania zgodnie z ustalonym terminarzem. Jeśli wybrano ten tryb uruchamiania, zadanie skanowania może również zostać uruchomione ręcznie.
Odrocz uruchomienie zadania po starcie aplikacji o N minut	Odroczone uruchomienie zadania skanowania po uruchomieniu aplikacji. Przy uruchamianiu systemu operacyjnego wiele procesów jest uruchomionych, dlatego korzystne jest odroczenie uruchomienia zadania skanowania zamiast uruchomienie do od razu po uruchomieniu Kaspersky Endpoint Security.
Uruchom pominięte zadania	Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security uruchamia pominięte zadanie, kiedy tylko będzie to możliwe. Zadanie może zostać pominięte, na przykład, jeśli komputer był wyłączony w zaplanowanym czasie uruchomienia zadania. Gdy aplikacja uzyska możliwość wykonania pominiętych zadań, uruchamia zadania losowo w określonym przedziale czasu, aby rozłożyć obciążenie na komputerze. Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security nie uruchamia pominiętych zadań. Zamiast tego uruchomi następne zadanie zgodnie z bieżącym terminarzem.
Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności	Odroczono uruchomienie zadania, gdy zasoby komputera są zajęte. Kaspersky Endpoint Security uruchamia zadanie skanowania, jeśli komputer jest zablokowany lub wygaszacz ekranu jest włączony. Jeśli przerwałeś wykonywanie zadania, na przykład, poprzez odblokowanie komputera, Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane. Ta opcja terminarza umożliwia zaoszczędzenie zasobów komputera w trakcie korzystania z komputera.

Parametr	Opis
Uruchom skanowanie jako	Domyślnie zadanie skanowania jest uruchamiane w imieniu użytkownika, z którego uprawnieniami jesteś zarejestrowany w systemie operacyjnym. Obszar ochrony może zawierać dyski sieciowe lub inne obiekty, które wymagają specjalnych uprawnień dostępu. Możesz wskazać użytkownika, który posiada odpowiednie uprawnienia, w ustawieniach aplikacji i uruchomić zadanie skanowania z poziomu konta tego użytkownika.
Typy plików	Program Kaspersky Endpoint Security traktuje pliki bez rozszerzeń jak pliki wykonywalne. Aplikacja zawsze skanuje pliki wykonywalne bez względu na typy plików wybrane do skanowania. **Wszystkie pliki**. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanować wszystkie pliki bez wyjątku (wszystkie formaty i rozszerzenia). **Pliki skanowane według formatu**. Jeżeli wybierzesz tę opcję, aplikacja będzie skanować tylko infekowalne pliki. Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików. **Pliki skanowane według rozszerzenia**. Jeżeli wybierzesz tę opcję, aplikacja będzie skanować tylko infekowalne pliki. Format pliku będzie określany w oparciu o jego rozszerzenie. Domyślnie program Kaspersky Endpoint Security skanuje pliki według ich formatu. Skanowanie plików według rozszerzenia jest mniej bezpieczne, ponieważ szkodliwy plik może mieć rozszerzenie, które nie znajduje się na liście potencjalnie infekowalnych (na przykład: `.123`).
Skanuj tylko nowe i zmienione pliki	Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.
Pomiń plik skanowany dłużej niż N s	Ograniczenie czasu wykonywania zadania. Po określonym czasie Kaspersky Endpoint Security zatrzyma zadanie. Zadanie nie zostanie oznaczone jako zakończone. Następnym razem, gdy Kaspersky Endpoint Security uruchomi zadanie, zostanie ono uruchomione od początku i zgodnie z terminarzem.
Nie uruchamiaj wielu zadań skanowania w tym samym czasie	Opóźnione rozpoczęcie zadań skanowania, jeśli skanowanie jest już w toku. Kaspersky Endpoint Security będzie wysyłał nowe zadania skanowania, jeśli bieżące skanowanie będzie kontynuowane. Pomaga to zoptymalizować obciążenie komputera. Na przykład załóżmy, że aplikacja uruchomiła zadanie Pełnego skanowania zgodnie z harmonogramem. Jeżeli użytkownik spróbuje uruchomić skanowanie plików z menu kontekstowego, Kaspersky Endpoint Security zapisze to zadanie na listę zadań skanowania plików, a następnie automatycznie uruchomi je po zakończeniu zadania Pełnego skanowania. Jednak Kaspersky Endpoint Security natychmiast uruchamia zadanie skanowania, nawet jeśli jest uruchomione jedno z poniższych zadań skanowania: • Skanowanie dysków wymiennych przy połączeniu. • Skanowanie z menu kontekstowego. • Skanowanie obszarów krytycznych, które zostało uruchomione po wykryciu wskaźnika włamania (Indicator of Compromise, IoC). Jeśli to pole wyboru jest odznaczone, Kaspersky Endpoint Security pozwala uruchamiać wiele zadań skanowania w tym samym czasie. Wykonywanie wielu zadań skanowania wymaga większych zasobów komputera.
Skanuj archiwa	Skanowanie ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE i innych archiwów. Aplikacja skanuje archiwa nie tylko według rozszerzenia, ale także według formatu. Podczas sprawdzania archiwów aplikacja przeprowadzi cykliczne rozpakowywanie. Pozwala to na wykrywanie zagrożeń w archiwach wielopoziomowych (archiwach wewnątrz archiwów).
Skanuj pakiety dystrybucyjne	Skanowanie pakietów dystrybucyjnych aplikacji firm trzecich.
Skanuj pliki w formatach Microsoft Office	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty. Aplikacja skanuje pliki w formacie Office, które są mniejsze niż 1 MB, niezależnie od tego, czy pole wyboru jest zaznaczone, czy nie.

Parametr	Opis
Skanuj pliki formatu poczty elektronicznej	Skanowanie plików w formacie poczty elektronicznej i bazy danych e-mail. Aplikacja skanuje pliki PST i OST używane przez klienty poczty MS Outlook i Poczta systemu Windows, a także pliki EML. Kaspersky Endpoint Security nie obsługuje 64-bitowych wersji klienta poczty Microsoft Outlook. Oznacza to, że Kaspersky Endpoint Security nie skanuje plików Microsoft Outlook (plików PST i OST), jeśli na komputerze jest zainstalowana 64-bitowa wersja Microsoft Outlook, nawet jeśli poczta jest objęta zakresem skanowania. Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security rozkłada pliki w formatach pocztowych na składniki (nagłówek, ciało, załączniki) i skanuje je w poszukiwaniu zagrożeń. Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security skanuje pliki w formatach pocztowych jako pojedyncze pliki. Jeśli w plikach PST lub OST zostanie wykryty złośliwy obiekt, Kaspersky Endpoint Security unieszkodliwi go zgodnie z wybraną akcją (na przykład wyleczy lub usunie plik). Jeśli w plikach innych klientów poczty e-mail (np. Mozilla Thunderbird) zostanie wykryty złośliwy plik, Kaspersky Endpoint Security oznaczy tylko zainfekowaną wiadomość. Musisz ręcznie usunąć wiadomość z zainfekowanym załącznikiem.
Skanuj archiwa zabezpieczone hasłem	Jeżeli pole jest zaznaczone, aplikacja skanuje archiwa zabezpieczone hasłem. Zanim pliki w archiwum zostaną przeskanowane, zostaniesz poproszony o wpisanie hasła. Jeśli pole nie jest zaznaczone, aplikacja pomija skanowanie archiwów chronionych hasłem.
Nie rozpakowuj dużych plików złożonych	Jeżeli to pole jest zaznaczone, aplikacja nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość. Jeśli pole nie jest zaznaczone, aplikacja skanuje pliki złożone o wszystkich rozmiarach. Aplikacja skanuje pliki o dużych rozmiarach, które zostają wypakowane z archiwów niezależnie od tego, czy pole jest zaznaczone.
Uczenie maszynowe i analiza sygnatur	Metoda uczenia maszynowego i analiza sygnatur używa baz danych Kaspersky Endpoint Security, które zawierają opisy znanych zagrożeń oraz metody ich neutralizowania. Ochrona korzystająca z tej metody zapewnia minimalny dopuszczalny poziom ochrony. W oparciu o zalecenia ekspertów z Kaspersky, uczenie maszynowe i analiza sygnatur jest zawsze włączona.
Analiza heurystyczna	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa. Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.
Technologia iSwift *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.
Technologia iChecker *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).

Skanowanie napędów wymiennych po ich podłączeniu do komputera

Kaspersky Endpoint Security skanuje wszystkie pliki, które uruchamiasz lub kopiujesz nawet wtedy, gdy plik znajduje się na dysku wymiennym (komponent Ochrona plików). Aby zapobiec rozprzestrzenianiu wirusów i innych szkodliwych programów, możesz skonfigurować automatyczne skanowania dysków wymiennych po ich podłączeniu do komputera. Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeżeli leczenie nie powiedzie się, Kaspersky Endpoint Security usunie pliki. Komponent zapewnia ochronę komputera poprzez wykonywanie skanowań, które implementują uczenie maszynowe, analizę heurystyczną (wysoki poziom) i analizę przy użyciu sygnatur. Kaspersky Endpoint Security używa także technologii optymalizacji skanowania iSwift i iChecker. Technologie są zawsze włączone i nie mogą zostać wyłączone.

Jak w Konsoli administracyjnej (MMC) skonfigurować uruchamianie Skanowania dysków wymiennych?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zadania lokalne** → **Skanowanie dysków wymiennych**.
4. Z listy rozwijalnej **Akcja po podłączeniu dysku wymiennego** wybierz **Skanowanie szczegółowe** lub **Szybkie skanowanie**.
5. Skonfiguruj zaawansowane opcje Skanowania dysków wymiennych (patrz tabela poniżej).
6. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console skonfigurować uruchamianie Skanowania dysków wymiennych?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Skanowanie dysków wymiennych**.
5. Użyj przełącznika **Skanowanie dysków wymiennych WŁĄCZONE**, aby włączyć lub wyłączyć komponent.
6. W bloku **Typ skanowania** wybierz **Skanowanie szczegółowe** lub **Szybkie skanowanie**.
7. Skonfiguruj zaawansowane opcje Skanowania dysków wymiennych (patrz tabela poniżej).
8. Zapisz swoje zmiany.

Jak w interfejsie aplikacji skonfigurować uruchamianie Skanowania dysków wymiennych?

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. Na liście zadań wybierz zadanie skanowania i kliknij ⚙.

3. Użyj przełącznika **Skanowanie dysków wymiennych**, aby włączyć lub wyłączyć skanowanie nośników wymiennych po podłączeniu do komputera.

4. Skonfiguruj zaawansowane opcje Skanowania dysków wymiennych (patrz tabela poniżej).

5. Zapisz swoje zmiany.

W wyniku tego działania Kaspersky Endpoint Security uruchomi Skanowanie dysków wymiennych dla dysków wymiennych, które nie są większe niż określony maksymalny rozmiar. Jeśli zadanie *Skanowanie dysków wymiennych* nie jest wyświetlane, oznacza to, że administrator zabronił używania zadań lokalnych w zasadzie.

Ustawienia zadania Skanowanie dysków wymiennych

Parametr	Opis
Typ skanowania	**Skanowanie szczegółowe**. Jeśli ta opcja została wybrana, po podłączeniu dysku wymiennego, Kaspersky Endpoint Security skanuje wszystkie pliki, w tym pliki zagnieżdżone w obiektach złożonych, archiwa, pakiety dystrybucyjne oraz pliki w formatach Office. Kaspersky Endpoint Security nie skanuje plików w formatach pocztowych ani archiwach chronionych hasłem. **Szybkie skanowanie**. Jeśli ta opcja jest zaznaczona, po podłączeniu nośnika wymiennego, Kaspersky Endpoint Security skanuje tylko pliki określonych formatów, które są najbardziej podatne na infekcje, i nie rozpakowuje obiektów złożonych.
Maksymalny rozmiar dysku (MB)	Jeżeli pole jest zaznaczone, Kaspersky Endpoint Security wykona wybrane działanie na nośnikach wymiennych, których rozmiar nie przekracza zdefiniowanej wartości. Jeśli rozmiar dysku wymiennego przekroczy skonfigurowaną wartość, Kaspersky Endpoint Security pominie skanowanie. Jeśli pole wyboru nie jest zaznaczone, Kaspersky Endpoint Security wykona wybrane działanie na dyskach wymiennych o dowolnym rozmiarze.
Ukryj pasek postępu skanowania	Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security wyświetli postęp skanowania nośników wymiennych w oddzielnym oknie oraz w sekcji **Zadania**. Jeśli pole jest odznaczone, Kaspersky Endpoint Security uruchomi skanowanie nośników wymiennych w tle.
Zapobiegaj zatrzymywaniu skanowania przez użytkowników	Jeśli to pole jest zaznaczone, wówczas dla zadania skanowania dysków wymiennych w lokalnym interfejsie Kaspersky Endpoint Security, nie są dostępne następujące przyciski: **Zatrzymaj** w sekcji **Zadania** oraz **Zatrzymaj** w sekcji skanowania dysków wymiennych.

Skanowanie w tle

Skanowanie w tle to tryb skanowania programu Kaspersky Endpoint Security, który nie wyświetla powiadomień. Skanowanie w tle wymaga mniej zasobów komputera niż inne typy skanowań (takie jak pełne skanowanie). W tym trybie Kaspersky Endpoint Security skanuje obiekty startowe, sektory startowe, pamięć systemową i partycje systemowe.

Aby zachować zasoby komputera, zalecane jest użycie zadania skanowania w tle zamiast zadania pełnego skanowania. Nie wpłynie to na poziom ochrony komputera. Zadania te mają taki sam obszar skanowania. Aby zoptymalizować obciążenie komputera, aplikacja nie uruchamia jednocześnie zadania pełnego skanowania i zadania skanowania w tle. Jeśli uruchomiono już zadanie Pełne skanowanie, Kaspersky Endpoint Security nie uruchomi zadania Skanowanie w tle przez siedem dni po zakończeniu zadania Pełnego skanowania.

Skanowanie w tle jest uruchamiane w następujących przypadkach:

- Po aktualizacji antywirusowych baz danych.
- 30 minut po uruchomieniu Kaspersky Endpoint Security.
- Co sześć godzin.
- Gdy komputer jest w stanie bezczynności przez pięć minut lub dłużej (komputer jest zablokowany lub włączony jest wygaszacz ekranu).

Skanowanie w tle, gdy komputer jest w stanie bezczynności, zostaje przerwane, gdy którykolwiek z poniższych warunków jest prawdziwy:

- Komputer działa w trybie aktywnym.

  Jeśli skanowanie w tle nie było wykonywane dłużej niż dziesięć dni temu, skanowanie nie jest przerywane.

- Komputer (laptop) przełączył się w tryb pracy na bateriach.

Jeśli uruchamiasz zadanie skanowania w tle, Kaspersky Endpoint Security nie skanuje plików, których zawartość znajduje się w magazynie w chmurze OneDrive.

Jak w Konsoli administracyjnej (MMC) włączyć skanowanie w tle?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zadania lokalne** → **Skanowanie w tle**.
4. Użyj pola **Włącz skanowanie w tle**, aby włączyć lub wyłączyć skanowanie w tle.
5. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console włączyć skanowanie w tle?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Ochrona plików**.
5. W sekcji **Skanowanie w tle** użyj przełącznika **Skanowanie w tle WŁĄCZONE**, aby włączyć lub wyłączyć skanowanie w tle.
6. Zapisz swoje zmiany.

Jak w interfejsie aplikacji włączyć skanowanie w tle?

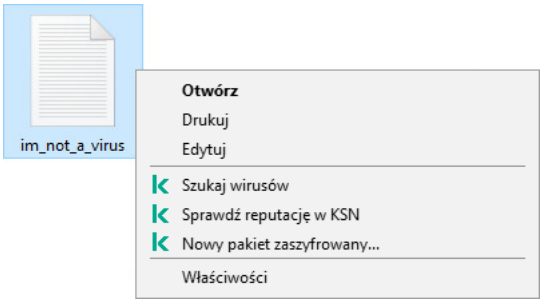
1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. Na liście zadań wybierz zadanie skanowania i kliknij ⚙.
3. Użyj przełącznika **Skanowanie w tle**, aby włączyć lub wyłączyć skanowanie w tle.
4. Zapisz swoje zmiany.

Jeśli *Skanowanie w tle* nie jest wyświetlane, to oznacza, że administrator zabronił używania zadań lokalnych w zasadzie.

Skanowanie z menu kontekstowego

Kaspersky Endpoint Security umożliwia uruchomienie skanowania pojedynczych plików w poszukiwaniu wirusów i innych szkodliwych programów z poziomu menu kontekstowego (patrz rysunek poniżej).

Jeśli uruchamiasz skanowanie z poziomu menu kontekstowego, Kaspersky Endpoint Security nie skanuje plików, których zawartość znajduje się w magazynie w chmurze OneDrive.



Skanowanie z menu kontekstowego

Jak w Konsoli administracyjnej (MMC) skonfigurować Skanowanie z menu kontekstowego?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zadania lokalne** → **Skanowanie z menu kontekstowego**.
4. Skonfiguruj Skanowanie z menu kontekstowego (patrz tabela poniżej).
5. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console skonfigurować Skanowanie z menu kontekstowego?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Ochrona plików**.
5. W obszarze **Skanowanie z menu kontekstowego** skonfiguruj Skanowanie z menu kontekstowego (patrz tabela poniżej).
6. Zapisz swoje zmiany.

Jak w interfejsie aplikacji skonfigurować Skanowanie z menu kontekstowego?

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. Na liście zadań wybierz zadanie skanowania i kliknij ⚙.
3. Skonfiguruj Skanowanie z menu kontekstowego (patrz tabela poniżej).
4. Zapisz swoje zmiany.

Jeśli zadanie *Skanowanie z menu kontekstowego* nie jest wyświetlane, oznacza to, że administrator zabronił używania zadań lokalnych w zasadzie.

Ustawienia zadania Skanowanie z menu kontekstowego

Parametr	Opis
Poziom ochrony	Kaspersky Endpoint Security może używać różnych grup ustawień uruchamiania skanowania. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane *poziomami ochrony*. • **Wysoki**. Kaspersky Endpoint Security skanuje wszystkie typy plików. Podczas skanowania plików złożonych aplikacja skanuje archiwa, pakiety dystrybucyjne i pliki w formatach biurowych, ale nie skanuje archiwów chronionych hasłem. Po ustawieniu tego poziomu bezpieczeństwa aplikacja korzysta z analizy heurystycznej z poziomem szczegółowości **Poziom szczegółowy**. • **Zalecany**. Kaspersky Endpoint Security skanuje wszystkie typy plików. Podczas skanowania plików złożonych aplikacja skanuje archiwa, pakiety dystrybucyjne i pliki w formatach biurowych, ale nie skanuje archiwów chronionych hasłem. Po ustawieniu tego poziomu bezpieczeństwa aplikacja korzysta z analizy heurystycznej z poziomem szczegółowości **Poziom średni**. • **Niski**. Kaspersky Endpoint Security skanuje tylko określone formaty plików. Podczas skanowania plików złożonych aplikacja skanuje archiwa, pakiety dystrybucyjne i pliki w formatach biurowych, ale nie skanuje archiwów chronionych hasłem. Po ustawieniu tego poziomu bezpieczeństwa aplikacja korzysta z analizy heurystycznej z poziomem szczegółowości **Poziom niski**.
Działanie po wykryciu zagrożenia	**Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik. **Wylecz; poinformuj, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeśli leczenie się nie powiedzie, Kaspersky Endpoint Security doda informacje o wykrytych zainfekowanych plikach do listy aktywnych zagrożeń. **Poinformuj**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików.
Typy plików	Program Kaspersky Endpoint Security traktuje pliki bez rozszerzeń jak pliki wykonywalne. Aplikacja zawsze skanuje pliki wykonywalne bez względu na typy plików wybrane do skanowania. **Wszystkie pliki**. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanować wszystkie pliki bez wyjątku (wszystkie formaty i rozszerzenia). **Pliki skanowane według formatu**. Jeżeli wybierzesz tę opcję, aplikacja będzie skanować tylko infekowalne pliki. Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików. **Pliki skanowane według rozszerzenia**. Jeżeli wybierzesz tę opcję, aplikacja będzie skanować tylko infekowalne pliki. Format pliku będzie określany w oparciu o jego rozszerzenie. Domyślnie program Kaspersky Endpoint Security skanuje pliki według ich formatu. Skanowanie plików według rozszerzenia jest mniej bezpieczne, ponieważ szkodliwy plik może mieć rozszerzenie, które nie znajduje się na liście potencjalnie infekowalnych (na przykład: `.123`).
Skanuj tylko nowe i zmienione pliki	Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.
Pomiń plik skanowany dłużej niż N s	Ograniczenie czasu wykonywania zadania. Po określonym czasie Kaspersky Endpoint Security zatrzyma zadanie. Zadanie nie zostanie oznaczone jako zakończone. Następnym razem, gdy Kaspersky Endpoint Security uruchomi zadanie, zostanie ono uruchomione od początku i zgodnie z terminarzem.
Skanuj archiwa	Skanowanie ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE i innych archiwów. Aplikacja skanuje archiwa nie tylko według rozszerzenia, ale także według formatu. Podczas sprawdzania archiwów aplikacja przeprowadzi cykliczne rozpakowywanie. Pozwala to na wykrywanie zagrożeń w archiwach wielopoziomowych (archiwach wewnątrz archiwów).
Skanuj pakiety dystrybucyjne	To pole włącza/wyłącza skanowanie pakietów dystrybucyjnych.

Parametr	Opis
Skanuj pliki w formatach Microsoft Office	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty. Aplikacja skanuje pliki w formacie Office, które są mniejsze niż 1 MB, niezależnie od tego, czy pole wyboru jest zaznaczone, czy nie.
Skanuj pliki formatu poczty elektronicznej	Skanowanie plików w formacie poczty elektronicznej i bazy danych e-mail. Aplikacja skanuje pliki PST i OST używane przez klienty poczty MS Outlook i Poczta systemu Windows, a także pliki EML. Kaspersky Endpoint Security nie obsługuje 64-bitowych wersji klienta poczty Microsoft Outlook. Oznacza to, że Kaspersky Endpoint Security nie skanuje plików Microsoft Outlook (plików PST i OST), jeśli na komputerze jest zainstalowana 64-bitowa wersja Microsoft Outlook, nawet jeśli poczta jest objęta zakresem skanowania. Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security rozkłada pliki w formatach pocztowych na składniki (nagłówek, ciało, załączniki) i skanuje je w poszukiwaniu zagrożeń. Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security skanuje pliki w formatach pocztowych jako pojedyncze pliki. Jeśli w plikach PST lub OST zostanie wykryty złośliwy obiekt, Kaspersky Endpoint Security unieszkodliwi go zgodnie z wybraną akcją (na przykład wyleczy lub usunie plik). Jeśli w plikach innych klientów poczty e-mail (np. Mozilla Thunderbird) zostanie wykryty złośliwy plik, Kaspersky Endpoint Security oznaczy tylko zainfekowaną wiadomość. Musisz ręcznie usunąć wiadomość z zainfekowanym załącznikiem.
Skanuj archiwa zabezpieczone hasłem	Jeżeli pole jest zaznaczone, aplikacja skanuje archiwa zabezpieczone hasłem. Zanim pliki w archiwum zostaną przeskanowane, zostaniesz poproszony o wpisanie hasła. Jeśli pole nie jest zaznaczone, aplikacja pomija skanowanie archiwów chronionych hasłem.
Nie rozpakowuj dużych plików złożonych	Jeżeli to pole jest zaznaczone, aplikacja nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość. Jeśli pole nie jest zaznaczone, aplikacja skanuje pliki złożone o wszystkich rozmiarach. Aplikacja skanuje pliki o dużych rozmiarach, które zostają wypakowane z archiwów niezależnie od tego, czy pole jest zaznaczone.
Uczenie maszynowe i analiza sygnatur	Metoda uczenia maszynowego i analiza sygnatur używa baz danych Kaspersky Endpoint Security, które zawierają opisy znanych zagrożeń oraz metody ich neutralizowania. Ochrona korzystająca z tej metody zapewnia minimalny dopuszczalny poziom ochrony. W oparciu o zalecenia ekspertów z Kaspersky, uczenie maszynowe i analiza sygnatur jest zawsze włączona.
Analiza heurystyczna	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa. Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.
Technologia iSwift	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.
Technologia iChecker	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).

Sprawdzanie integralności aplikacji

Kaspersky Endpoint Security sprawdza, czy moduły aplikacji nie są uszkodzone lub zmodyfikowane. Na przykład, jeśli biblioteka aplikacji posiada nieprawidłowy podpis cyfrowy, zostanie ona uznana za uszkodzoną. Zadanie *Sprawdzanie integralności aplikacji* jest przeznaczone do sprawdzania plików aplikacji. Uruchom zadanie *Sprawdzanie integralności aplikacji*, jeśli Kaspersky Endpoint Security wykrył szkodliwy obiekt, ale go nie zneutralizował.

Możesz utworzyć zadanie *Sprawdzanie integralności aplikacji* tylko w konsoli Kaspersky Security Center Web Console i w Konsoli administracyjnej. Nie można utworzyć zadania w konsoli Kaspersky Security Center Cloud Console.

Naruszenia integralności aplikacji mogą pojawić się w następujących przypadkach:

- Szkodliwy obiekt zmodyfikował pliki Kaspersky Endpoint Security. W tym przypadku przeprowadź procedurę przywracania Kaspersky Endpoint Security przy pomocy narzędzi systemu operacyjnego. Po przywróceniu uruchom pełne skanowanie komputera i powtórz sprawdzanie integralności.
- Podpis cyfrowy utracił ważność. W tym przypadku zaktualizuj Kaspersky Endpoint Security.

Jak uruchomić sprawdzanie integralności aplikacji za pomocą Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Sprawdzanie integralności aplikacji**.

Krok 2. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 3. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz uruchamiania zadania, na przykład, ręcznie lub gdy wykrywana jest epidemia wirusów.

Krok 4. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład, *Sprawdzanie integralności po zainfekowaniu komputera*.

Krok 5. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania. W wyniku tego program Kaspersky Endpoint Security będzie sprawdzał integralność aplikacji. Możesz także skonfigurować terminarz sprawdzania integralności aplikacji we właściwościach zadania (patrz tabela poniżej).

Jak uruchomić sprawdzanie integralności aplikacji za pomocą konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Sprawdzanie integralności aplikacji**.

   c. W polu **Nazwa zadania** wpisz krótki opis, na przykład *Sprawdzanie integralności aplikacji po infekcji komputera*.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.

5. Wybierz konto do uruchomienia zadania. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika.

6. Zakończ działanie Kreatora.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Zaznacz pole obok zadania.

W wyniku tego program Kaspersky Endpoint Security będzie sprawdzał integralność aplikacji. Możesz także skonfigurować terminarz sprawdzania integralności aplikacji we właściwościach zadania (patrz tabela poniżej).

Jak w interfejsie aplikacji uruchomić sprawdzanie integralności?

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. To spowoduje otwarcie listy zadań; wybierz zadanie *Sprawdzanie integralności aplikacji* i kliknij **Uruchom**.

W wyniku tego program Kaspersky Endpoint Security będzie sprawdzał integralność aplikacji. Możesz także skonfigurować terminarz sprawdzania integralności aplikacji we właściwościach zadania (patrz tabela poniżej). Jeśli zadanie *Sprawdzanie integralności aplikacji* nie jest wyświetlane, oznacza to, że administrator zabronił używania zadań lokalnych w zasadzie.

Ustawienia zadania Sprawdzanie integralności

Parametr	Opis
Terminarz skanowania	**Ręcznie**. Tryb uruchamiania, w którym możesz ręcznie uruchomić skanowanie w wygodnym dla siebie momencie. **Zgodnie z terminarzem**. W tym trybie aplikacja uruchamia zadanie skanowania zgodnie z ustalonym terminarzem. Jeśli wybrano ten tryb uruchamiania, zadanie skanowania może również zostać uruchomione ręcznie.
Uruchom pominięte zadania	Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security uruchamia pominięte zadanie, kiedy tylko będzie to możliwe. Zadanie może zostać pominięte, na przykład, jeśli komputer był wyłączony w zaplanowanym czasie uruchomienia zadania. Gdy aplikacja uzyska możliwość wykonania pominiętych zadań, uruchamia zadania losowo w określonym przedziale czasu, aby rozłożyć obciążenie na komputerze. Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security nie uruchamia pominiętych zadań. Zamiast tego uruchomi następne zadanie zgodnie z bieżącym terminarzem.
Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności	Odroczono uruchomienie zadania, gdy zasoby komputera są zajęte. Kaspersky Endpoint Security uruchamia zadanie skanowania, jeśli komputer jest zablokowany lub wygaszacz ekranu jest włączony. Jeśli przerwałeś wykonywanie zadania, na przykład, poprzez odblokowanie komputera, Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane. Ta opcja terminarza umożliwia zaoszczędzenie zasobów komputera w trakcie korzystania z komputera.

Modyfikowanie obszaru skanowania

Obszar skanowania to lista ścieżek do folderów oraz ścieżek, które Kaspersky Endpoint Security skanuje podczas wykonywania zadania. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

Aby edytować obszar skanowania, zalecane jest użycie zadania *Skanowanie niestandardowe*. Eksperci z Kaspersky zalecają, aby nie zmieniać obszaru skanowania zadania *Pełne skanowanie* ani *Skanowanie obszarów krytycznych*.

Kaspersky Endpoint Security posiada następujące predefiniowane obiekty jako część obszaru skanowania:

- **Pamięć systemowa**.
- **Uruchomione procesy i obiekty startowe**.

  Pamięć zajęta przez procesy i pliki wykonywalne aplikacji, które są uruchamiane przy starcie systemu.
- **Sektory startowe dysków**.

  Sektory startowe dysków wymiennych i dysku twardego.
- **Kopia zapasowa systemu**.

  Zawartość folderu informacji o woluminie systemowym.
- **Wszystkie urządzenia zewnętrzne**.

- **Wszystkie dyski twarde**.
- **Wszystkie dyski sieciowe**.

> W programie Kaspersky Endpoint Security for Windows 12.12 poczta e-mail jest wykluczona z zakresu skanowania aplikacji. Skanowanie przychodzących i wychodzących wiadomości e-mail odbywa się za pomocą komponentu Ochrona poczty. Jeśli używasz starszej wersji wtyczki zarządzającej, aplikacja wyklucza pocztę e-mail z zakresu skanowania, nawet jeśli zasady je uwzględniają.

> Zalecamy utworzenie osobnego zadania skanowania dysków sieciowych lub folderów współdzielonych. W ustawieniach *Skanowanie w poszukiwaniu złośliwego oprogramowania* zadanie, określ użytkownika, który ma prawo zapisu na tym dysku; jest to konieczne w celu ograniczenia wykrytych zagrożeń. Jeśli serwer, na którym znajduje się dysk sieciowy, ma własne narzędzia zabezpieczające, nie uruchamiaj zadania skanowania tego dysku. W ten sposób można uniknąć podwójnego sprawdzania danego obiektu i zwiększyć wydajność serwera.

Aby wykluczyć foldery lub pliki z obszaru skanowania, dodaj folder lub plik do strefy zaufanej.

Jak w Konsoli administracyjnej (MMC) edytować obszar skanowania?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zadania**.
3. Wybierz zadanie skanowania i kliknij je dwukrotnie, aby otworzyć właściwości zadania.
   W razie konieczności utworzyć zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.
4. W oknie właściwości zadania wybierz sekcję **Ustawienia**.
5. W sekcji **Obszar skanowania** kliknij **Ustawienia**.
6. W otwartym oknie wybierz obiekty, które chcesz dodać do obszaru skanowania lub wykluczyć z niego.
7. Jeśli chcesz dodać nowy obiekt do obszaru skanowania:
   a. Kliknij **Dodaj**.
   b. W polu **Obiekt** wprowadź ścieżkę do folderu lub pliku.

Użyj masek:

- Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.

- Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.

- Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

W dowolnym miejscu ścieżki pliku lub folderu można używać masek. Na przykład, jeśli chcesz, aby zakres skanowania obejmował folder Pobrane dla wszystkich kont użytkowników na komputerze, należy wprowadzić maskę `C:\Users\*\Downloads\`.

Obiekt **Ten komputer** na liście zasobów plikowych komputera zawiera następujące obiekty: **Wszystkie dyski twarde**, **Wszystkie dyski sieciowe** and **Wszystkie dyski wymienne**.

Możesz wykluczyć obiekt ze skanowań bez usuwania go z listy obiektów w obszarze skanowania. W tym celu odznacz pole obok obiektu.

8. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak w konsoli Web Console i Cloud Console edytować obszar skanowania?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie skanowania.

   Zostanie otwarte okno właściwości zadania. W razie konieczności utworzyć zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. W sekcji **Obszar skanowania** wybierz obiekty, które chcesz dodać do obszaru skanowania lub wykluczyć z niego.

5. Jeśli chcesz dodać nowy obiekt do obszaru skanowania:

   a. Kliknij **Dodaj**.

   b. Wprowadź ścieżkę do pliku lub folderu.

Użyj masek:

- Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.

- Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.

- Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

W dowolnym miejscu ścieżki pliku lub folderu można używać masek. Na przykład, jeśli chcesz, aby zakres skanowania obejmował folder Pobrane dla wszystkich kont użytkowników na komputerze, należy wprowadzić maskę `C:\Users\*\Downloads\`.

Możesz wykluczyć obiekt ze skanowań bez usuwania go z listy obiektów w obszarze skanowania. W tym celu ustaw przycisk przełącznika obok obiektu na pozycję wyłączenia.

6. Zapisz swoje zmiany.

Jak w interfejsie aplikacji edytować obszar skanowania?

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.

2. To spowoduje otwarcie listy zadań; wybierz zadanie *Skanowanie niestandardowe* i kliknij **Wybierz**.

   Możesz także edytować obszar skanowania dla innych zadań. Eksperci z Kaspersky zalecają, aby nie zmieniać obszaru skanowania zadania *Pełne skanowanie* ani *Skanowanie obszarów krytycznych*.

3. W otwartym oknie wybierz obiekty, które chcesz dodać do obszaru skanowania.

4. Zapisz swoje zmiany.

Jeśli zadanie skanowania nie jest wyświetlane, oznacza to, że administrator zabronił użycia zadań lokalnych w zasadzie.

Uruchamianie zaplanowanego skanowania

Używanie zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania* może być czasochłonne i zwiększać wykorzystanie zasobów komputera przez Kaspersky Endpoint Security. W związku z tym zaleca się wybranie optymalnego czasu uruchomienia zadania, aby zminimalizować jego wpływ na działanie innych aplikacji.

Jeśli na przykład pracownicy w Twojej organizacji pracują według ścisłego harmonogramu, możesz skonfigurować skanowanie komputera tak, aby uruchamiało się w nocy lub w weekendy. Jeżeli z jakiegoś powodu zadania nie będzie możliwe (na przykład komputer nie będzie włączony o określonym czasie), można skonfigurować automatyczne uruchamianie pominiętego zadania przy najbliższej możliwej okazji. Należy zachować ostrożność podczas korzystania z tej funkcji, ponieważ może ona spowolnić działanie aplikacji na komputerze użytkownika po włączeniu go rano.

Jeśli nie możesz ustalić optymalnego harmonogramu skanowania odpowiadającego Twoim potrzebom, możesz skonfigurować skanowanie tak, aby zostało uruchomione, gdy spełniony zostanie jeden z następujących warunków specjalnych:

- Po aktualizacji baz danych.

  Kaspersky Endpoint Security uruchamia skanowanie komputera wraz z zaktualizowanymi bazami danych.

- Po uruchomieniu aplikacji.

  Kaspersky Endpoint Security uruchamia skanowanie komputera, gdy od uruchomienia aplikacji minie określony czas. Przy uruchamianiu systemu operacyjnego wiele procesów jest uruchomionych, dlatego korzystne jest odroczenie uruchomienia zadania skanowania zamiast uruchomienie do od razu po uruchomieniu Kaspersky Endpoint Security.

- Funkcja Wake-on-LAN.

  Kaspersky Endpoint Security uruchamia skanowanie komputera zgodnie z terminarzem nawet wtedy, gdy komputer jest wyłączony. Aby to zrobić, aplikacja używa funkcji Wake-on-LAN systemu operacyjnego. Funkcja Wake-on-LAN umożliwia zdalne włączenie komputera poprzez wysłanie specjalnego sygnału przez sieć lokalną. Aby użyć tej funkcji, musisz włączyć Wake-on-LAN w ustawieniach BIOS-u.

  Możesz skonfigurować uruchamianie skanowania przy użyciu Wake-on-LAN tylko dla zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania* w Kaspersky Security Center. Nie możesz włączyć Wake-on-LAN dla skanowania komputera w interfejsie aplikacji.

- Kiedy komputer jest w stanie bezczynności.

  Kaspersky Endpoint Security uruchamia skanowanie komputera zgodnie z terminarzem, gdy wygaszacz ekranu jest aktywny lub ekran jest zablokowany. Jeśli użytkownik odblokuje komputer, Kaspersky Endpoint Security wstrzyma skanowanie. W takim przypadku pełne skanowanie może potrwać kilka dni.

- Gdy zadanie zostało pominięte.

  Kaspersky Endpoint Security uruchomi je, gdy tylko będzie to możliwe. Zadanie może zostać pominięte, na przykład, jeśli komputer był wyłączony w zaplanowanym czasie uruchomienia zadania. Gdy aplikacja uzyska możliwość wykonania pominiętych zadań, uruchamia zadania losowo w określonym przedziale czasu, aby rozłożyć obciążenie na komputerze.

Jak w konsoli Web Console i Cloud Console skonfigurować terminarz skanowania?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie skanowania.

   Zostanie otwarte okno właściwości zadania.

3. W oknie właściwości zadania wybierz zakładkę **Terminarz**.

4. Skonfiguruj terminarz zadania skanowania.

5. W zależności od wybranej częstotliwości, skonfiguruj ustawienia zaawansowane, które określają terminarz uruchamiania zadania (patrz tabela poniżej).

6. Zapisz swoje zmiany.

Jak w interfejsie aplikacji skonfigurować terminarz skanowania?

Możesz skonfigurować terminarz skanowania tylko wtedy, gdy zasada nie jest stosowana do komputera. Dla komputerów pracujących pod kontrolą zasady możesz skonfigurować terminarz zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania* w Kaspersky Security Center.

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. Na liście zadań wybierz zadanie skanowania i kliknij ⚙.

   Możesz skonfigurować terminarz uruchamiania Pełnego skanowania, Skanowania obszarów krytycznych lub Sprawdzania integralności. Możesz tylko ręcznie uruchomić Skanowanie obiektów.
3. Kliknij **Terminarz skanowania**.
4. W otwartym oknie skonfiguruj terminarz uruchamiania zadania skanowania.
5. W zależności od wybranej częstotliwości, skonfiguruj ustawienia zaawansowane, które określają terminarz uruchamiania zadania (patrz tabela poniżej).
6. Zapisz swoje zmiany.

Ustawienia terminarza skanowania

Parametr	Opis
Terminarz skanowania	**Ręcznie**. Tryb uruchamiania, w którym możesz ręcznie uruchomić skanowanie w wygodnym dla siebie momencie. **Zgodnie z terminarzem**. W tym trybie aplikacja uruchamia zadanie skanowania zgodnie z ustalonym terminarzem. Jeśli wybrano ten tryb uruchamiania, zadanie skanowania może również zostać uruchomione ręcznie.
Odrocz uruchomienie zadania po starcie aplikacji o N minut	Odroczone uruchomienie zadania skanowania po uruchomieniu aplikacji. Przy uruchamianiu systemu operacyjnego wiele procesów jest uruchomionych, dlatego korzystne jest odroczenie uruchomienia zadania skanowania zamiast uruchomienie do od razu po uruchomieniu Kaspersky Endpoint Security.
Uruchom pominięte zadania	Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security uruchamia pominięte zadanie, kiedy tylko będzie to możliwe. Zadanie może zostać pominięte, na przykład, jeśli komputer był wyłączony w zaplanowanym czasie uruchomienia zadania. Gdy aplikacja uzyska możliwość wykonania pominiętych zadań, uruchamia zadania losowo w określonym przedziale czasu, aby rozłożyć obciążenie na komputerze. Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security nie uruchamia pominiętych zadań. Zamiast tego uruchomi następne zadanie zgodnie z bieżącym terminarzem.
Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności	Odroczono uruchomienie zadania, gdy zasoby komputera są zajęte. Kaspersky Endpoint Security uruchamia zadanie skanowania, jeśli komputer jest zablokowany lub wygaszacz ekranu jest włączony. Jeśli przerwałeś wykonywanie zadania, na przykład, poprzez odblokowanie komputera, Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane. Ta opcja terminarza umożliwia zaoszczędzenie zasobów komputera w trakcie korzystania z komputera.
Używaj automatycznie losowego opóźnienia dla uruchamiania zadań *(dostępny tylko w Kaspersky Security Center Console)*	Jeśli pole jest zaznaczone, zadanie nie jest uruchamiane ściśle zgodnie z terminarzem, ale losowo w obrębie pewnego przedziału czasu, czyli czasy uruchomień zadania są rozłożone w czasie. Losowe czasy uruchomień pomagają w uniknięciu dostępu do Serwera administracyjnego przez znaczną liczbę komputerów jednocześnie, gdy zadanie jest uruchomione zgodnie z terminarzem. Zakres losowych czasów uruchomień jest automatycznie wyliczany po utworzeniu zadania, w zależności od liczby komputerów, do których przypisano zadanie. Następnie zadanie jest zawsze uruchamiane w wyliczonym czasie uruchomienia. Jednakże za każdym razem, gdy ustawienia zadania są modyfikowane lub zadanie jest uruchamiane ręcznie, obliczony czas uruchomienia zmienia się. Jeśli pole jest odznaczone, zadanie jest uruchamiane dokładnie o zaplanowanym czasie.
Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)	Jeśli to pole wyboru jest zaznaczone, zadanie zostanie uruchomione na komputerach o przypadkowej godzinie w określonym przedziale czasowym. Losowe czasy uruchomień pomagają w uniknięciu dostępu do Serwera administracyjnego przez znaczną liczbę komputerów jednocześnie, gdy zadanie jest uruchomione zgodnie z terminarzem. Jeśli pole jest odznaczone, zadanie jest uruchamiane dokładnie o zaplanowanym czasie.

Parametr	Opis
Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż (min) *(dostępny tylko w Kaspersky Security Center Console)*	Ograniczenie czasu wykonywania zadania. Po określonym czasie Kaspersky Endpoint Security zatrzyma zadanie. Zadanie nie zostanie oznaczone jako zakończone. Następnym razem, gdy Kaspersky Endpoint Security uruchomi zadanie, zostanie ono uruchomione od początku i zgodnie z terminarzem. Aby zmniejszyć czas wykonania zadania, możesz, na przykład, skonfigurować obszar skanowania lub zoptymalizować skanowanie.
Włącz urządzenia przed uruchomieniem zadania (min) przy użyciu funkcji Wake-on-LAN *(dostępny tylko w Kaspersky Security Center Console)*	Jeśli pole jest zaznaczone, system operacyjny komputera ma określony czas realizacji na zakończenie uruchamiania przed uruchomieniem zadania. Domyślny czas realizacji wynosi 5 minut. Zaznacz pole, jeśli chcesz uruchomić zadanie na wszystkich komputerach, w tym wyłączonych komputerach.
Wyłącz urządzenia po zakończeniu zadania *(dostępny tylko w Kaspersky Security Center Console)*	Możesz na przykład włączyć tę funkcję, aby skanować komputer w piątki po godzinach pracy. Po zakończeniu zadania aplikacja wyłącza komputer na weekend.
Wstrzymaj zadanie	Można określić przedział czasu, w którym wykonywanie wcześniej zaplanowanego zadania zostanie wstrzymane. Po upływie określonego czasu zadanie zostanie wznowione. Może się to okazać konieczne na przykład w celu zminimalizowania wpływu programu Kaspersky Endpoint Security na wydajność komputera w okresach szczytowego obciążenia.
Wyłącz terminarz od	Jeśli to pole wyboru jest zaznaczone, Kaspersky Endpoint Security zatrzyma wykonywanie zaplanowanego zadania od określonej daty. Zadanie zostanie ustawione w trybie **Ręcznie**.

Uruchamianie skanowania jako inny użytkownik

Domyślnie zadanie skanowania jest uruchamiane w imieniu użytkownika, z którego uprawnieniami jesteś zarejestrowany w systemie operacyjnym. Obszar ochrony może zawierać dyski sieciowe lub inne obiekty, które wymagają specjalnych uprawnień dostępu. Możesz wskazać użytkownika, który posiada odpowiednie uprawnienia, w ustawieniach aplikacji i uruchomić zadanie skanowania z poziomu konta tego użytkownika.

Jako inny użytkownik możesz uruchomić następujące skanowania:

- Skanowanie obszarów krytycznych.
- Pełne skanowanie.
- Skanowanie obiektów.
- Skanowanie z menu kontekstowego.

Nie możesz skonfigurować uprawnień użytkownika do uruchomienia Skanowania dysków wymiennych, Skanowania w tle lub Sprawdzania integralności.

Jak w Konsoli administracyjnej (MMC) uruchomić skanowanie jako inny użytkownik?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Zadania**.
4. Wybierz zadanie skanowania i kliknij je dwukrotnie, aby otworzyć właściwości zadania.
5. W oknie właściwości zadania wybierz sekcję **Konto**.

6. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania skanowania.

7. Zapisz swoje zmiany.

Jak w konsoli Web Console lub Cloud Console uruchomić skanowanie jako inny użytkownik?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie skanowania.

   Zostanie otwarte okno właściwości zadania.

3. Wybierz zakładkę **Ustawienia**.

4. W sekcji **Konto** kliknij przycisk **Ustawienia**.

5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania skanowania.

6. Zapisz swoje zmiany.

Jak w interfejsie aplikacji uruchomić skanowanie jako inny użytkownik?

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.

2. Na liście zadań wybierz zadanie skanowania i kliknij ⚙.

3. We właściwościach zadania wybierz **Ustawienia zaawansowane** → **Uruchom skanowanie jako**.

4. W otwartym oknie wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania skanowania.

5. Zapisz swoje zmiany.

Jeśli zadanie skanowania nie jest wyświetlane, oznacza to, że administrator zabronił użycia zadań lokalnych w zasadzie.

Optymalizacja skanowania

Ograniczanie użycia procesora podczas skanowania komputera

Możesz ograniczyć użycie procesora przez zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Może to wydłużyć czas skanowania komputera.

Jak ograniczyć użycie procesora podczas skanowania komputera w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.

4. W sekcji **Wydajność** zaznacz pole wyboru **Ogranicz użycie procesora do zadań skanowania** i wprowadź średnią wartość zużycia zasobów procesora w procentach.

5. Zapisz swoje zmiany.

Jak ograniczyć użycie procesora podczas skanowania komputera w konsoli Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne** → **Wydajność**.

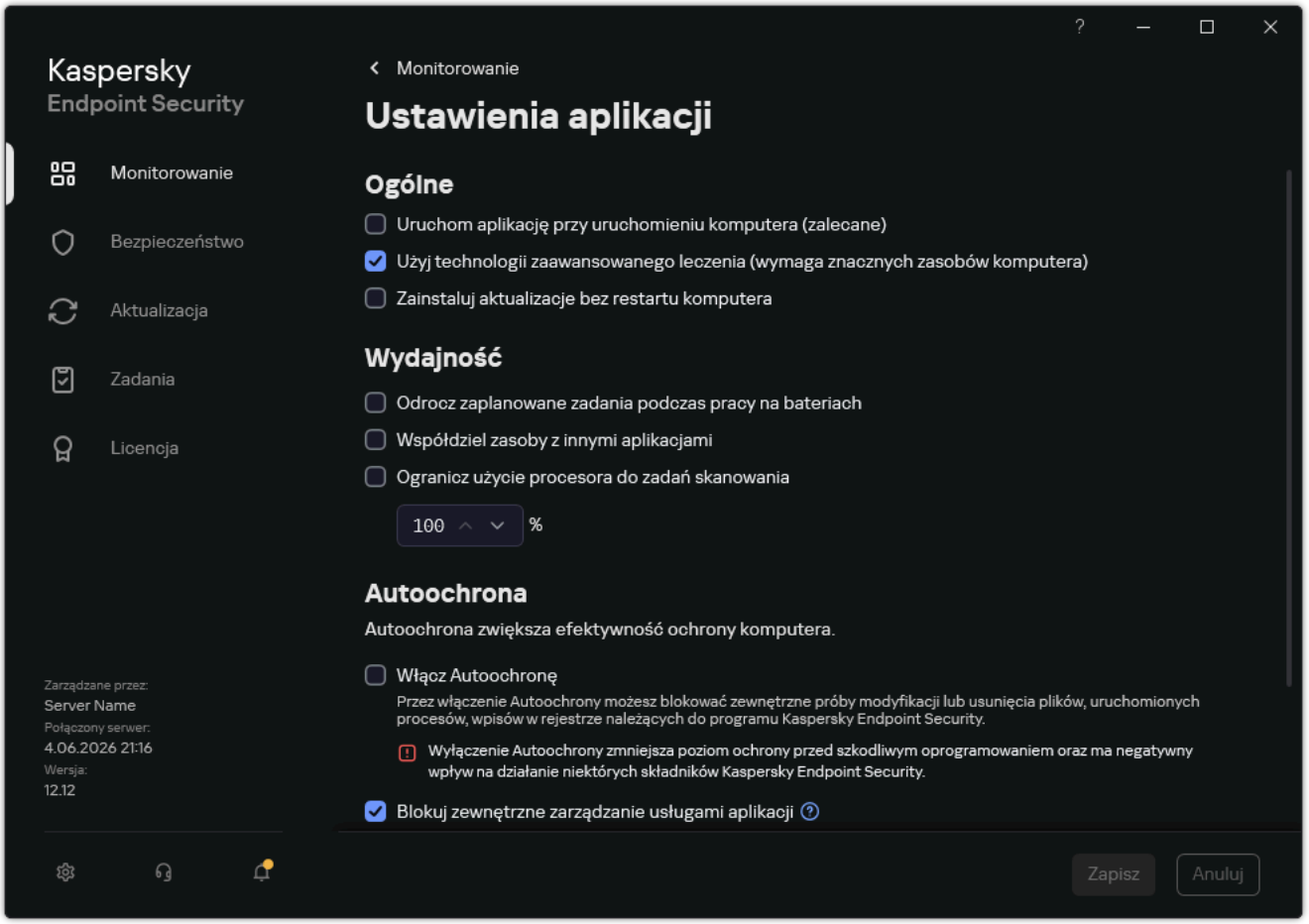
5. W sekcji **Ogranicz użycie procesora do zadań skanowania** ustaw przełącznik na **Ogranicz użycie procesora do zadań skanowania** i wprowadź średnią wartość zużycia zasobów procesora w procentach.

6. Zapisz swoje zmiany.

Jak ograniczyć użycie procesora podczas skanowania komputera w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.



Ustawienia Kaspersky Endpoint Security for Windows

3. W sekcji **Wydajność** zaznacz pole wyboru **Ogranicz użycie procesora do zadań skanowania** i wprowadź średnią wartość zużycia zasobów procesora w procentach.

4. Zapisz swoje zmiany.

Skonfiguruj zaawansowane ustawienia zadań dla Skanowanie w poszukiwaniu złośliwego oprogramowania.

Możesz zoptymalizować skanowanie plików, zmniejszając czas skanowania i zwiększając szybkość działania programu Kaspersky Endpoint Security. Można to uzyskać poprzez skanowanie tylko nowych plików i tych plików, które zostały zmodyfikowane od ostatniego skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych. Możesz również ustawić ograniczenie skanowania pojedynczego pliku. Po upłynięciu określonego czasu, obiekt zostanie wykluczony z bieżącego skanowania (poza archiwami i plikami zawierającymi wiele obiektów).

Popularną techniką ukrywania wirusów i innego szkodliwego oprogramowania jest osadzanie ich w plikach złożonych, takich jak archiwa czy bazy danych. W celu wykrycia ukrytych w ten sposób wirusów i innego szkodliwego oprogramowania, plik złożony musi zostać rozpakowany, co może spowolnić skanowanie. Możesz ograniczyć typy skanowanych plików złożonych, dzięki czemu skanowanie będzie szybsze.

Możesz także włączyć technologie: iChecker i iSwift. Technologie iChecker i iSwift optymalizują prędkość skanowania plików poprzez wykluczenie plików, które nie zostały zmodyfikowane od ostatniego skanowania.

Jak w Konsoli administracyjnej (MMC) zoptymalizować skanowanie?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W drzewie konsoli wybierz **Zadania**.

3. Wybierz zadanie skanowania i kliknij je dwukrotnie, aby otworzyć właściwości zadania.

   W razie konieczności utworzyć zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

4. W oknie właściwości zadania wybierz sekcję **Ustawienia**.

5. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

   To spowoduje otwarcie okna ustawień zadania skanowania.

6. W sekcji **Optymalizacja** skonfiguruj ustawienia skanowania:

   - **Skanuj tylko nowe i zmienione pliki**. Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.

     Możesz także skonfigurować skanowanie nowych plików według typu. Na przykład, możesz przeskanować wszystkie pakiety dystrybucyjne i przeskanować tylko nowe archiwa i pliki formatów office.

- **Pomiń pliki skanowane dłużej niż N sek**. Ograniczenie czasu wykonywania zadania. Po określonym czasie Kaspersky Endpoint Security zatrzyma zadanie. Zadanie nie zostanie oznaczone jako zakończone. Następnym razem, gdy Kaspersky Endpoint Security uruchomi zadanie, zostanie ono uruchomione od początku i zgodnie z terminarzem.

- **Nie uruchamiaj wielu zadań skanowania w tym samym czasie**. Opóźnione rozpoczęcie zadań skanowania, jeśli skanowanie jest już w toku. Kaspersky Endpoint Security będzie wysyłał nowe zadania skanowania, jeśli bieżące skanowanie będzie kontynuowane. Pomaga to zoptymalizować obciążenie komputera. Na przykład załóżmy, że aplikacja uruchomiła zadanie Pełnego skanowania zgodnie z harmonogramem. Jeżeli użytkownik spróbuje uruchomić skanowanie plików z menu kontekstowego, Kaspersky Endpoint Security zapisze to zadanie na listę zadań skanowania plików, a następnie automatycznie uruchomi je po zakończeniu zadania Pełnego skanowania.

7. Kliknij **Dodatkowe**.

   To spowoduje otwarcie okna ustawień skanowania plików złożonych.

8. W sekcji **Ograniczenie rozmiaru** zaznacz pole **Nie rozpakowuj dużych plików złożonych**. Ograniczenie czasu wykonywania zadania. Po określonym czasie Kaspersky Endpoint Security zatrzyma zadanie. Zadanie nie zostanie oznaczone jako zakończone. Następnym razem, gdy Kaspersky Endpoint Security uruchomi zadanie, zostanie ono uruchomione od początku i zgodnie z terminarzem.

   Kaspersky Endpoint Security skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

9. Kliknij **OK**.

10. Przejdź do zakładki **Dodatkowe**.

11. W sekcji **Technologie skanowania** zaznacz pola obok nazw technologii, których chcesz użyć podczas skanowania:

    - **Technologia iSwift**. Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.

    - **Technologia iChecker**. Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).

12. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console zoptymalizować skanowanie?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie skanowania.

   Zostanie otwarte okno właściwości zadania. W razie konieczności utworzyć zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. W sekcji **Działanie po wykryciu zagrożenia** zaznacz pole **Skanuj tylko nowe i zmienione pliki**. Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.

   Możesz także skonfigurować skanowanie nowych plików według typu. Na przykład, możesz przeskanować wszystkie pakiety dystrybucyjne i przeskanować tylko nowe archiwa i pliki formatów office.

5. W sekcji **Optymalizacja skanowania** zaznacz pole **Nie rozpakowuj dużych plików złożonych**. Ograniczenie czasu wykonywania zadania. Po określonym czasie Kaspersky Endpoint Security zatrzyma zadanie. Zadanie nie zostanie oznaczone jako zakończone. Następnym razem, gdy Kaspersky Endpoint Security uruchomi zadanie, zostanie ono uruchomione od początku i zgodnie z terminarzem.

   Kaspersky Endpoint Security skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

6. Zaznacz pole **Nie uruchamiaj wielu zadań skanowania w tym samym czasie**. Opóźnione rozpoczęcie zadań skanowania, jeśli skanowanie jest już w toku. Kaspersky Endpoint Security będzie wysyłał nowe zadania skanowania, jeśli bieżące skanowanie będzie kontynuowane. Pomaga to zoptymalizować obciążenie komputera. Na przykład załóżmy, że aplikacja uruchomiła zadanie Pełnego skanowania zgodnie z harmonogramem. Jeżeli użytkownik spróbuje uruchomić skanowanie plików z menu kontekstowego, Kaspersky Endpoint Security zapisze to zadanie na listę zadań skanowania plików, a następnie automatycznie uruchomi je po zakończeniu zadania Pełnego skanowania.

7. W sekcji **Ustawienia zaawansowane** zaznacz pole **Pomiń plik skanowany dłużej niż (sek.)**. Ograniczenie czasu wykonywania zadania. Po określonym czasie Kaspersky Endpoint Security zatrzyma zadanie. Zadanie nie zostanie oznaczone jako zakończone. Następnym razem, gdy Kaspersky Endpoint Security uruchomi zadanie, zostanie ono uruchomione od początku i zgodnie z terminarzem.

8. Zapisz swoje zmiany.

Jak w interfejsie aplikacji zoptymalizować skanowanie?

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.

2. Na liście zadań wybierz zadanie skanowania i kliknij ⚙.

3. Kliknij **Ustawienia zaawansowane**.

4. W sekcji **Optymalizacja** skonfiguruj ustawienia skanowania:

   - **Skanuj tylko nowe i zmienione pliki**. Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.

     Możesz także skonfigurować skanowanie nowych plików według typu. Na przykład, możesz przeskanować wszystkie pakiety dystrybucyjne i przeskanować tylko nowe archiwa i pliki formatów office.

- **Pomiń plik skanowany dłużej niż N s**. Ograniczenie czasu wykonywania zadania. Po określonym czasie Kaspersky Endpoint Security zatrzyma zadanie. Zadanie nie zostanie oznaczone jako zakończone. Następnym razem, gdy Kaspersky Endpoint Security uruchomi zadanie, zostanie ono uruchomione od początku i zgodnie z terminarzem.

- **Nie uruchamiaj wielu zadań skanowania w tym samym czasie**. Opóźnione rozpoczęcie zadań skanowania, jeśli skanowanie jest już w toku. Kaspersky Endpoint Security będzie wysyłał nowe zadania skanowania, jeśli bieżące skanowanie będzie kontynuowane. Pomaga to zoptymalizować obciążenie komputera. Na przykład załóżmy, że aplikacja uruchomiła zadanie Pełnego skanowania zgodnie z harmonogramem. Jeżeli użytkownik spróbuje uruchomić skanowanie plików z menu kontekstowego, Kaspersky Endpoint Security zapisze to zadanie na listę zadań skanowania plików, a następnie automatycznie uruchomi je po zakończeniu zadania Pełnego skanowania.

5. W sekcji **Ograniczenie rozmiaru** zaznacz pole **Nie rozpakowuj dużych plików złożonych**. Ograniczenie czasu wykonywania zadania. Po określonym czasie Kaspersky Endpoint Security zatrzyma zadanie. Zadanie nie zostanie oznaczone jako zakończone. Następnym razem, gdy Kaspersky Endpoint Security uruchomi zadanie, zostanie ono uruchomione od początku i zgodnie z terminarzem.

   Kaspersky Endpoint Security skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

6. W sekcji **Technologie skanowania** zaznacz pola obok nazw technologii, których chcesz użyć podczas skanowania:

   - **Technologia iSwift**. Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.

   - **Technologia iChecker**. Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).

7. Zapisz swoje zmiany.

Jeśli zadanie skanowania nie jest wyświetlane, oznacza to, że administrator zabronił użycia zadań lokalnych w zasadzie.

Aktualizowanie baz danych i modułów aplikacji

Aktualizowanie baz danych i modułów aplikacji Kaspersky Endpoint Security zapewnia aktualną ochronę Twojego komputera. Codziennie na całym świecie pojawia się duża ilość nowych wirusów i innego typu szkodliwego oprogramowania. Bazy danych Kaspersky Endpoint Security zawierają informacje o zagrożeniach i sposoby ich neutralizowania. Aby szybko wykrywać zagrożenia, zalecamy regularnie aktualizować bazy danych i moduły aplikacji.

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), które mogą nie być dostępne w oprogramowaniu na terytorium Stanów Zjednoczonych.

Regularne aktualizacje wymagają ważnej licencji na aplikację. Jeżeli nie ma bieżącej licencji, wówczas możliwe będzie wykonanie tylko jednej aktualizacji.

Aby możliwe było pobieranie pakietów aktualizacji z serwerów aktualizacji Kaspersky, komputer musi być podłączony do internetu. Domyślnie ustawienia połączenia internetowego są określane automatycznie. Jeśli korzystasz z serwera proxy, konieczne może być dostosowanie ustawień serwera proxy.

Uaktualnienia są pobierane po protokole HTTPS. Mogą także zostać pobrane po protokole HTTP, jeśli niemożliwe jest pobranie uaktualnień po protokole HTTPS.

Podczas procesu aktualizacji, na komputer są pobierane i instalowane następujące obiekty:

- Bazy danych programu Kaspersky Endpoint Security. Ochrona komputera jest zapewniana przy pomocy baz danych zawierających sygnatury wirusów i innych zagrożeń oraz informacje o sposobach ich neutralizacji. Moduły ochrony korzystają z tych informacji przy wyszukiwaniu i neutralizowaniu zainfekowanych plików na Twoim komputerze. Bazy danych są ciągle aktualizowane o wpisy nowych zagrożeń i metody ich zwalczania. Dlatego zalecamy regularne aktualizowanie baz danych.

  Oprócz baz danych Kaspersky Endpoint Security aktualizowane są również sterowniki sieciowe, które umożliwiają modułom aplikacji przechwytywanie ruchu sieciowego.

- Moduły aplikacji. Oprócz baz danych Kaspersky Endpoint Security można także aktualizować jej moduły. Aktualizowanie modułów aplikacji likwiduje luki w Kaspersky Endpoint Security, dodaje nowe funkcje lub poprawia te istniejące.

Podczas aktualizacji moduły i bazy danych aplikacji znajdujące się na komputerze porównywane są z tymi aktualnymi, znajdującymi się w źródle uaktualnień. Jeśli Twoje bieżące bazy danych i moduły różnią się od najnowszych wersji, na Twoim komputerze zainstalowana zostanie brakująca część uaktualnień.

Jeśli bazy danych są bardzo stare, pakiet uaktualnień może być duży, co spowoduje zwiększony ruch internetowy (kilkadziesiąt MB).

Informacje o bieżącym stanie baz danych Kaspersky Endpoint Security jest wyświetlany w oknie głównym aplikacji lub w dymku, który jest wyświetlany po najechaniu kursorem na ikonę aplikacji w obszarze powiadomień.

Informacje o wynikach aktualizacji i wszystkich zdarzeniach zaistniałych podczas wykonywania zadania aktualizacji zapisywane są w raporcie Kaspersky Endpoint Security.

Jeśli aplikacja działa w trybie Light Agent, podczas aktualizowania baz danych i modułów aplikacji należy zwrócić uwagę na pewne szczególne kwestie.

Scenariusze aktualizacji baz danych i modułów aplikacji

Aktualizowanie baz danych i modułów aplikacji Kaspersky Endpoint Security zapewnia aktualną ochronę Twojego komputera. Codziennie na całym świecie pojawia się duża ilość nowych wirusów i innego typu szkodliwego oprogramowania. Bazy danych Kaspersky Endpoint Security zawierają informacje o zagrożeniach i sposoby ich neutralizowania. Aby szybko wykrywać zagrożenia, zalecamy regularnie aktualizować bazy danych i moduły aplikacji.

Na komputerach użytkowników aktualizowane są następujące obiekty:

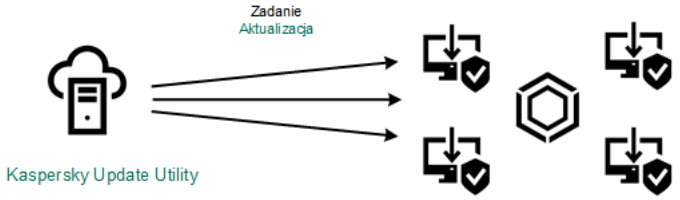
- Antywirusowe bazy danych. Antywirusowe bazy danych zawierają bazy danych sygnatur szkodliwych programów, opisy ataków sieciowych, bazy danych szkodliwych i phishingowych adresów internetowych, bazy danych banerów, bazy danych spamu oraz inne dane.

- Moduły aplikacji. Aktualizacje modułów są przeznaczone do eliminowania lun w aplikacji i do udoskonalania metod ochrony komputera. Aktualizacje modułów mogą zmieniać zachowanie komponentów aplikacji i dodawać nowe możliwości.

Kaspersky Endpoint Security obsługuje następujące scenariusze aktualizowania baz danych i modułów:

- Aktualizacja z serwerów Kaspersky.

  Serwery aktualizacji Kaspersky znajdują się w różnych krajach na całym świecie. To zapewnia wysoką niezawodność aktualizacji. Jeśli aktualizacja nie może zostać wykonana z jednego serwera, Kaspersky Endpoint Security przełączy się do kolejnego serwera.



Aktualizacja z serwerów Kaspersky

- Scentralizowana aktualizacja.

  Scentralizowana aktualizacja zmniejsza zewnętrzny ruch internetowy i zapewnia wygodne monitorowanie aktualizacji.

  Scentralizowana aktualizacja składa się na następujące kroki:

  1. Pobierz pakiet aktualizacji do repozytorium w obrębie sieci organizacji.

     Pakiet aktualizacji jest pobierany do repozytorium przez zadanie Serwera administracyjnego o nazwie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

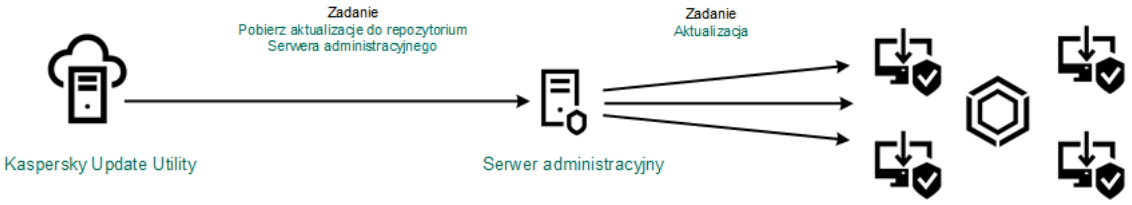
  2. Pobierz pakiet aktualizacji do folderu współdzielonego (opcjonalnie).

Pakiet aktualizacji można pobrać do folderu współdzielonego, korzystając z następujących metod:

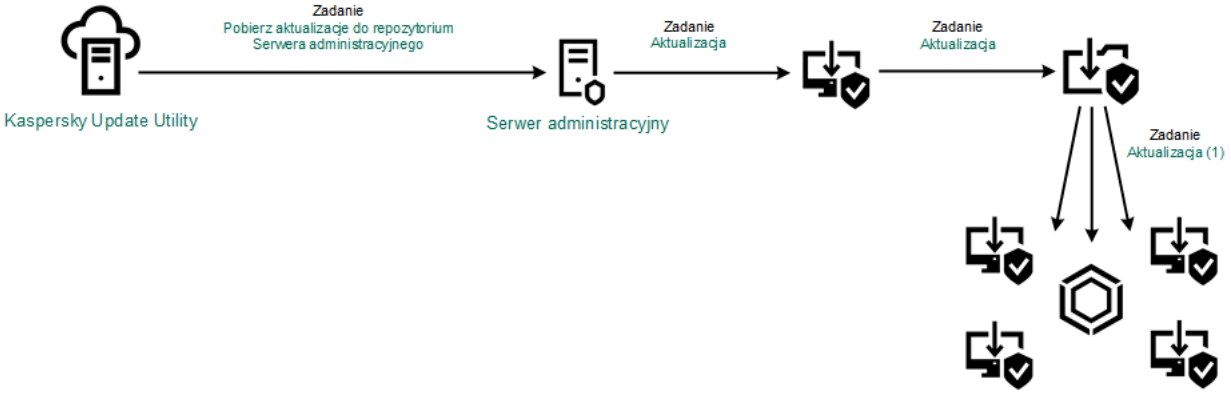
- Korzystając z zadania *Aktualizacja baz danych i modułów aplikacji* programu Kaspersky Endpoint Security. Zadanie jest przeznaczone dla jednego z komputerów w lokalnej sieci komputerowej.
- Przy użyciu narzędzia Kaspersky Update Utility. Szczegółowe informacje na temat korzystania z narzędzia Kaspersky Update Utility znajdziesz w Bazie wiedzy Kaspersky.

3. Roześlij pakiet aktualizacji na komputery klienckie.

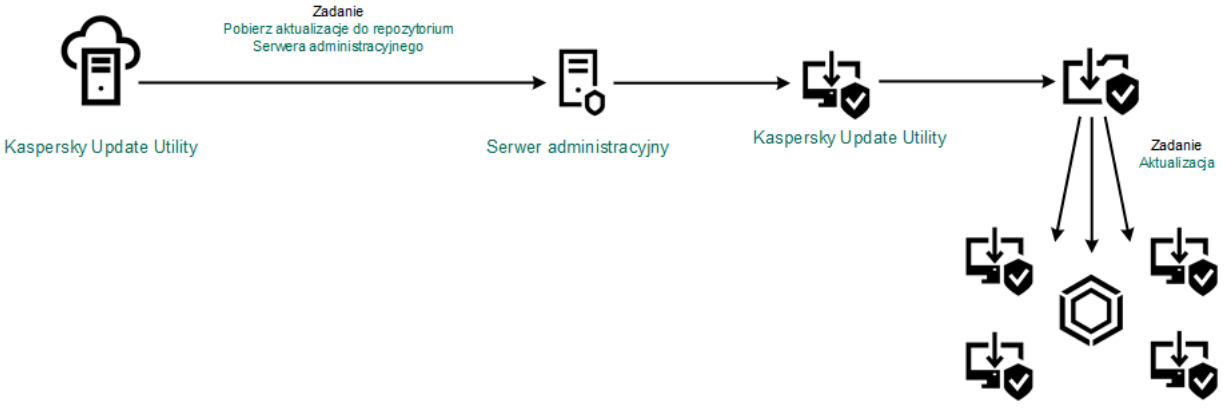
   Pakiet aktualizacji jest rozsyłany na komputery klienckie przez zadanie *Aktualizacja baz danych i modułów aplikacji* programu Kaspersky Endpoint Security. Dla każdej grupy administracyjnej możesz utworzyć nieograniczoną liczbę zadań aktualizacji.



Aktualizowanie z repozytorium serwera



Aktualizowanie z folderu współdzielonego



Aktualizowanie przy użyciu narzędzia Kaspersky Update Utility

Dla Kaspersky Security Center domyślna lista źródeł uaktualnień zawiera Serwer administracyjny Kaspersky Security Center i serwery aktualizacji Kaspersky. W przypadku konsoli Kaspersky Security Center Cloud Console domyślna lista źródeł uaktualnień zawiera punkty dystrybucji i serwery aktualizacji Kaspersky. Więcej informacji o punktach dystrybucji znajdziesz w pomocy do Kaspersky Security Center Cloud Console. Do listy można dodać inne źródło uaktualnień. Źródłem uaktualnień mogą być serwery HTTP/FTP oraz foldery współdzielone. Jeśli aktualizacja nie może zostać wykonana z jednego źródła uaktualnień, Kaspersky Endpoint Security przełączy się do kolejnego serwera.

Uaktualnienia są pobierane z serwerów aktualizacji Kaspersky lub z innych serwerów FTP lub HTTP za pośrednictwem standardowych protokołów sieciowych. Jeśli do uzyskania dostępu do serwerów aktualizacji wymagane jest połączenie z serwerem proxy, w ustawieniach profilu Kaspersky Endpoint Security określ ustawienia serwera proxy.

Aktualizowanie z repozytorium serwera

Aby oszczędzić ruch sieciowy, możesz skonfigurować aktualizacje baz danych i modułów aplikacji na komputerach sieci LAN organizacji z repozytorium serwera. W tym celu Kaspersky Security Center musi pobrać pakiet aktualizacyjny do repozytorium (serwer FTP lub HTTP, folder sieciowy lub lokalny) z serwerów aktualizacji Kaspersky. Pozostałe komputery w sieci LAN organizacji będą mogły pobierać pakiety aktualizacyjne z repozytorium serwera.

Konfigurowanie aktualizacji baz danych i modułów aplikacji z repozytorium serwera obejmuje następujące kroki:

1. Konfigurację pobrania pakietu aktualizacji do repozytorium Serwera administracyjnego (zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*).

   Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego i to zadanie może mieć tylko jedną instancję. Domyślnie Kaspersky Security Center kopiuje pakiet aktualizacji do folderu `\\<server name>\KLSHARE\Updates`. Więcej informacji na temat pobierania aktualizacji do repozytorium Serwera administracyjnego można znaleźć w pomocy do Kaspersky Security Center.

2. Konfigurację aktualizacji baz danych i modułów aplikacji z określonego repozytorium serwera do pozostałych komputerów w sieci LAN organizacji (zadanie *Aktualizacja baz danych i modułów aplikacji*).

   Konfigurowanie aktualizacji Kaspersky Endpoint Security z określonego magazynu serwera w Konsoli administracyjnej (MMC)

   1. Otwórz Konsolę administracyjną Kaspersky Security Center.

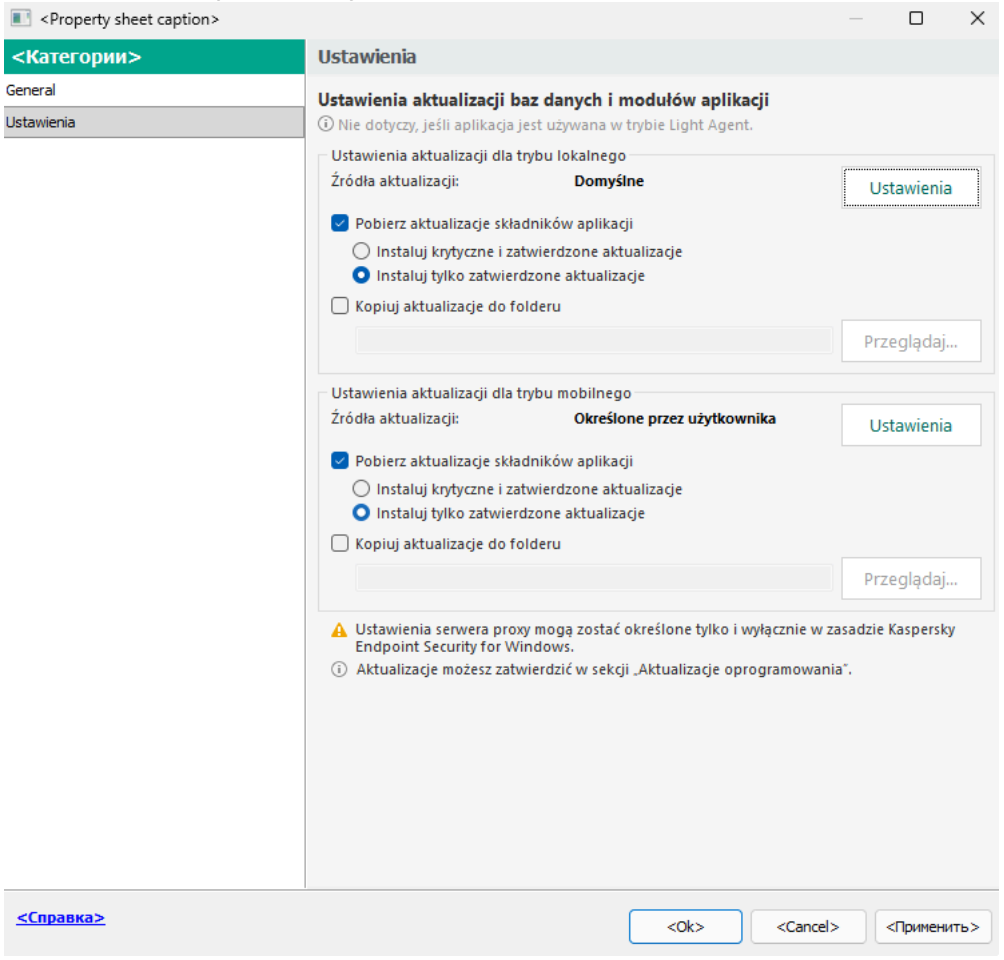
      W drzewie konsoli wybierz **Zadania**.

   2. Kliknij zadanie **Aktualizacja baz danych i modułów aplikacji** Kaspersky Endpoint Security.

      Zostanie otwarte okno właściwości zadania.

      Zadanie *Aktualizacja baz danych i modułów aplikacji* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja baz danych i modułów aplikacji*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

3. W oknie właściwości zadania wybierz sekcję **Ustawienia**.



Ustawienia zadania Aktualizacja baz danych i modułów aplikacji

4. W sekcji **Ustawienia aktualizacji dla trybu lokalnego** kliknij przycisk **Ustawienia**.

5. Na liście źródeł aktualizacji upewnij się, że aktualizacja ze źródła **Kaspersky Security Center** jest włączona. Dodatkowo, źródło **Kaspersky Security Center** musi mieć najwyższy priorytet.

6. W razie potrzeby dodaj źródła aktualizacji:

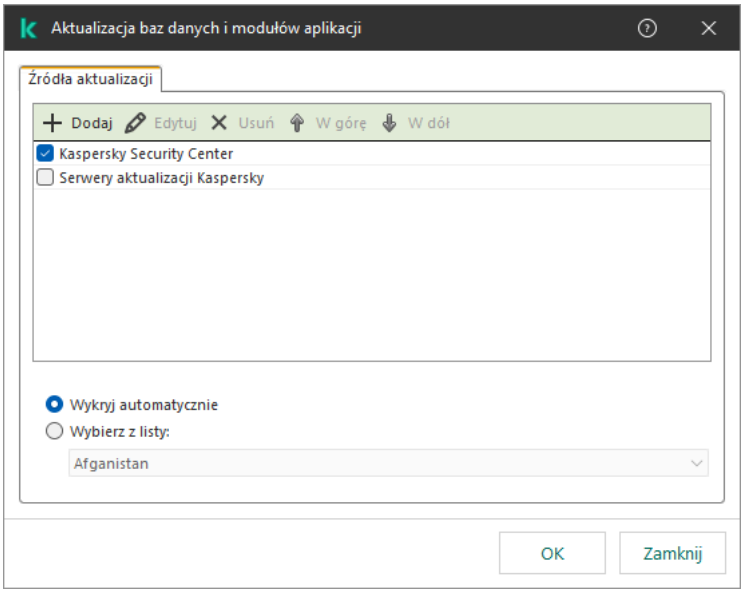
   a. Na liście źródeł uaktualnień kliknij przycisk **Dodaj**.

   b. W polu **Źródła aktualizacji** określ adres serwera FTP lub HTTP, folderu sieciowego lub lokalnego, do którego Kaspersky Security Center skopiuje pakiet aktualizacji, pobrany z serwerów Kaspersky.

      Adres źródła aktualizacji musi być zgodny z adresem podanym w polu **Folder do przechowywania aktualizacji** podczas konfigurowania pobierania aktualizacji do pamięci serwera (zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*).

   c. Kliknij **OK**.

Możesz wykluczyć źródło aktualizacji bez usuwania go z listy źródeł aktualizacji. W tym celu odznacz pole obok obiektu.



Źródła aktualizacji

7. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

   Jeśli aktualizacja nie może zostać wykonana z pierwszego źródła uaktualnień, Kaspersky Endpoint Security automatycznie przełączy się do kolejnego źródła.

8. W oknie właściwości zadania wybierz sekcję **Terminarz** i skonfiguruj tryb uruchamiania zadania.

9. Domyślnie Kaspersky Endpoint Security uruchamia zadanie w trybie ręcznym.

10. Zapisz swoje zmiany.

Konfigurowanie aktualizacji Kaspersky Endpoint Security z określonego magazynu serwera w Web Console

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie **Aktualizacja** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

   Zadanie *Aktualizacja* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

3. Wybierz zakładkę **Ustawienia aplikacji** → **Tryb lokalny**.

4. Na liście źródeł aktualizacji upewnij się, że aktualizacja ze źródła **Kaspersky Security Center** jest włączona. Dodatkowo, źródło **Kaspersky Security Center** musi mieć najwyższy priorytet.

5. W razie potrzeby dodaj źródła aktualizacji:

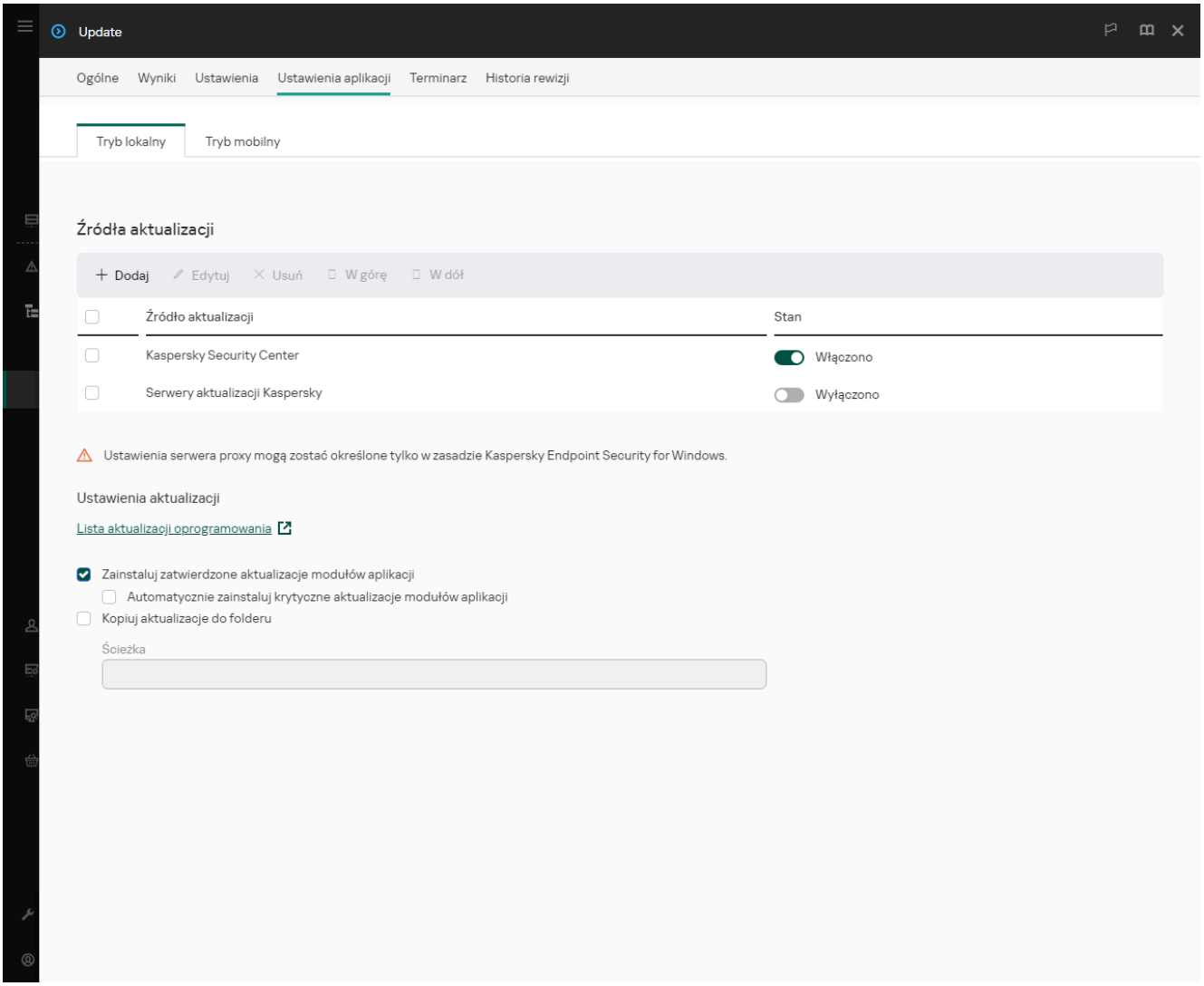
   a. Na liście źródeł uaktualnień kliknij przycisk **Dodaj**.

   b. W polu **Źródła aktualizacji** określ adres serwera FTP lub HTTP, folderu sieciowego lub lokalnego, do którego Kaspersky Security Center skopiuje pakiet aktualizacji, pobrany z serwerów Kaspersky.

   > Adres źródła aktualizacji musi być zgodny z adresem podanym w polu **Folder do przechowywania aktualizacji** podczas konfigurowania pobierania aktualizacji do pamięci serwera (zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*).

   c. Kliknij **Zapisz**.

Możesz wykluczyć źródło aktualizacji bez usuwania go z listy źródeł aktualizacji. W tym celu ustaw przycisk przełącznika obok obiektu na pozycję wyłączenia.



Źródła aktualizacji

6. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

   Jeśli aktualizacja nie może zostać wykonana z pierwszego źródła uaktualnień, Kaspersky Endpoint Security automatycznie przełączy się do kolejnego źródła.

7. W oknie właściwości zadania wybierz sekcję **Terminarz** i skonfiguruj tryb uruchamiania zadania.

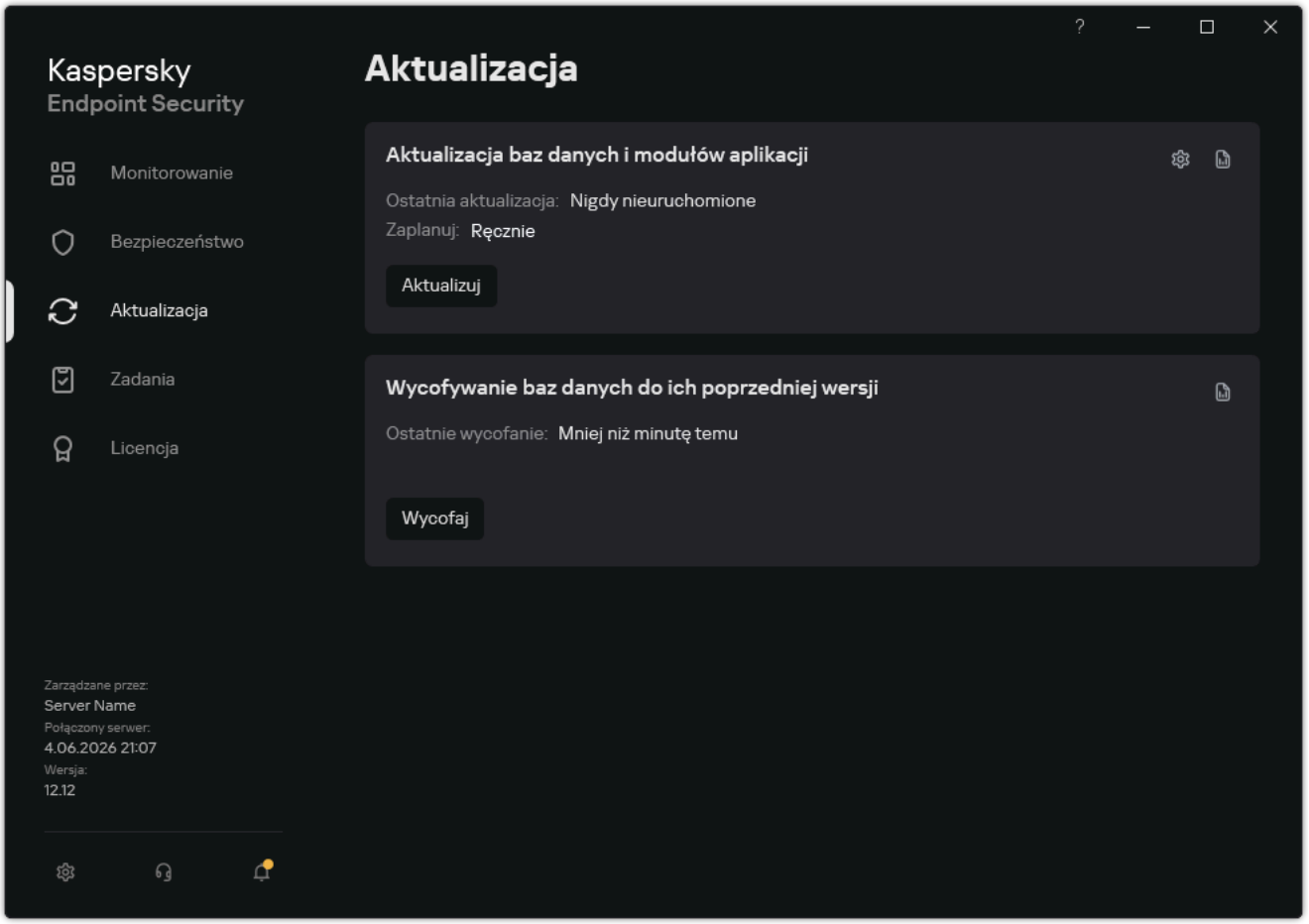
8. Domyślnie Kaspersky Endpoint Security uruchamia zadanie w trybie ręcznym.

9. Zapisz swoje zmiany.

Konfigurowanie aktualizacji Kaspersky Endpoint Security z określonego magazynu serwera w interfejsie aplikacji

Nie możesz skonfigurować zadania grupowego *Aktualizacja baz danych i modułów aplikacji* w interfejsie aplikacji. Tylko lokalne zadanie aktualizacji, *Aktualizacja baz danych i modułów aplikacji*, jest dostępne dla użytkownika. Jeśli zadanie *Aktualizacja baz danych i modułów aplikacji* nie jest wyświetlane, oznacza to, że administrator zabronił używania zadań lokalnych w zasadzie.

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.



Lokalne zadania aktualizacji

2. To spowoduje otwarcie listy zadań; wybierz zadanie *Aktualizacja baz danych i modułów aplikacji* i kliknij ⚙.

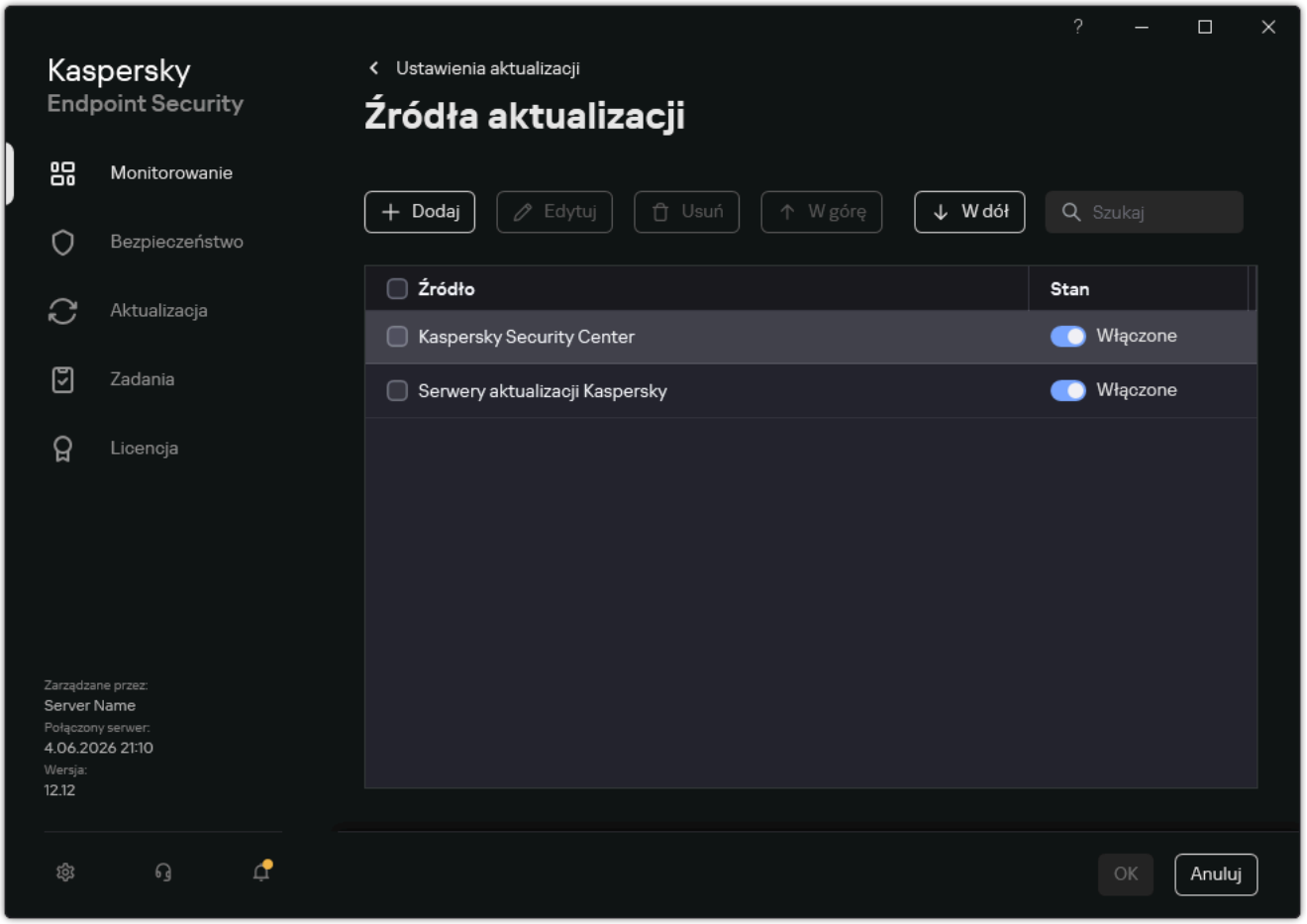
   Zostanie otwarte okno właściwości zadania.

3. W oknie właściwości zadania kliknij **Wybierz źródła aktualizacji**.

4. Na liście źródeł aktualizacji upewnij się, że aktualizacja ze źródła **Kaspersky Security Center** jest włączona. Dodatkowo, źródło **Kaspersky Security Center** musi mieć najwyższy priorytet.

5. W razie potrzeby dodaj źródła aktualizacji:

   a. Na liście źródeł uaktualnień kliknij przycisk **Dodaj**.



Źródła aktualizacji

   a. Określ adres serwera FTP lub HTTP, folderu sieciowego albo folderu lokalnego, do którego Kaspersky Security Center skopiuje pakiet aktualizacji odebrany z serwerów aktualizacji Kaspersky.

      Adres źródła aktualizacji musi być zgodny z adresem podanym w polu **Folder do przechowywania aktualizacji** podczas konfigurowania pobierania aktualizacji do pamięci serwera (zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*).

   b. Kliknij **Wybierz**.

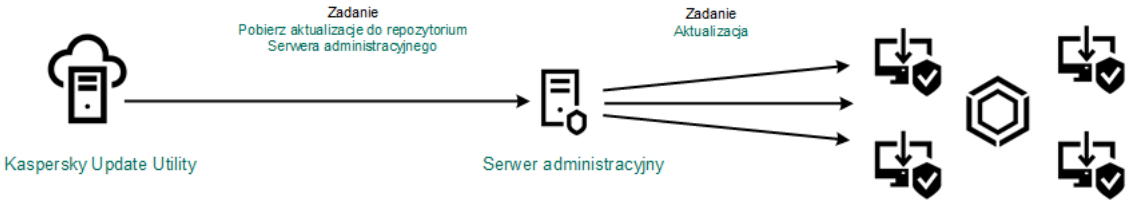
   Możesz wykluczyć źródło aktualizacji bez usuwania go z listy źródeł aktualizacji. W tym celu ustaw przycisk przełącznika obok obiektu na pozycję wyłączenia.

6. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

   Jeśli aktualizacja nie może zostać wykonana z pierwszego źródła uaktualnień, Kaspersky Endpoint Security automatycznie przełączy się do kolejnego źródła.

   Jeśli komputer jest zarządzany przez Kaspersky Security Center, nie jest możliwe skonfigurowanie trybu uruchamiania dla zadania *Aktualizacja baz danych i modułów aplikacji*. Zadanie można uruchomić tylko ręcznie.

7. Zapisz swoje zmiany.



Aktualizowanie z repozytorium serwera

Aktualizowanie z folderu współdzielonego

Aby oszczędzić ruch sieciowy, możesz skonfigurować aktualizacje baz danych i modułów aplikacji na komputerach sieci LAN organizacji z folderu współdzielonego. W tym celu jeden z komputerów w sieci LAN organizacji musi odbierać pakiety aktualizacji z Serwera administracyjnego Kaspersky Security Center lub z serwerów aktualizacji Kaspersky i kopiuje go do folderu współdzielonego. Pozostałe komputery w sieci LAN organizacji będą mogły pobrać pakiety aktualizacji z tego folderu współdzielonego.

Wersja i lokalizacja aplikacji Kaspersky Endpoint Security, która kopiuje pakiet aktualizacyjny do folderu współdzielonego, musi odpowiadać wersji i lokalizacji aplikacji, która aktualizuje bazy danych z folderu współdzielonego. Jeśli wersje lub lokalizacje aplikacji nie odpowiadają, aktualizacja baz danych może zakończyć się błędem.

Konfigurowanie aktualizacji baz danych i modułów aplikacji z folderu współdzielonego obejmuje następujące kroki:

1. Konfigurowanie aktualizacji caz danych i modułów aplikacji z repozytorium serwera.
2. Włączenia kopiowania pakietu uaktualnień do foldera współdzielonego na jednym z komputerów w sieci lokalnej.

   Jak włączyć kopiowanie pakietu aktualizacji do folderu współdzielonego w Konsoli administracyjnej (MMC)

   1. Otwórz Konsolę administracyjną Kaspersky Security Center.
   2. W drzewie konsoli wybierz **Zadania**.

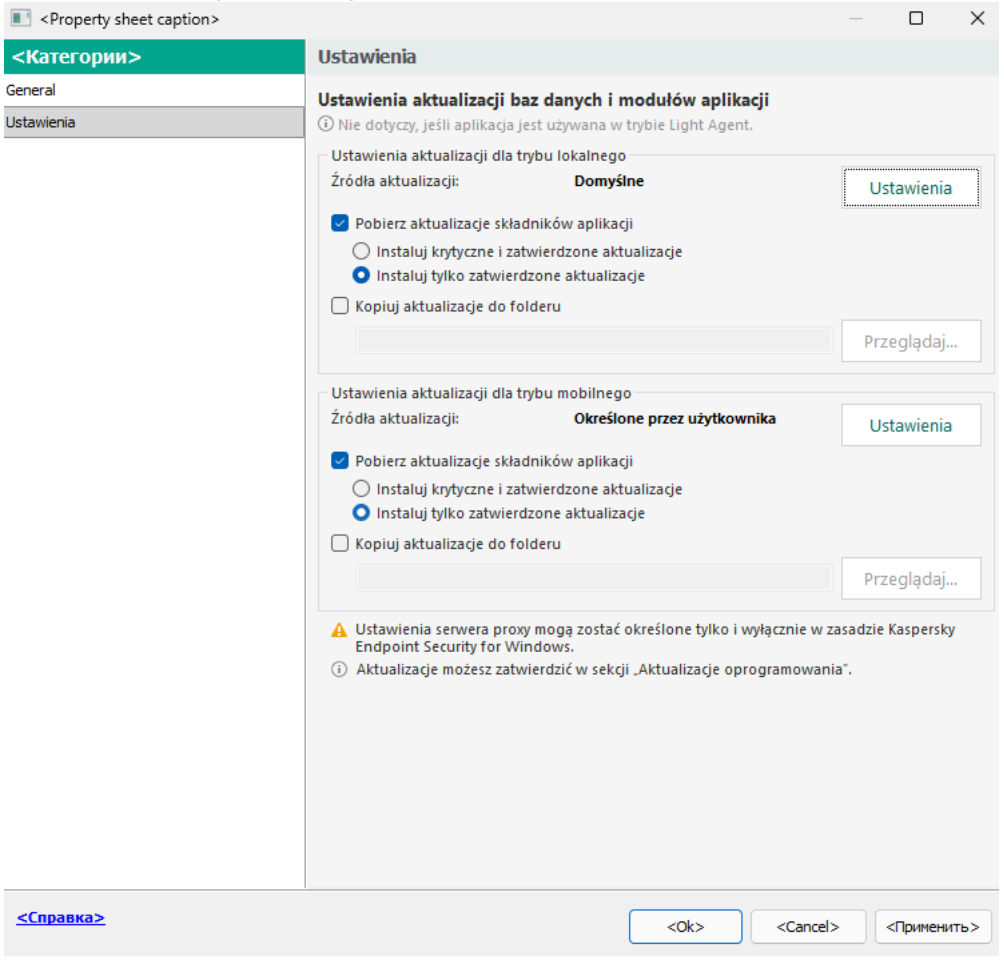
      Zadanie *Aktualizacja baz danych i modułów aplikacji* musi zostać przypisane do jednego komputera, który będzie pełnił rolę źródła uaktualnień.

   3. Kliknij zadanie **Aktualizacja baz danych i modułów aplikacji** Kaspersky Endpoint Security.

      Zostanie otwarte okno właściwości zadania.

      Zadanie *Aktualizacja baz danych i modułów aplikacji* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja baz danych i modułów aplikacji*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

4. W oknie właściwości zadania wybierz sekcję **Ustawienia**.



Ustawienia zadania Aktualizacja baz danych i modułów aplikacji

5. W sekcji **Ustawienia aktualizacji dla trybu lokalnego** kliknij przycisk **Ustawienia**.

6. Skonfiguruj źródła uaktualnień.

   Źródłami uaktualnień mogą być serwery aktualizacji Kaspersky, Serwer administracyjny Kaspersky Security Center, inne serwery FTP lub HTTP, foldery lokalne lub foldery sieciowe.

7. Zaznacz pole **Kopiuj aktualizacje do folderu**.

8. W polu **Ścieżka do folderu** wprowadź ścieżkę UNC do folderu współdzielonego (na przykład: `\\<server name>\KLSHARE\Updates`).

   Jeśli pole pozostanie puste, Kaspersky Endpoint Security skopiuje pakiet aktualizacji do folderu `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

9. Zapisz swoje zmiany.

Jak włączyć kopiowanie pakietu aktualizacji do folderu współdzielonego w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

   Zadanie *Aktualizacja* musi zostać przypisane do jednego komputera, który będzie pełnił rolę źródła uaktualnień.

2. Kliknij zadanie **Aktualizacja** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

   Zadanie *Aktualizacja* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

3. Wybierz zakładkę **Ustawienia aplikacji** → **Tryb lokalny**.

4. Skonfiguruj źródła uaktualnień.

   Źródłami uaktualnień mogą być serwery aktualizacji Kaspersky, Serwer administracyjny Kaspersky Security Center, inne serwery FTP lub HTTP, foldery lokalne lub foldery sieciowe.

5. Zaznacz pole **Kopiuj aktualizacje do folderu**.

6. W polu **Ścieżka** wprowadź ścieżkę UNC do folderu współdzielonego (na przykład: `\\<server name>\KLSHARE\Updates`).

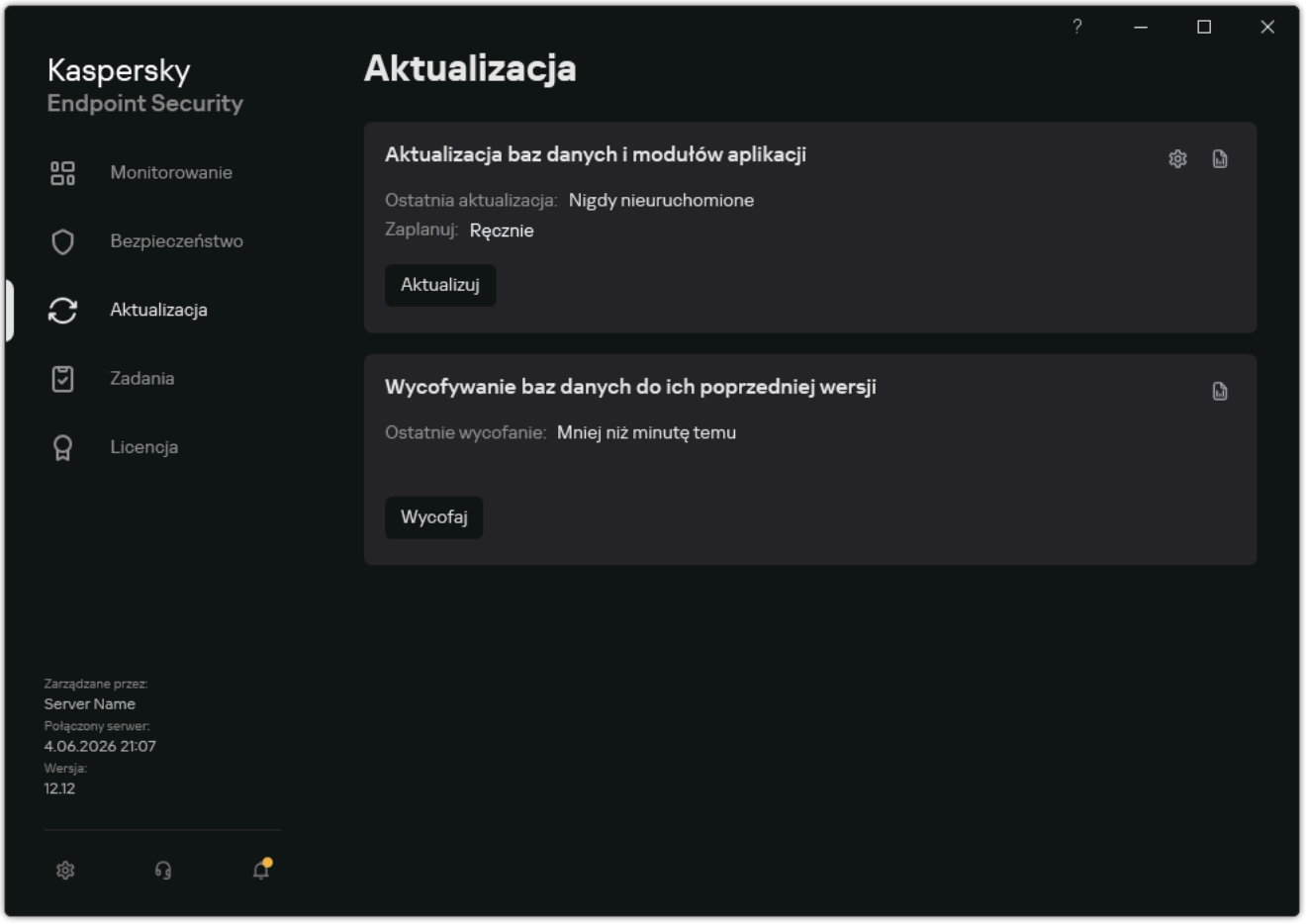
   Jeśli pole pozostanie puste, Kaspersky Endpoint Security skopiuje pakiet aktualizacji do folderu `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. Zapisz swoje zmiany.

Jak włączyć kopiowanie pakietu aktualizacji do folderu współdzielonego w interfejsie aplikacji

Nie możesz skonfigurować zadania grupowego *Aktualizacja baz danych i modułów aplikacji* w interfejsie aplikacji. Tylko lokalne zadanie aktualizacji, *Aktualizacja baz danych i modułów aplikacji*, jest dostępne dla użytkownika. Jeśli zadanie *Aktualizacja baz danych i modułów aplikacji* nie jest wyświetlane, oznacza to, że administrator zabronił używania zadań lokalnych w zasadzie.

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.



Lokalne zadania aktualizacji

2. To spowoduje otwarcie listy zadań; wybierz zadanie *Aktualizacja baz danych i modułów aplikacji* i kliknij ⚙.

   Zostanie otwarte okno właściwości zadania.

3. W sekcji **Dystrybucja uaktualnień** zaznacz pole **Kopiuj aktualizacje do folderu**.

4. Wprowadź ścieżkę UNC do folderu współdzielonego (na przykład: `\\<server name>\KLSHARE\Updates`).

5. Zapisz swoje zmiany.

3. Konfigurację aktualizacji baz danych i modułów aplikacji z określonego folderu współdzielonego do pozostałych komputerów w sieci LAN organizacji.

   Jak w Konsoli administracyjnej (MMC) skonfigurować aktualizacje z folderu współdzielonego

   1. W oknie głównym Web Console wybierz **Zadania**.

      Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Aktualizacja baz danych i modułów aplikacji**.

4. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

5. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Aktualizacja baz danych i modułów aplikacji**.

Krok 2. Wybór źródeł aktualizacji

Dodaj nowe źródło aktualizacji: folder udostępniony. Adres źródłowy musi odpowiadać adresowi, który wcześniej określono w polu **Ścieżka do folderu** podczas konfiguracji kopiowania pakietu aktualizacyjnego do folderu współdzielonego. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

Krok 3. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Zadanie *Aktualizacja baz danych i modułów aplikacji* musi zostać przypisane do komputerów sieci LAN organizacji, za wyjątkiem komputera, który pełni rolę źródła uaktualnień.

Krok 4. Wybieranie konta do uruchomienia zadania

Wybierz konto, aby uruchomić zadanie *Aktualizacja baz danych i modułów aplikacji*. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika.

Krok 5. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz uruchamiania zadania, na przykład, ręcznie lub po pobraniu antywirusowych baz danych do repozytorium.

Krok 6. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład: *Aktualizowanie z folderu współdzielonego*.

Krok 7. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania. W rezultacie zadanie aktualizacji zostanie wykonane na komputerach użytkowników zgodnie z określonym terminarzem.

Jak w konsoli Web Console i Cloud Console skonfigurować aktualizacje z folderu współdzielonego

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Aktualizacja**.

   c. W polu **Nazwa zadania** wpisz krótki opis, na przykład, *Aktualizowanie z folderu współdzielonego*.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

   > Zadanie *Aktualizacja* musi zostać przypisane do komputerów sieci LAN organizacji, za wyjątkiem komputera, który pełni rolę źródła uaktualnień.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania i przejdź do kolejnego kroku.

5. Zakończ działanie Kreatora.

   Nowe zadanie zostanie wyświetlone w tabeli zadań.

6. Kliknij nowo utworzone zadanie *Aktualizacja*.

   Zostanie otwarte okno właściwości zadania.

7. Wybierz zakładkę **Ustawienia aplikacji** → **Tryb lokalny**.

8. W sekcji **Źródła aktualizacji** kliknij przycisk **Dodaj**.

9. W otwartym oknie wprowadź ścieżkę dostępu do folderu współdzielonego.

   Adres źródłowy musi odpowiadać adresowi, który wcześniej określono w polu **Ścieżka** podczas konfiguracji kopiowania pakietu aktualizacyjnego do folderu współdzielonego (patrz powyższa instrukcja).

10. Kliknij **OK**.

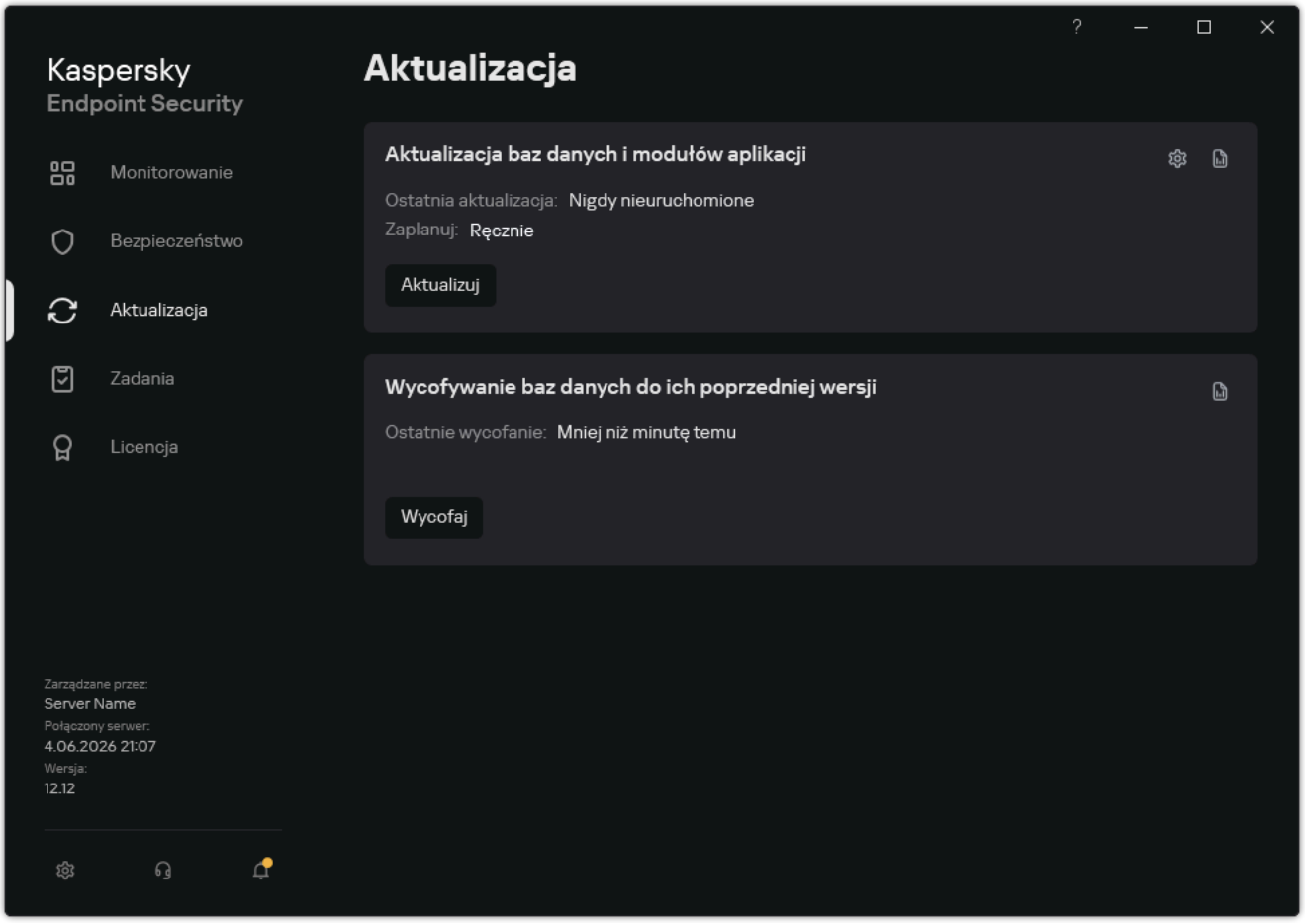
11. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

12. Zapisz swoje zmiany.

Jak w interfejsie aplikacji skonfigurować aktualizacje z folderu współdzielonego

Nie możesz skonfigurować zadania grupowego *Aktualizacja baz danych i modułów aplikacji* w interfejsie aplikacji. Tylko lokalne zadanie aktualizacji, *Aktualizacja baz danych i modułów aplikacji*, jest dostępne dla użytkownika. Jeśli zadanie *Aktualizacja baz danych i modułów aplikacji* nie jest wyświetlane, oznacza to, że administrator zabronił używania zadań lokalnych w zasadzie.

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.



Lokalne zadania aktualizacji

2. To spowoduje otwarcie listy zadań; wybierz zadanie *Aktualizacja baz danych i modułów aplikacji* i kliknij ⚙. Zostanie otwarte okno właściwości zadania.
3. Kliknij **Wybierz źródła aktualizacji**.
4. W otwartym oknie kliknij przycisk **Dodaj**.
5. W otwartym oknie wprowadź ścieżkę dostępu do folderu współdzielonego.

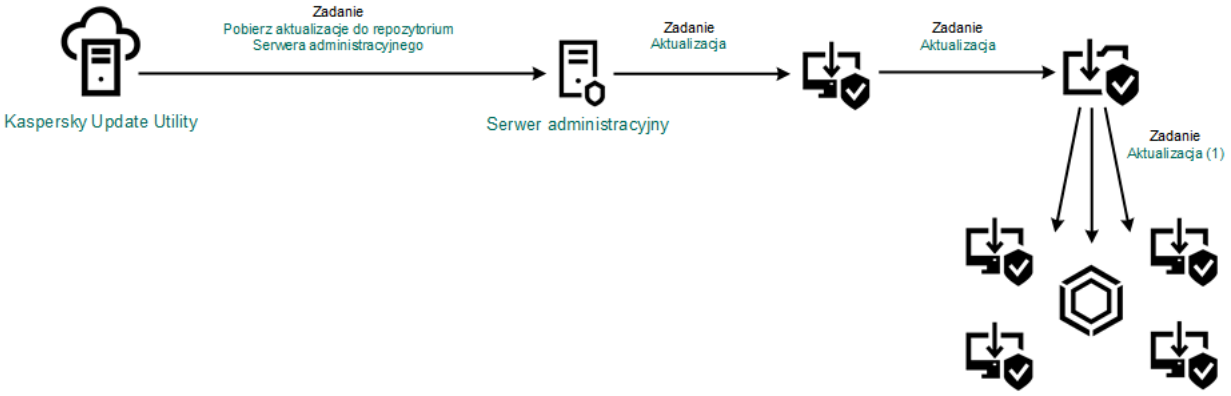
   Adres źródłowy musi odpowiadać adresowi, który wcześniej określono podczas konfiguracji kopiowania pakietu aktualizacyjnego do folderu współdzielonego (patrz powyższa instrukcja).

6. Kliknij **Wybierz**.

7. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

   Jeśli aktualizacja nie może zostać wykonana z pierwszego źródła uaktualnień, Kaspersky Endpoint Security automatycznie przełączy się do kolejnego źródła.

8. Zapisz swoje zmiany.



Aktualizowanie z folderu współdzielonego

Aktualizowanie przy użyciu narzędzia Kaspersky Update Utility

Aby oszczędzić ruch sieciowy, możesz skonfigurować aktualizacje baz danych i modułów aplikacji na komputerach sieci LAN organizacji z folderu współdzielonego przy użyciu Kaspersky Update Utility. W tym celu jeden z komputerów w sieci LAN organizacji musi odbierać pakiety aktualizacji z Serwera administracyjnego Kaspersky Security Center lub z serwerów aktualizacji Kaspersky i kopiuje te pakiety aktualizacji do folderu współdzielonego przy użyciu narzędzia. Pozostałe komputery w sieci LAN organizacji będą mogły pobrać pakiety aktualizacji z tego folderu współdzielonego.

Wersja i lokalizacja aplikacji Kaspersky Endpoint Security, która kopiuje pakiet aktualizacyjny do folderu współdzielonego, musi odpowiadać wersji i lokalizacji aplikacji, która aktualizuje bazy danych z folderu współdzielonego. Jeśli wersje lub lokalizacje aplikacji nie odpowiadają, aktualizacja baz danych może zakończyć się błędem.

Konfigurowanie aktualizacji baz danych i modułów aplikacji z folderu współdzielonego obejmuje następujące kroki:

1. Konfigurowanie aktualizacji caz danych i modułów aplikacji z repozytorium serwera.
2. Zainstaluj narzędzie Kaspersky Update Utility na jednym z komputerów w sieci LAN organizacji.
3. Skonfiguruj kopiowanie pakietu aktualizacji do folderu współdzielonego w ustawieniach narzędzia Kaspersky Update Utility.

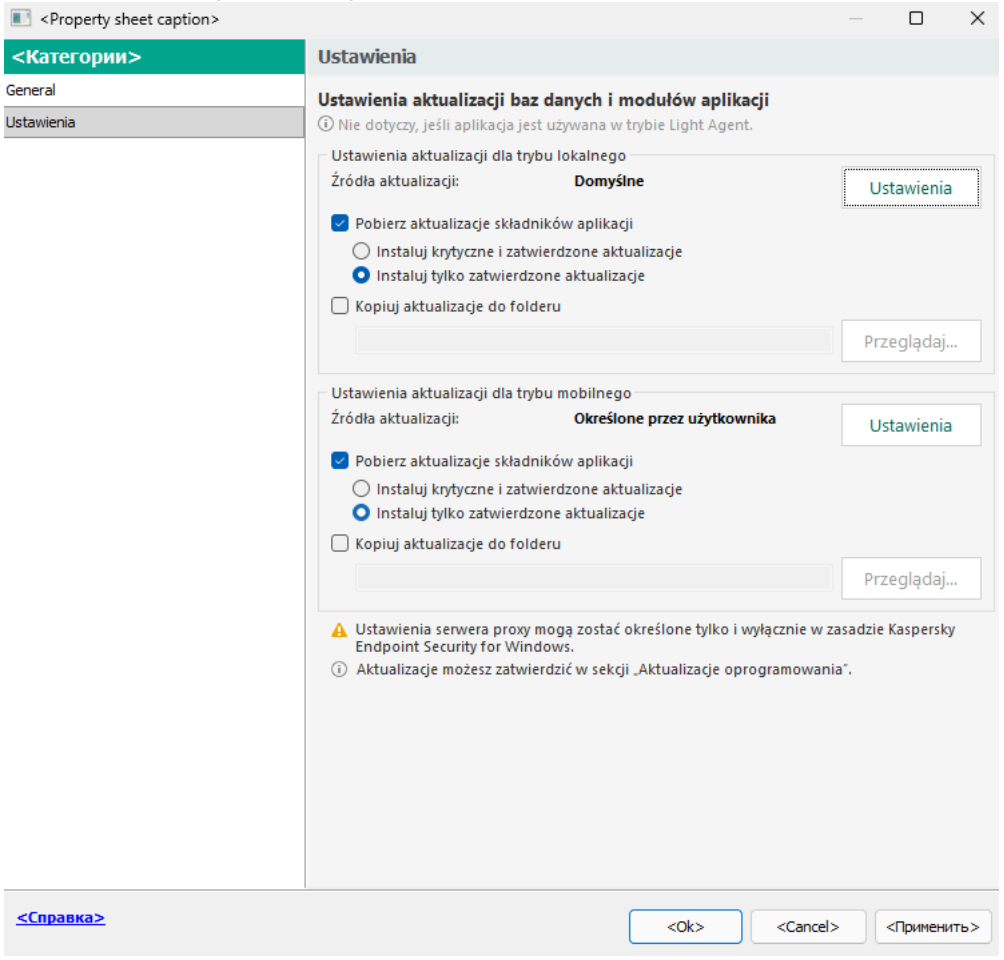
   Możesz pobrać pakiet dystrybucyjny Kaspersky Update Utility ze strony internetowej pomocy technicznej Kaspersky. Po zainstalowaniu narzędzia, wybierz źródło uaktualnień (na przykład, repozytorium Serwera administracyjnego) i folder współdzielony, do którego narzędzie Kaspersky Update Utility skopiuje pakiety aktualizacji. Szczegółowe informacje na temat korzystania z narzędzia Kaspersky Update Utility znajdziesz w Bazie wiedzy Kaspersky.
4. Konfigurację aktualizacji baz danych i modułów aplikacji z określonego folderu współdzielonego do pozostałych komputerów w sieci LAN organizacji.

Jak w Konsoli administracyjnej (MMC) skonfigurować aktualizacje z folderu współdzielonego

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zadania**.
3. Kliknij zadanie **Aktualizacja baz danych i modułów aplikacji** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

   Zadanie *Aktualizacja baz danych i modułów aplikacji* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja baz danych i modułów aplikacji*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.
4. W oknie właściwości zadania wybierz sekcję **Ustawienia**.



Ustawienia zadania Aktualizacja baz danych i modułów aplikacji

5. W sekcji **Ustawienia aktualizacji dla trybu lokalnego** kliknij przycisk **Ustawienia**.
6. Na liście źródeł uaktualnień kliknij przycisk **Dodaj**.
7. W oknie, które zostanie otwarte, wprowadź ścieżkę UNC do folderu współdzielonego (na przykład: `\\<server name>\KLSHARE\Updates`).

   Adres źródłowy musi odpowiadać adresowi wskazanemu w ustawieniach Kaspersky Update Utility.
8. Kliknij **OK**.

9. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

   Jeśli aktualizacja nie może zostać wykonana z pierwszego źródła uaktualnień, Kaspersky Endpoint Security automatycznie przełączy się do kolejnego źródła.

10. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console skonfigurować aktualizacje z folderu współdzielonego

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie **Aktualizacja** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

   Zadanie *Aktualizacja* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

3. Wybierz zakładkę **Ustawienia aplikacji** → **Tryb lokalny**.

4. Na liście źródeł uaktualnień kliknij przycisk **Dodaj**.

5. W oknie, które zostanie otwarte, wprowadź ścieżkę UNC do folderu współdzielonego (na przykład: `\\<server name>\KLSHARE\Updates`).

   > Adres źródłowy musi odpowiadać adresowi wskazanemu w ustawieniach Kaspersky Update Utility.

6. Kliknij **OK**.

7. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

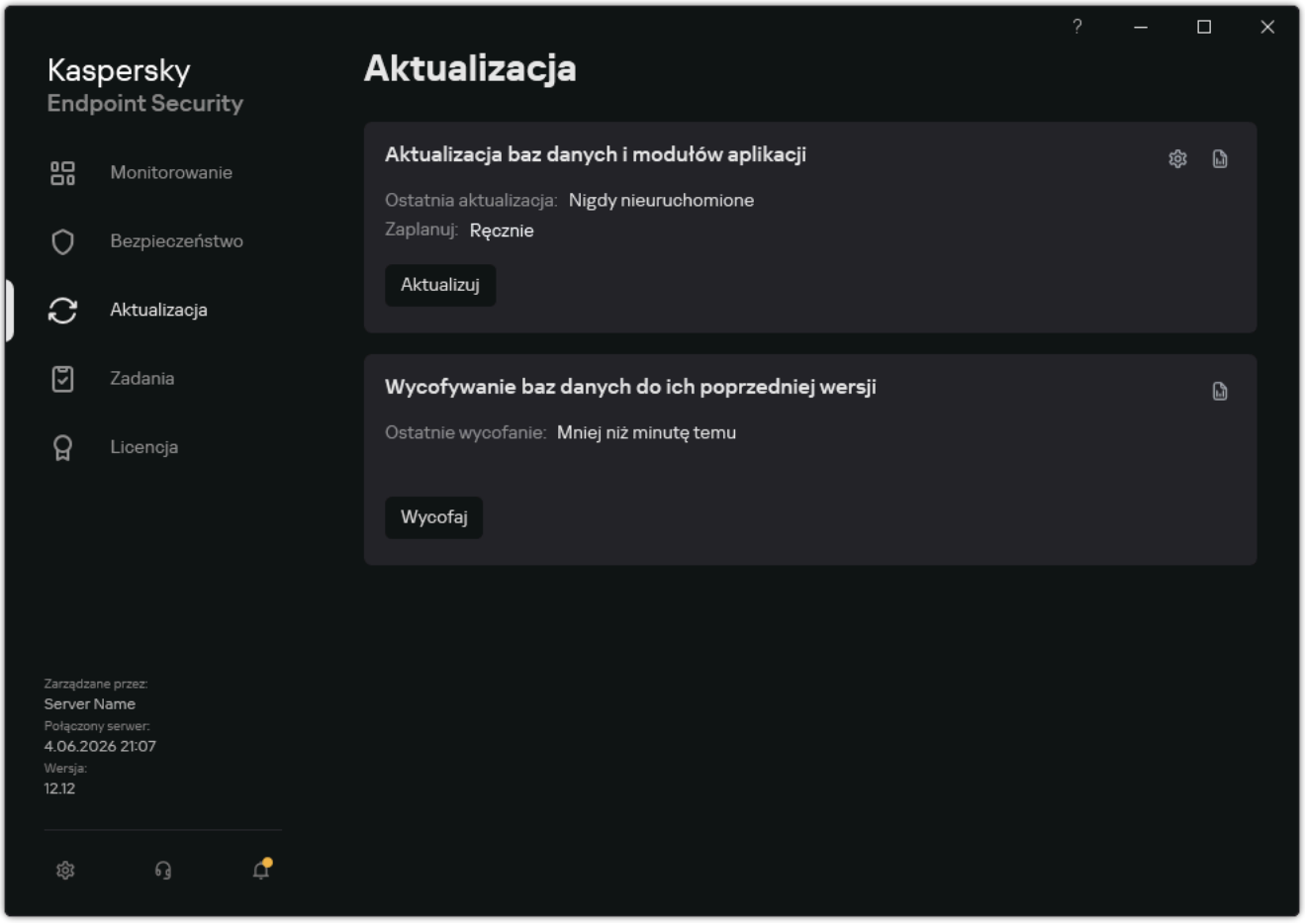
   Jeśli aktualizacja nie może zostać wykonana z pierwszego źródła uaktualnień, Kaspersky Endpoint Security automatycznie przełączy się do kolejnego źródła.

8. Zapisz swoje zmiany.

Jak w interfejsie aplikacji skonfigurować aktualizacje z folderu współdzielonego

Nie możesz skonfigurować zadania grupowego *Aktualizacja baz danych i modułów aplikacji* w interfejsie aplikacji. Tylko lokalne zadanie aktualizacji, *Aktualizacja baz danych i modułów aplikacji*, jest dostępne dla użytkownika. Jeśli zadanie *Aktualizacja baz danych i modułów aplikacji* nie jest wyświetlane, oznacza to, że administrator zabronił używania zadań lokalnych w zasadzie.

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.

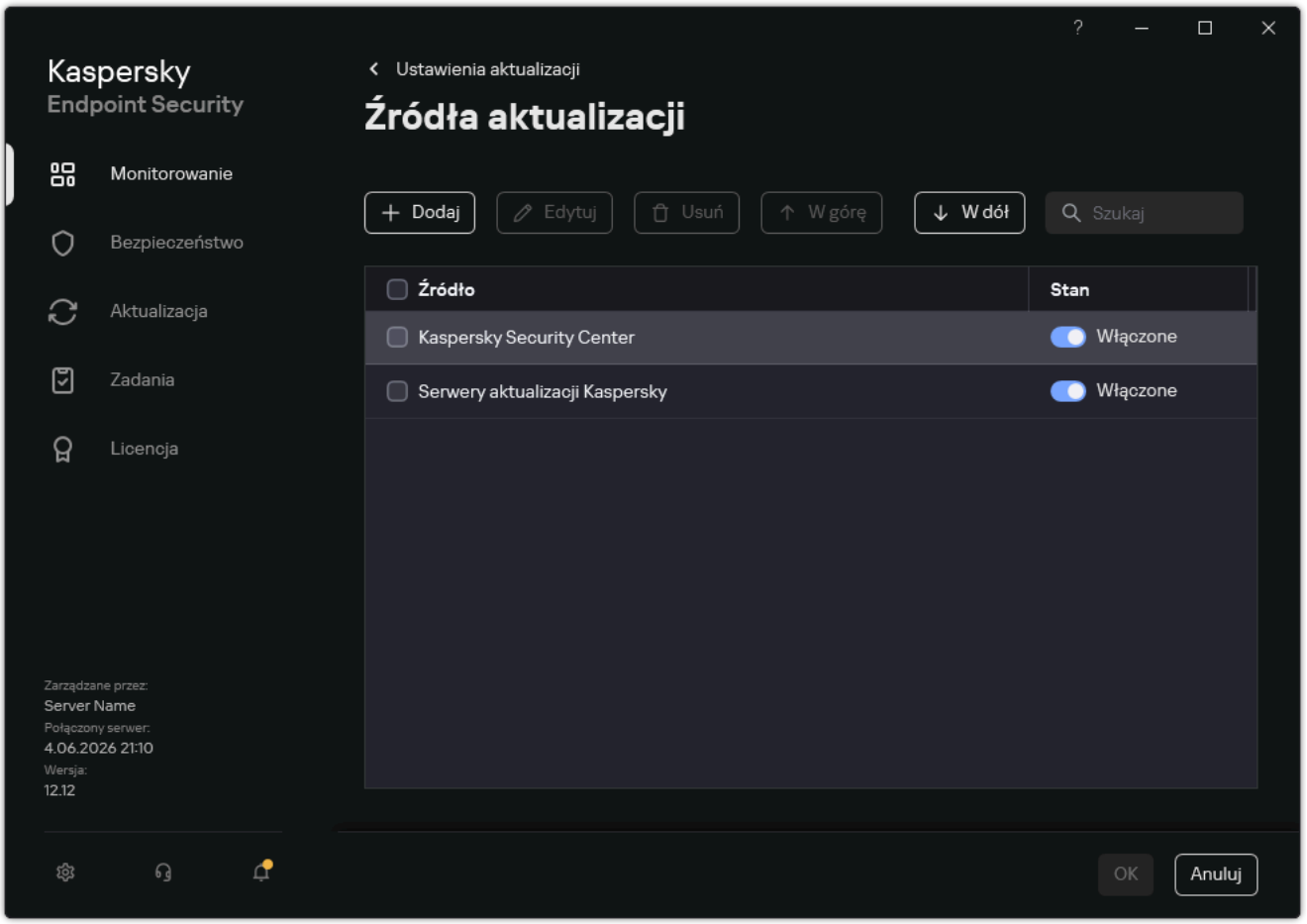


Lokalne zadania aktualizacji

2. To spowoduje otwarcie listy zadań; wybierz zadanie *Aktualizacja baz danych i modułów aplikacji* i kliknij ⚙. Zostanie otwarte okno właściwości zadania.

3. W oknie właściwości zadania kliknij **Wybierz źródła aktualizacji**.

4. Na liście źródeł uaktualnień kliknij przycisk **Dodaj**.



Źródła aktualizacji

5. Wprowadź ścieżkę UNC do folderu współdzielonego (na przykład: `\\<server name>\KLSHARE\Updates`).

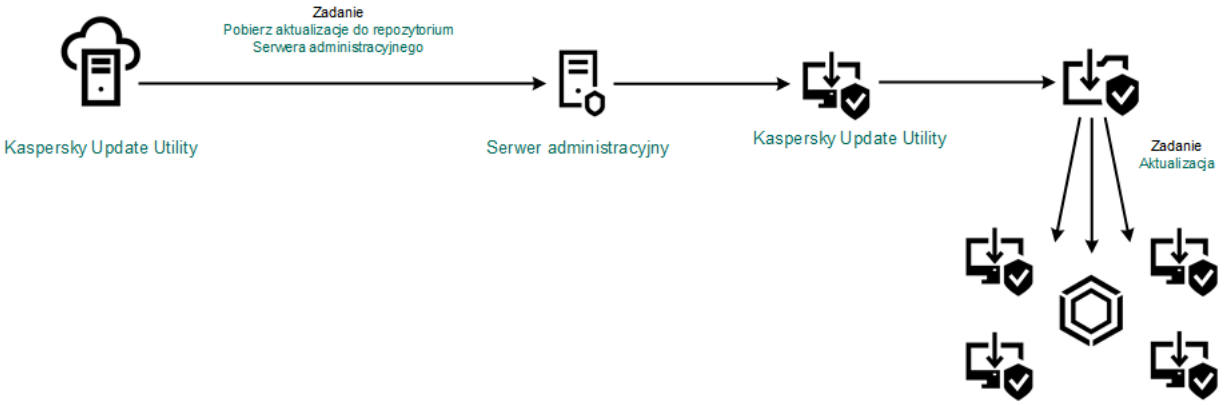
> Adres źródłowy musi odpowiadać adresowi wskazanemu w ustawieniach Kaspersky Update Utility.

6. Kliknij **Wybierz**.

7. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

   Jeśli aktualizacja nie może zostać wykonana z pierwszego źródła uaktualnień, Kaspersky Endpoint Security automatycznie przełączy się do kolejnego źródła.

8. Zapisz swoje zmiany.



Aktualizowanie przy użyciu narzędzia Kaspersky Update Utility

Aktualizowanie w trybie mobilnym

Tryb mobilny to tryb działania Kaspersky Endpoint Security, gdy komputer opuści sieć obwodową organizacji (*komputer offline*). Szczegółowe informacje na temat pracy z komputerami offline i użytkownikami mobilnymi można znaleźć w pomocy do Kaspersky Security Center.

Komputer offline poza siecią organizacji nie może nawiązać połączenia z Serwerem administracyjnym w celu zaktualizowania baz danych i modułów aplikacji. Domyślnie, tylko serwery aktualizacji Kaspersky są używane jako źródło uaktualnień do aktualizacji baz danych i modułów aplikacji w trybie mobilnym. Używanie serwera proxy do nawiązywania połączenia z internetem jest określane przez specjalny profil użytkownika mobilnego. Profil użytkownika mobilnego musi zostać utworzony oddzielnie. Jeśli program Kaspersky Endpoint Security zostanie przełączony do trybu mobilnego, zadanie aktualizacji będzie uruchamiane co dwie godziny.

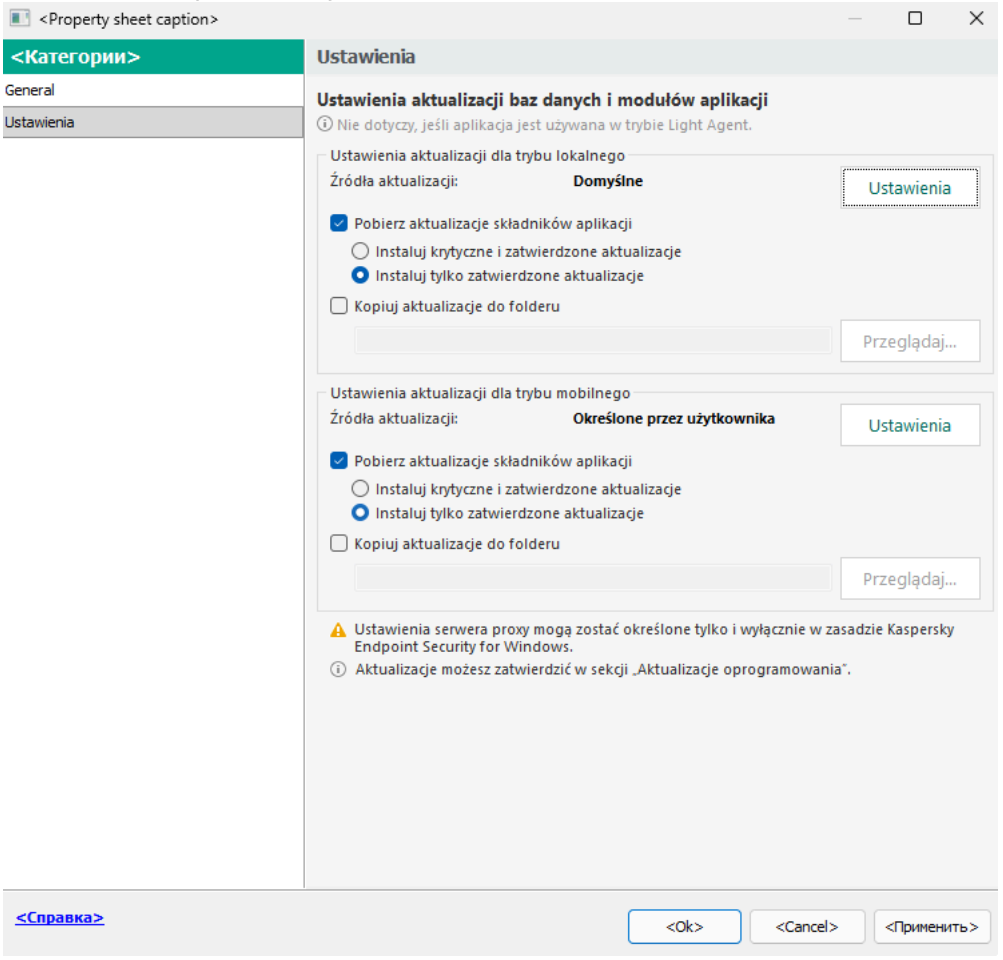
Jak skonfigurować ustawienia aktualizacji dla trybu mobilnego w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zadania**.
3. Kliknij zadanie **Aktualizacja baz danych i modułów aplikacji** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

   Zadanie *Aktualizacja baz danych i modułów aplikacji* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja baz danych i modułów aplikacji*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

4. W oknie właściwości zadania wybierz sekcję **Ustawienia**.



Ustawienia zadania Aktualizacja baz danych i modułów aplikacji

5. W sekcji **Ustawienia aktualizacji dla trybu mobilnego** kliknij przycisk **Ustawienia**.

6. Skonfiguruj źródła uaktualnień. Źródłami uaktualnień mogą być serwery aktualizacji Kaspersky, inne serwery FTP i HTTP, foldery lokalne lub foldery sieciowe.

7. Zapisz swoje zmiany.

Jak skonfigurować ustawień aktualizacji dla trybu mobilnego w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie **Aktualizacja** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

   Zadanie *Aktualizacja* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

3. Wybierz zakładkę **Ustawienia aplikacji** → **Tryb mobilny**.

4. Skonfiguruj źródła uaktualnień. Źródłami uaktualnień mogą być serwery aktualizacji Kaspersky, inne serwery FTP i HTTP, foldery lokalne lub foldery sieciowe.

5. Zapisz swoje zmiany.

W wyniku tego działania, bazy danych i moduły aplikacji zostaną zaktualizowane na komputerach użytkownika, gdy przełączą się do trybu mobilnego.

Uruchamianie i zatrzymywanie zadania aktualizacji

Bez względu na wybrany tryb uruchamiania zadania aktualizacji, możesz uruchomić lub zatrzymać zadanie aktualizacji Kaspersky Endpoint Security w dowolnym momencie.

W celu uruchomienia lub zatrzymania zadania aktualizacji:

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.
2. W sekcji **Aktualizacja baz danych i modułów aplikacji** kliknij przycisk **Aktualizuj**, jeśli chcesz uruchomić zadanie aktualizacji.

   Kaspersky Endpoint Security uruchomi aktualizację modułów i baz danych aplikacji. Aplikacja wyświetli postęp wykonywania zadania, rozmiar pobranych plików i źródło uaktualnień. Kliknij przycisk **Zatrzymaj aktualizację**, aby zatrzymać zadanie w dowolnym momencie.

W celu uruchomienia lub zatrzymania zadania aktualizacji, gdy wyświetlany jest uproszczony interfejs aplikacji:

1. Kliknij prawym przyciskiem myszy ikonę aplikacji znajdującą się w obszarze powiadomień paska zadań.
2. W menu kontekstowym, z listy rozwijalnej **Zadania**:
   - wybierz nieuruchomione zadanie aktualizacji, żeby je uruchomić
   - wybierz uruchomione zadanie aktualizacji, żeby je zatrzymać
   - wybierz wstrzymane zadanie aktualizacji, żeby je wznowić lub uruchomić ponownie

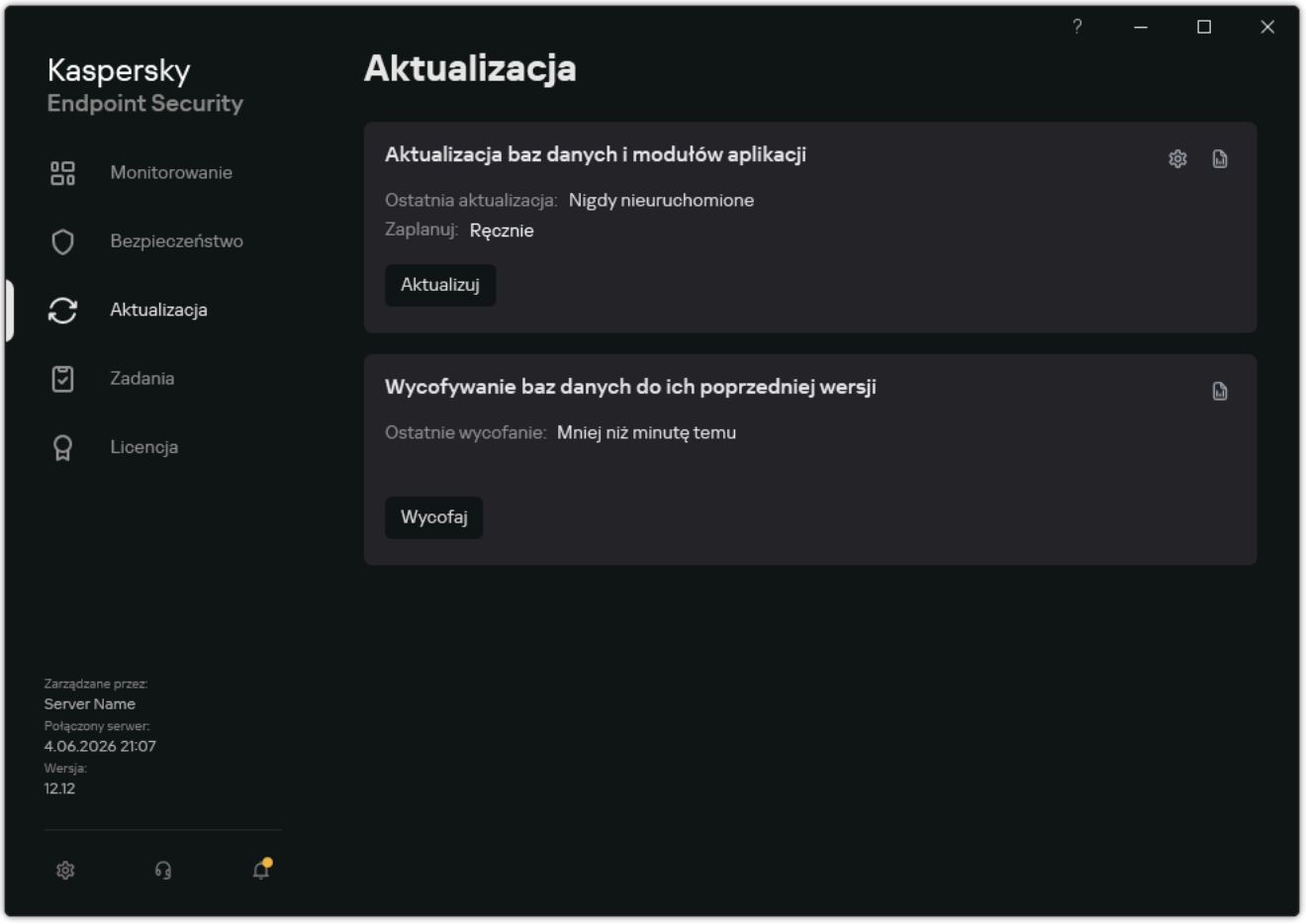
Uruchamianie zadania aktualizacji z poziomu konta innego użytkownika

Domyślnie zadanie aktualizacji Kaspersky Endpoint Security jest uruchamiane z poziomu konta użytkownika, którego użyłeś do uruchomienia systemu operacyjnego. Jednakże program Kaspersky Endpoint Security może zostać zaktualizowany ze źródła uaktualnień, do którego użytkownik nie ma dostępu ze względu na brak wymaganych uprawnień (na przykład, z folderu współdzielonego, który zawiera pakiet uaktualnień) lub ze źródła uaktualnień, dla którego nie skonfigurowano autoryzacji na serwerze proxy. W ustawieniach aplikacji możesz wskazać użytkownika, który posiada takie uprawnienia, i skonfigurować uruchamianie zadania aktualizacji Kaspersky Endpoint Security z poziomu konta tego użytkownika.

W celu uruchomienia zadania aktualizacji z poziomu konta innego użytkownika:

Nie możesz skonfigurować zadania grupowego *Aktualizacja baz danych i modułów aplikacji* w interfejsie aplikacji. Tylko lokalne zadanie aktualizacji, *Aktualizacja baz danych i modułów aplikacji*, jest dostępne dla użytkownika. Jeśli zadanie *Aktualizacja baz danych i modułów aplikacji* nie jest wyświetlane, oznacza to, że administrator zabronił używania zadań lokalnych w zasadzie.

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.



Lokalne zadania aktualizacji

2. To spowoduje otwarcie listy zadań; wybierz zadanie *Aktualizacja baz danych i modułów aplikacji* i kliknij ⚙.
   Zostanie otwarte okno właściwości zadania.
3. Kliknij **Uruchom zadania aktualizacji bazy danych z uprawnieniami użytkownika**.
4. W otwartym oknie wybierz **Inny użytkownik**.
5. Wprowadź dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami dostępu do źródła uaktualnień.
6. Zapisz swoje zmiany.

Wybieranie trybu uruchamiania zadania aktualizacji

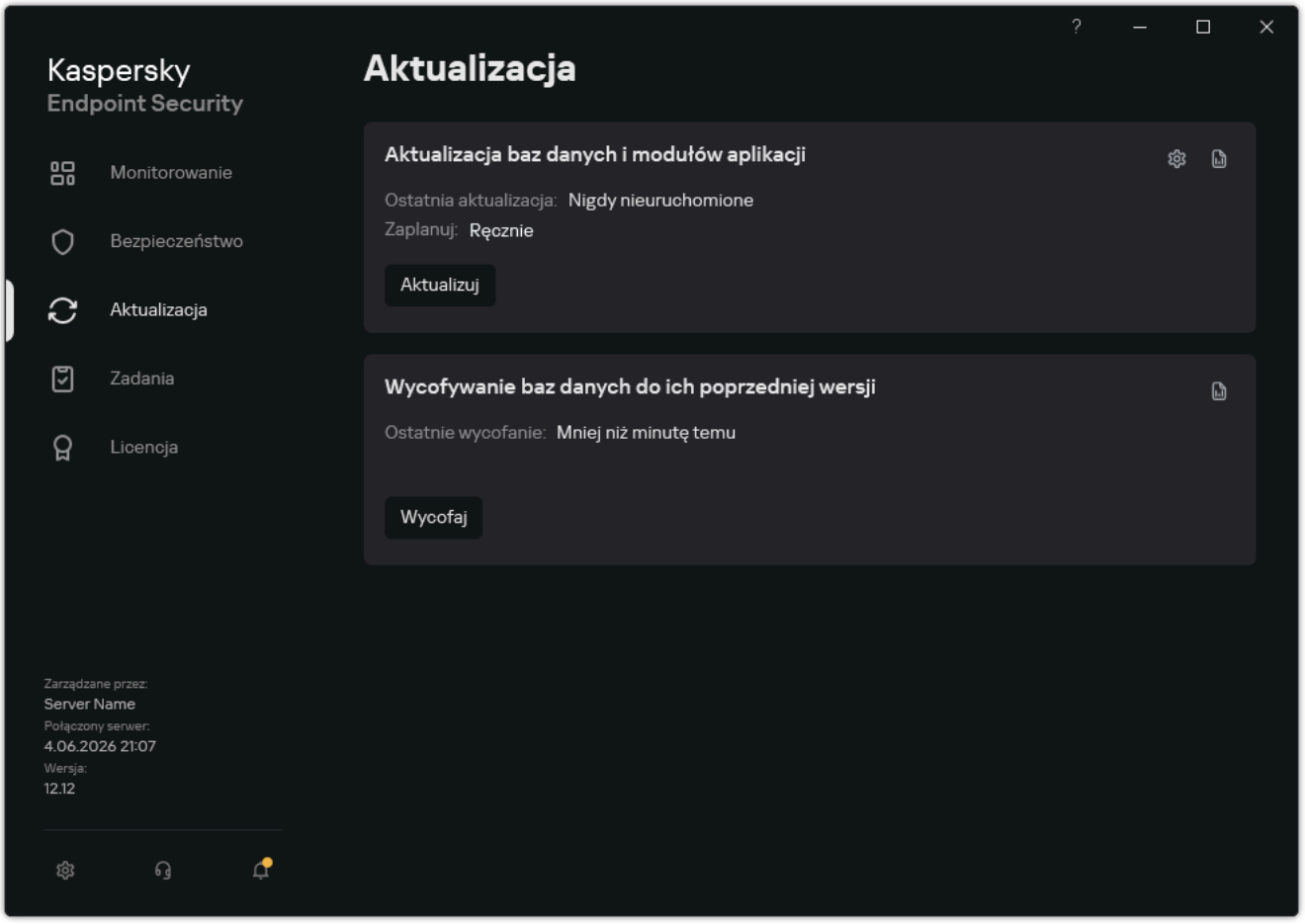
Jeżeli z jakiegoś powodu uruchomienie zadania aktualizacji nie będzie możliwe (na przykład komputer nie będzie włączony o określonym czasie), można skonfigurować automatyczne uruchamianie pominiętego zadania przy najbliższej możliwej okazji.

Możesz odroczyć rozpoczęcie zadania aktualizacji po uruchomieniu aplikacji, jeżeli wybrałeś tryb uruchamiania **Zgodnie z terminarzem**, a czas włączenia Kaspersky Endpoint Security pokrywa się z czasem uruchomienia zadania aktualizacji. Zadanie aktualizacji może zostać uruchomione dopiero po minięciu określonego czasu od uruchomienia programu Kaspersky Endpoint Security.

W celu wybrania trybu uruchamiania zadania aktualizacji:

Nie możesz skonfigurować zadania grupowego *Aktualizacja baz danych i modułów aplikacji* w interfejsie aplikacji. Tylko lokalne zadanie aktualizacji, *Aktualizacja baz danych i modułów aplikacji*, jest dostępne dla użytkownika. Jeśli zadanie *Aktualizacja baz danych i modułów aplikacji* nie jest wyświetlane, oznacza to, że administrator zabronił używania zadań lokalnych w zasadzie.

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.



Lokalne zadania aktualizacji

2. To spowoduje otwarcie listy zadań; wybierz zadanie *Aktualizacja baz danych i modułów aplikacji* i kliknij ⚙.

   Zostanie otwarte okno właściwości zadania.

3. Kliknij **Tryb uruchamiania**.

4. W otwartym oknie wybierz tryb uruchamiania zadania aktualizacji:

   - Jeżeli Kaspersky Endpoint Security ma uruchamiać zadanie aktualizacji w zależności od tego, czy w źródle uaktualnień dostępny jest pakiet uaktualnień, wybierz **Automatycznie**. Częstotliwość sprawdzania źródła uaktualnień przez Kaspersky Endpoint Security w poszukiwaniu pakietów uaktualnień wzrasta podczas epidemii wirusów.

   - Jeżeli chcesz uruchomić zadanie aktualizacji ręcznie, wybierz **Ręcznie**.

- Jeśli chcesz skonfigurować terminarz uruchamiania zadania aktualizacji, wybierz inne opcje. Skonfiguruj zaawansowane ustawienia uruchamiania zadania aktualizacji:

  - W polu **Odrocz uruchomienie zadania po starcie aplikacji o N minut** określ czas, na jaki chcesz odroczyć uruchomienie zadania aktualizacji po uruchomieniu Kaspersky Endpoint Security.

  - Wybierz **Jeśli komputer jest wyłączony, uruchom zaplanowane skanowanie następnego dnia**, jeśli chcesz, żeby Kaspersky Endpoint Security uruchamiał pominięte zadania aktualizacji przy pierwszej okazji. Gdy aplikacja uzyska możliwość wykonania pominiętych zadań, uruchamia zadania losowo w określonym przedziale czasu, aby rozłożyć obciążenie na komputerze.

5. Zapisz swoje zmiany.

Dodawanie źródła uaktualnień

Źródło uaktualnień jest zasobem zawierającym uaktualnienia baz danych oraz modułów aplikacji Kaspersky Endpoint Security.

Źródłami uaktualnień mogą być serwer Kaspersky Security Center, serwery aktualizacji Kaspersky i foldery lokalne lub sieciowe.

Jeśli serwery aktualizacji Kaspersky są niedostępne, Kaspersky Endpoint Security może użyć alternatywnych domen w celu zaktualizowania swoich baz danych i modułów oprogramowania aplikacji. Aby uzyskać szczegółowe informacje, zapoznaj się z Bazą wiedzy na stronie działu pomocy technicznej.

Domyślna lista źródeł uaktualnień zawiera serwery aktualizacji Kaspersky Security Center i Kaspersky. Do listy można dodać inne źródło uaktualnień. Źródłem uaktualnień mogą być serwery HTTP/FTP oraz foldery współdzielone.

Kaspersky Endpoint Security nie obsługuje aktualizacji z serwerów HTTPS, chyba że są to serwery aktualizacji Kaspersky.

Jeżeli jako aktywne ustawiono kilka źródeł uaktualnień, Kaspersky Endpoint Security będzie podejmował próby nawiązywania połączenia z każdym z nich, począwszy od góry listy; uaktualnienia zostaną pobrane z pierwszego dostępnego źródła.

Domyślnie Kaspersky Endpoint Security używa serwera Kaspersky Security Center jako pierwszego źródła aktualizacji. Pomaga to oszczędzać ruch podczas aktualizacji. Jeśli zasada nie zostanie zastosowana do komputera, serwery Kaspersky zostaną wybrane jako pierwsze źródło aktualizacji w ustawieniach lokalnego zadania *Aktualizacja baz danych i modułów aplikacji*, ponieważ aplikacja może nie mieć dostępu do serwera Kaspersky Security Center.

Jeśli aplikacja działa w trybie Light Agent, jako źródło aktualizacji wybierany jest folder na maszynie SVM.

Jak dodawać źródło aktualizacji w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

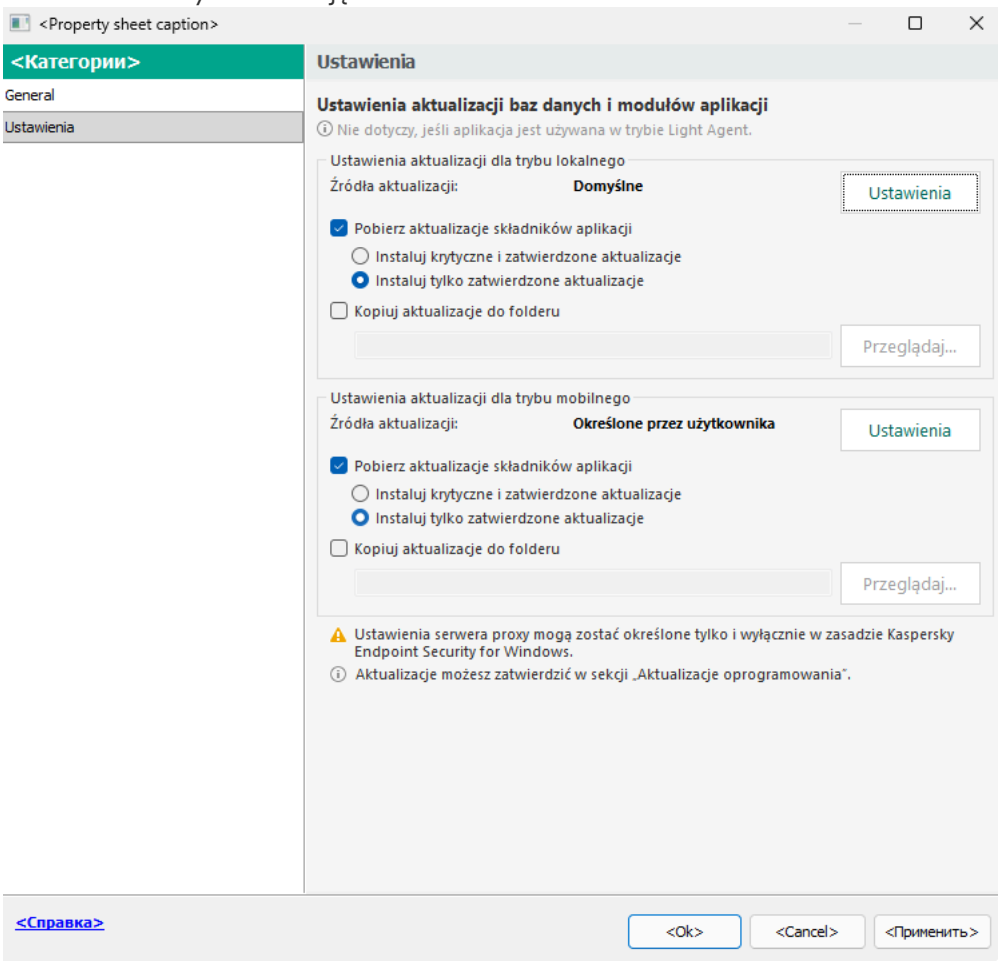
   W drzewie konsoli wybierz **Zadania**.

2. Kliknij zadanie **Aktualizacja baz danych i modułów aplikacji** Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości zadania.

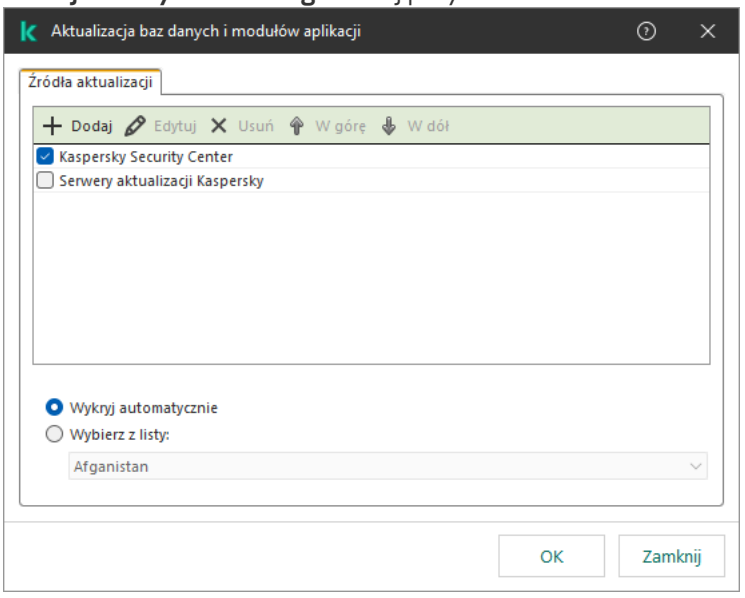
Zadanie *Aktualizacja baz danych i modułów aplikacji* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja baz danych i modułów aplikacji*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

3. W oknie właściwości zadania wybierz sekcję **Ustawienia**.



Ustawienia zadania Aktualizacja baz danych i modułów aplikacji

4. W sekcji **Ustawienia aktualizacji dla trybu lokalnego** kliknij przycisk **Ustawienia**.



Źródła aktualizacji

5. Na liście źródeł uaktualnień kliknij przycisk **Dodaj**.

6. W polu **Źródła aktualizacji** określ adres serwera FTP lub HTTP, folderu sieciowego lub folderu lokalnego, który zawiera pakiet aktualizacyjny.

   Dla źródła uaktualnień używany jest następujący format ścieżki dostępu:

   - Dla serwera FTP lub HTTP wprowadź jego adres internetowy lub adres IP.

     Na przykład: `http://dnl-01.geo.kaspersky.com/` lub `93.191.13.103`.

     Dla serwera FTP możesz określić ustawienia autoryzacji w adresie internetowym, w następującym formacie: `ftp://<user name>:<password>@<node>:<port>`.

   - Dla folderu sieciowego wprowadź ścieżkę UNC.

     Na przykład, `\\Server\Share\Update distribution`.

   - Dla folderu lokalnego wprowadź pełną ścieżkę do tego folderu.

     Na przykład, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   Możesz wykluczyć źródło aktualizacji bez usuwania go z listy źródeł aktualizacji. W tym celu odznacz pole obok obiektu.

7. Kliknij **OK**.

8. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

   Jeśli aktualizacja nie może zostać wykonana z pierwszego źródła uaktualnień, Kaspersky Endpoint Security automatycznie przełączy się do kolejnego źródła.

9. Jeśli to konieczne, dodaj źródło aktualizacji dla trybu mobilnego. *Tryb mobilny* to tryb działania Kaspersky Endpoint Security, gdy komputer opuści sieć obwodową organizacji (*komputer offline*).

10. Zapisz swoje zmiany.

Jak dodać źródło aktualizacji w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zadania**.

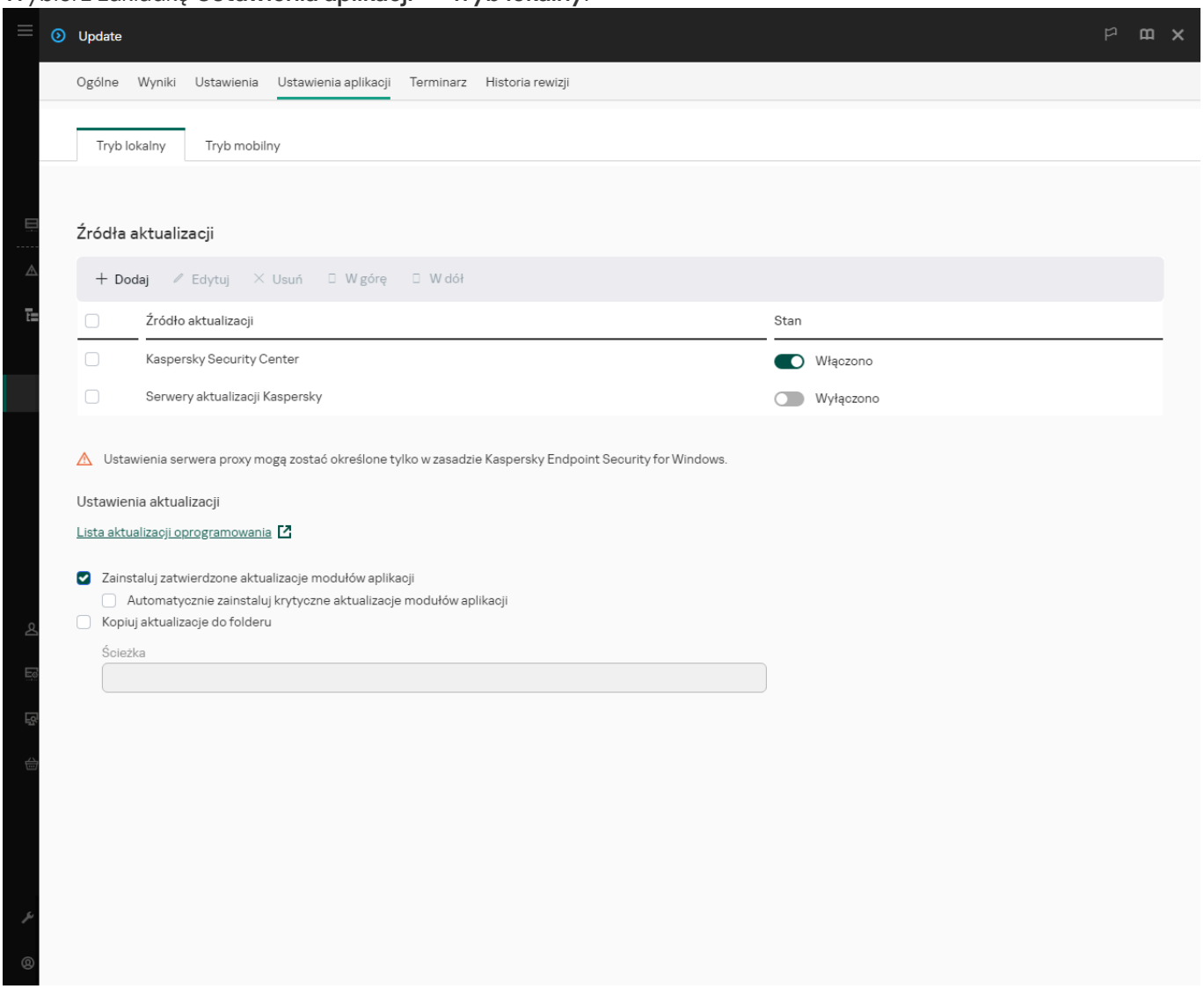
   Zostanie otwarta lista zadań.

2. Kliknij zadanie **Aktualizacja** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

   Zadanie *Aktualizacja* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

3. Wybierz zakładkę **Ustawienia aplikacji** → **Tryb lokalny**.



Źródła aktualizacji

4. Na liście źródeł uaktualnień kliknij przycisk **Dodaj**.

5. W otwartym oknie określ adres serwera FTP lub http, folderu sieciowego lub folderu lokalnego, który zawiera pakiet aktualizacyjny.

   Dla źródła uaktualnień używany jest następujący format ścieżki dostępu:

   - Dla serwera FTP lub HTTP wprowadź jego adres internetowy lub adres IP.

     Na przykład: `http://dnl-01.geo.kaspersky.com/` lub `93.191.13.103`.

     Dla serwera FTP możesz określić ustawienia autoryzacji w adresie internetowym, w następującym formacie: `ftp://<user name>:<password>@<node>:<port>`.

   - Dla folderu sieciowego wprowadź ścieżkę UNC.

     Na przykład, `\\Server\Share\Update distribution`.

   - Dla folderu lokalnego wprowadź pełną ścieżkę do tego folderu.

     Na przykład, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   Możesz wykluczyć źródło aktualizacji bez usuwania go z listy źródeł aktualizacji. W tym celu ustaw przycisk przełącznika obok obiektu na pozycję wyłączenia.

6. Kliknij **OK**.

7. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

   Jeśli aktualizacja nie może zostać wykonana z pierwszego źródła uaktualnień, Kaspersky Endpoint Security automatycznie przełączy się do kolejnego źródła.

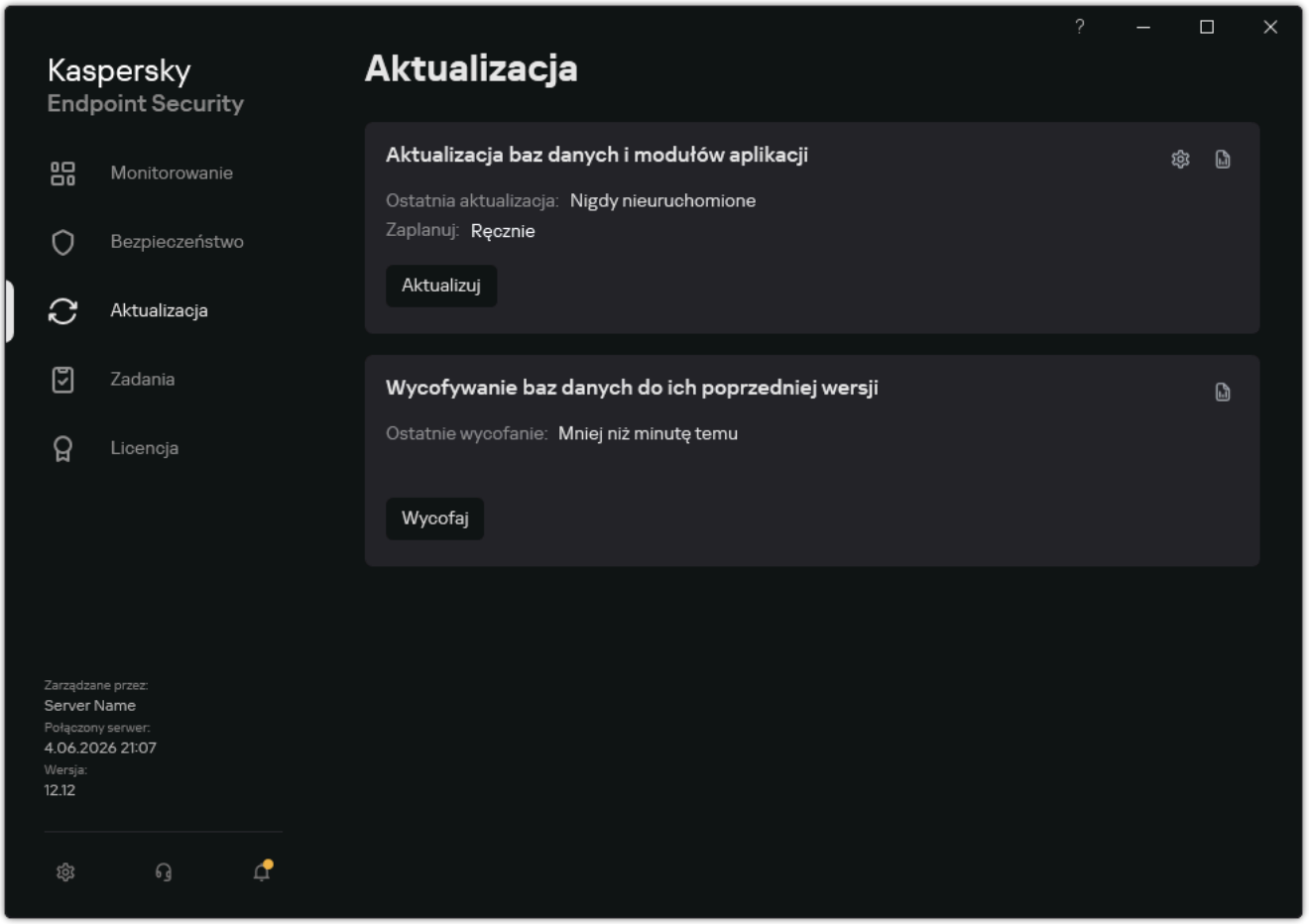
8. Jeśli to konieczne, dodaj źródło aktualizacji dla trybu mobilnego. *Tryb mobilny* to tryb działania Kaspersky Endpoint Security, gdy komputer opuści sieć obwodową organizacji (*komputer offline*).

9. Zapisz swoje zmiany.

Jak dodać źródło aktualizacji w interfejsie aplikacji

Nie możesz skonfigurować zadania grupowego *Aktualizacja baz danych i modułów aplikacji* w interfejsie aplikacji. Tylko lokalne zadanie aktualizacji, *Aktualizacja baz danych i modułów aplikacji*, jest dostępne dla użytkownika. Jeśli zadanie *Aktualizacja baz danych i modułów aplikacji* nie jest wyświetlane, oznacza to, że administrator zabronił używania zadań lokalnych w zasadzie.

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.



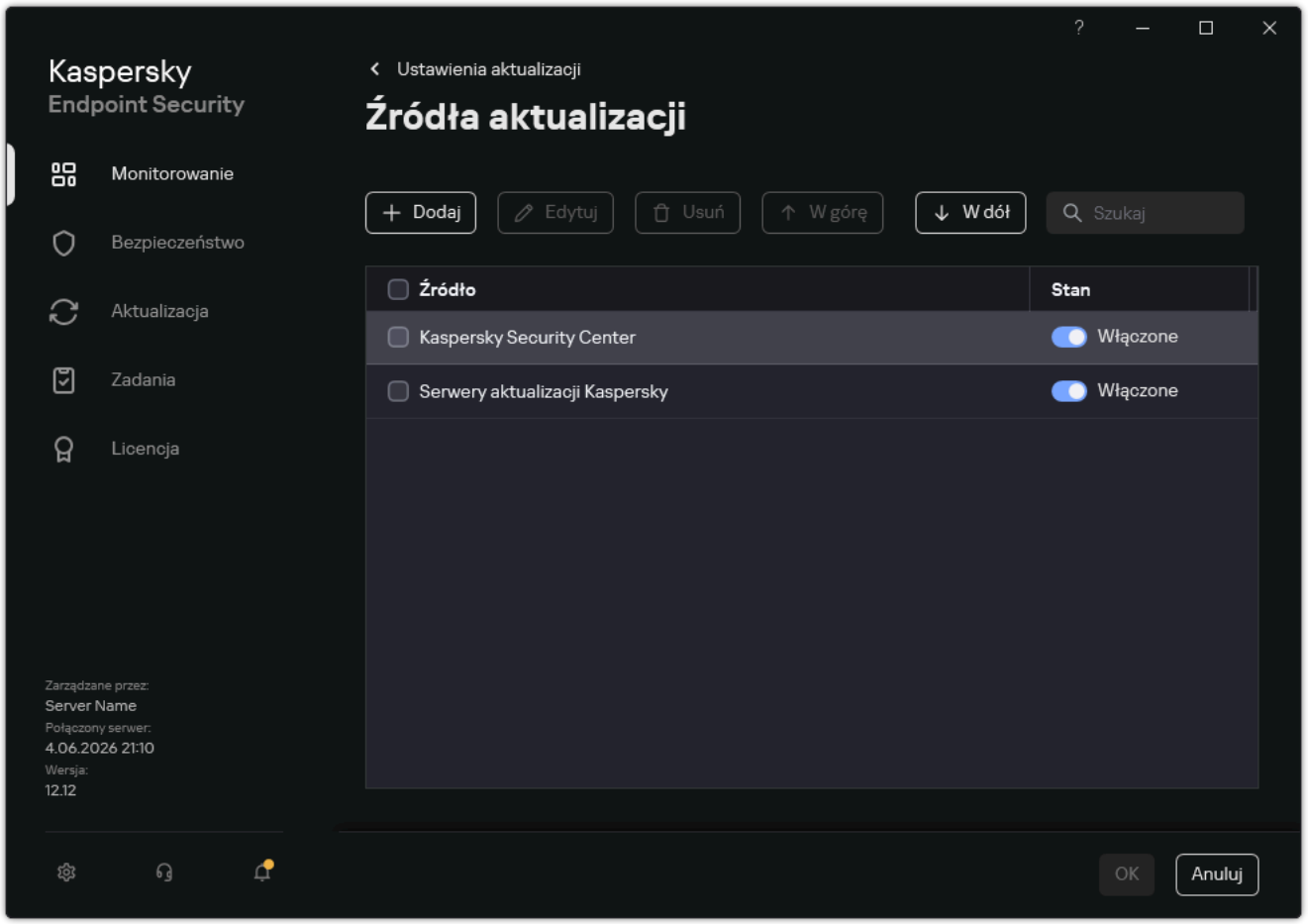
Lokalne zadania aktualizacji

2. To spowoduje otwarcie listy zadań; wybierz zadanie *Aktualizacja baz danych i modułów aplikacji* i kliknij ⚙.

   Zostanie otwarte okno właściwości zadania.

3. Kliknij **Wybierz źródła aktualizacji**.

4. W otwartym oknie kliknij przycisk **Dodaj**.



Źródła aktualizacji

5. W otwartym oknie określ adres serwera FTP lub http, folderu sieciowego lub folderu lokalnego, który zawiera pakiet aktualizacyjny.

   Dla źródła uaktualnień używany jest następujący format ścieżki dostępu:

   - Dla serwera FTP lub HTTP wprowadź jego adres internetowy lub adres IP.

     Na przykład: `http://dnl-01.geo.kaspersky.com/` lub `93.191.13.103`.

     Dla serwera FTP możesz określić ustawienia autoryzacji w adresie internetowym, w następującym formacie: `ftp://<user name>:<password>@<node>:<port>`.

   - Dla folderu sieciowego wprowadź ścieżkę UNC.

     Na przykład, `\\Server\Share\Update distribution`.

   - Dla folderu lokalnego wprowadź pełną ścieżkę do tego folderu.

     Na przykład, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Kliknij **Wybierz**.

7. Skonfiguruj priorytety źródeł aktualizacji, korzystając z przycisków **W górę** i **W dół**.

8. Zapisz swoje zmiany.

Aktualizowanie modułów aplikacji

Aktualizacje modułów aplikacji naprawiają błędy, udoskonalają działanie i dodają nowe funkcje. Jeśli nowe aktualizacje modułów aplikacji staną się dostępne, musisz potwierdzić instalację aktualizacji. Możesz potwierdzić instalację aktualizacji modułu aplikacji w interfejsie aplikacji lub w Kaspersky Security Center. Zawsze, gdy aktualizacja jest dostępna, aplikacja wyświetli powiadomienie w oknie głównym Kaspersky Endpoint Security: . Jeśli uaktualnienia modułów aplikacji wymagają przeczytanie i zaakceptowanie warunków Umowy licencyjnej, aplikacja zainstaluje uaktualnienia po zaakceptowaniu warunków Umowy licencyjnej.

Po zainstalowaniu aktualizacji aplikacji konieczne może być ponowne uruchomienie komputera.

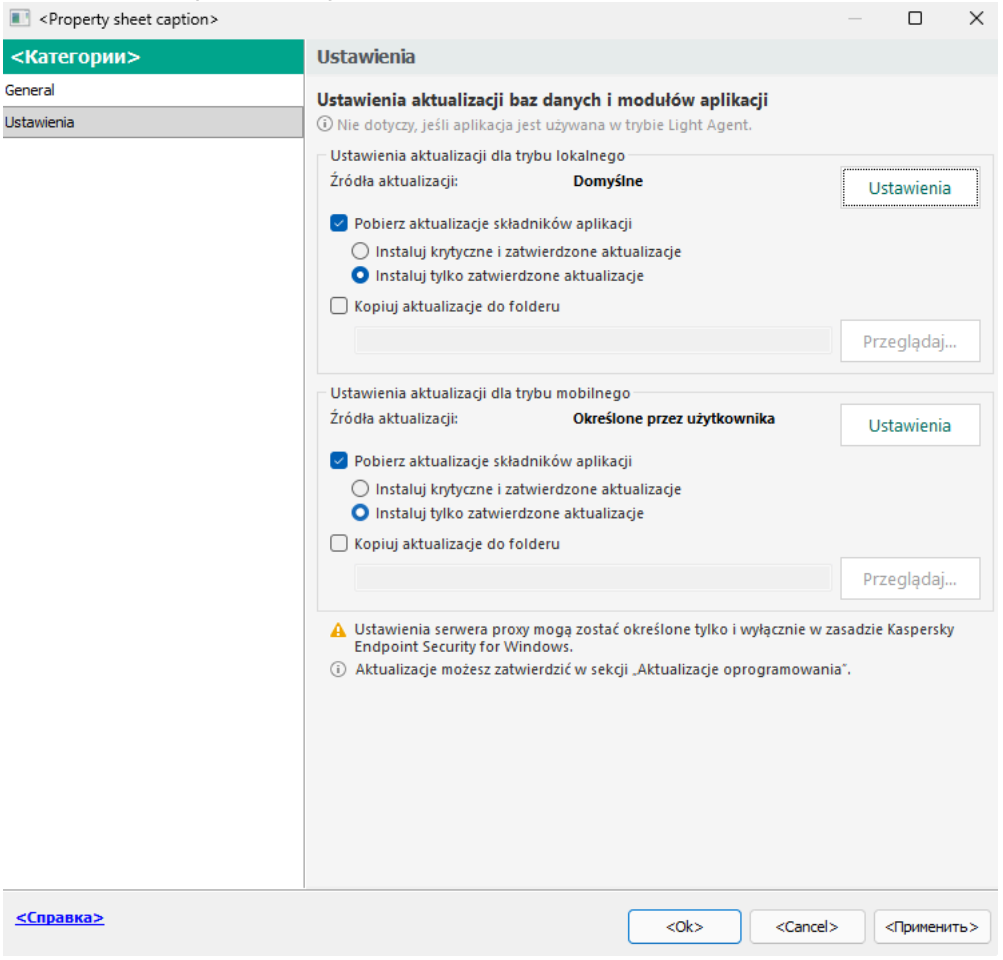
Jak w Konsoli administracyjnej (MMC) skonfigurować aktualizacje modułu aplikacji?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zadania**.
3. Kliknij zadanie **Aktualizacja baz danych i modułów aplikacji** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

   Zadanie *Aktualizacja baz danych i modułów aplikacji* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja baz danych i modułów aplikacji*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

4. W oknie właściwości zadania wybierz sekcję **Ustawienia**.



Ustawienia zadania Aktualizacja baz danych i modułów aplikacji

5. W sekcji **Ustawienia aktualizacji dla trybu lokalnego** zaznacz pole **Pobierz aktualizacje składników aplikacji**.

   Jeśli chcesz uniemożliwić pobieranie aktualizacji modułów aplikacji, usuń zaznaczenie pola wyboru **Pobierz aktualizacje składników aplikacji** i zabronić użytkownikowi korzystania z lokalnych zadań.

6. Wybierz aktualizacje modułów aplikacji, które chcesz zainstalować.

   - **Instaluj krytyczne i zatwierdzone aktualizacje**. Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security automatycznie instaluje krytyczne uaktualnienia, a także wszystkie inne uaktualnienia modułów aplikacji po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center.

   - **Instaluj tylko zatwierdzone aktualizacje**. Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security instaluje je po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center. Ta opcja jest wybrana domyślnie.

7. Jeśli to konieczne, skonfiguruj aktualizacje modułów aplikacji dla trybu mobilnego. *Tryb mobilny* to tryb działania Kaspersky Endpoint Security, gdy komputer opuści sieć obwodową organizacji (*komputer offline*).

8. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console skonfigurować aktualizacje modułu aplikacji?

1. W oknie głównym Web Console wybierz **Zadania**.

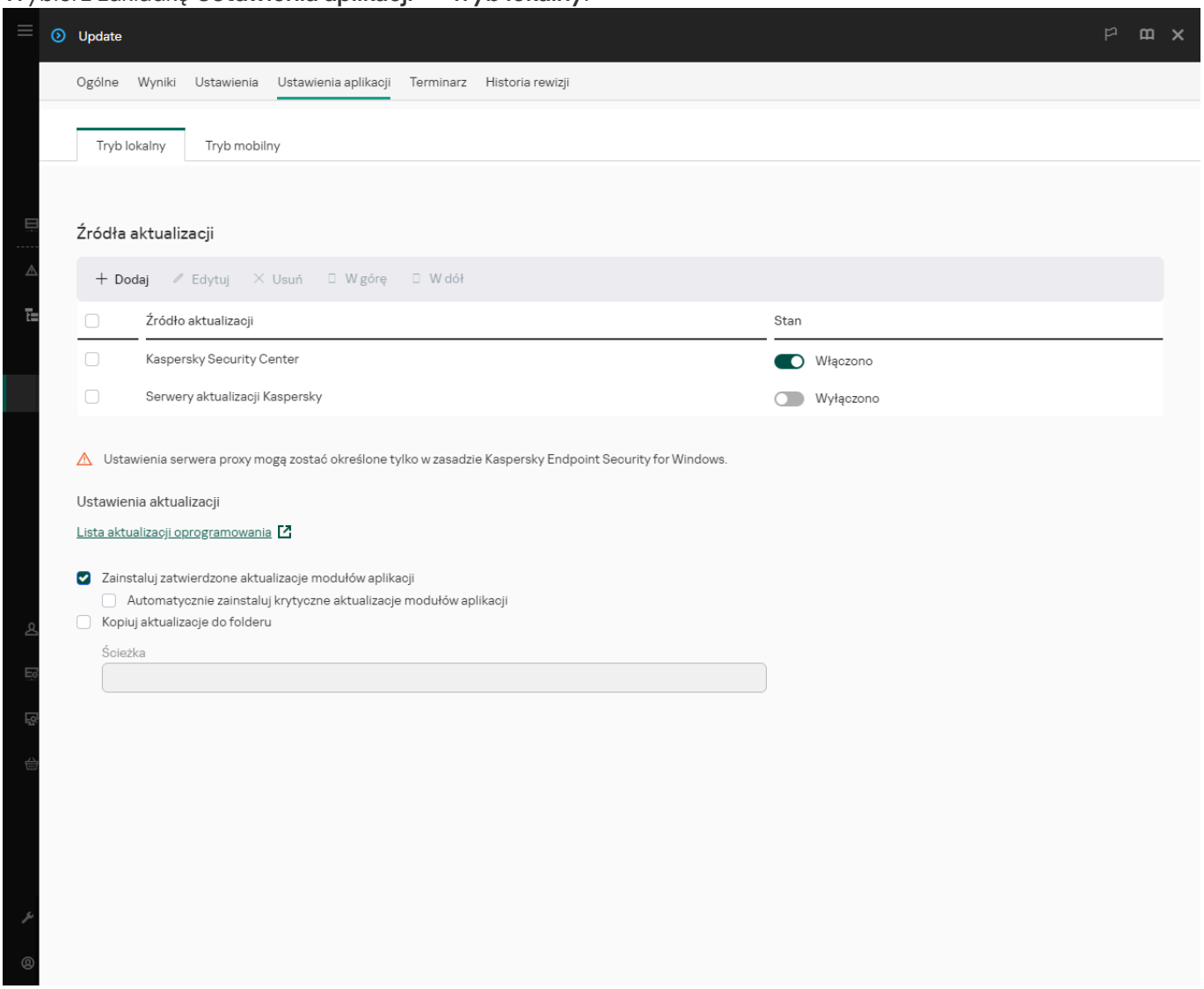
   Zostanie otwarta lista zadań.

2. Kliknij zadanie **Aktualizacja baz danych i modułów aplikacji** Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości zadania.

Zadanie *Aktualizacja baz danych i modułów aplikacji* jest tworzone automatycznie przez kreatora wstępnej konfiguracji Serwera administracyjnego. Aby utworzyć zadanie *Aktualizacja baz danych i modułów aplikacji*, zainstaluj Wtyczkę zarządzającą Kaspersky Endpoint Security for Windows podczas działania kreatora.

3. Wybierz zakładkę **Ustawienia aplikacji** → **Tryb lokalny**.



Ustawienia zadania Aktualizacja

4. W obszarze **Ustawienia aktualizacji**, wybierz opcję aktualizacji modułów aplikacji, które chcesz zainstalować:

   - **Zainstaluj zatwierdzone aktualizacje modułów aplikacji**. Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security instaluje je po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center. Ta opcja jest wybrana domyślnie.

   - **Automatycznie zainstaluj krytyczne aktualizacje modułów aplikacji**. Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security automatycznie instaluje krytyczne uaktualnienia, a także wszystkie inne uaktualnienia modułów aplikacji po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center.

Jeśli chcesz uniemożliwić pobieranie aktualizacji modułów aplikacji, usuń zaznaczenie pola wyboru **Zainstaluj zatwierdzone aktualizacje modułów aplikacji** i **Automatycznie zainstaluj krytyczne aktualizacje modułów aplikacji** i wprowadź zakaz korzystania z lokalnych zadań przez użytkownika.

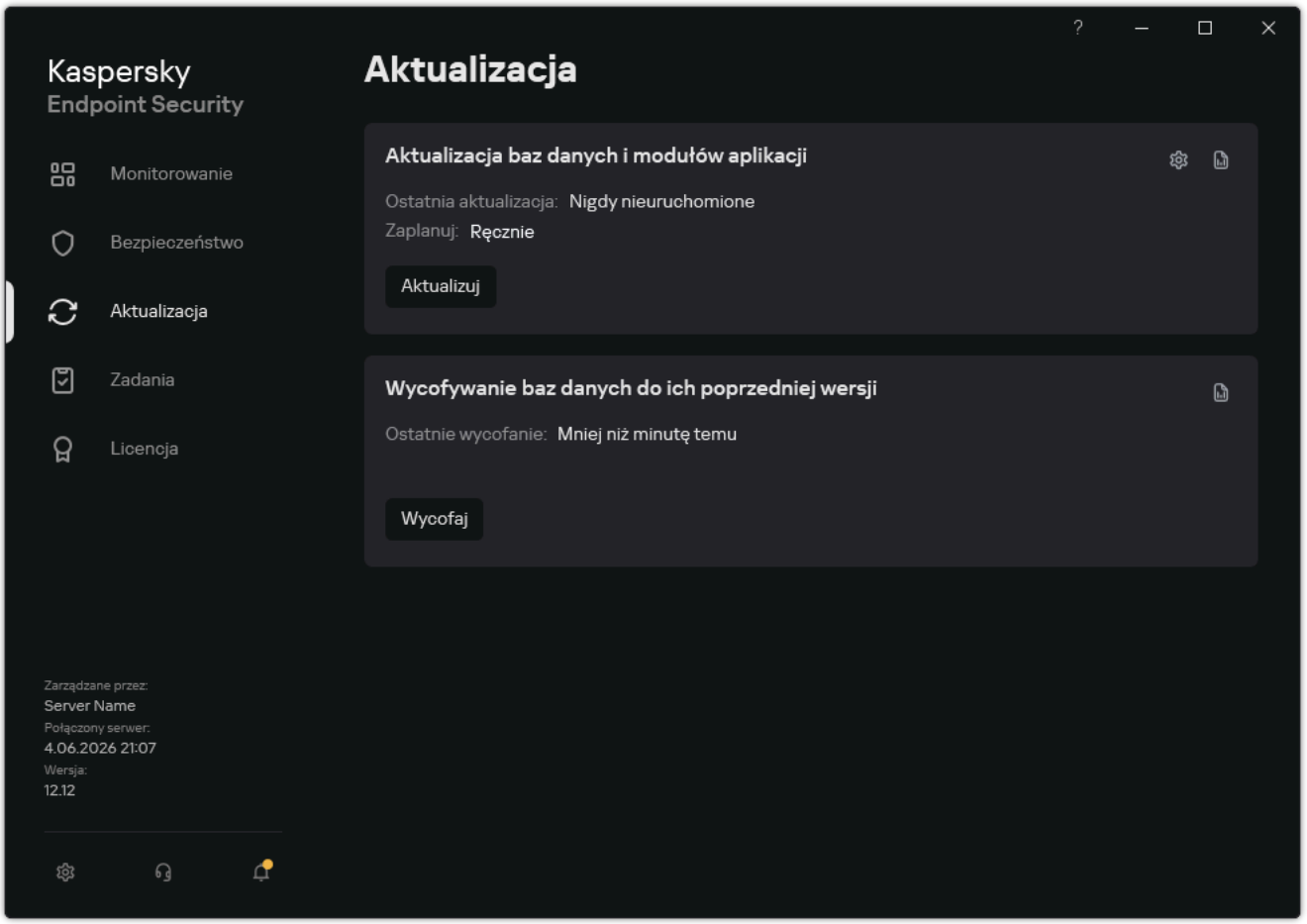
5. Jeśli to konieczne, skonfiguruj aktualizacje modułów aplikacji dla trybu mobilnego. *Tryb mobilny* to tryb działania Kaspersky Endpoint Security, gdy komputer opuści sieć obwodową organizacji (*komputer offline*).

6. Zapisz swoje zmiany.

Jak w interfejsie aplikacji skonfigurować aktualizacje modułu aplikacji?

Nie możesz skonfigurować zadania grupowego *Aktualizacja baz danych i modułów aplikacji* w interfejsie aplikacji. Tylko lokalne zadanie aktualizacji, *Aktualizacja baz danych i modułów aplikacji*, jest dostępne dla użytkownika. Jeśli zadanie *Aktualizacja baz danych i modułów aplikacji* nie jest wyświetlane, oznacza to, że administrator zabronił używania zadań lokalnych w zasadzie.

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.



Lokalne zadania aktualizacji

2. To spowoduje otwarcie listy zadań; wybierz zadanie *Aktualizacja baz danych i modułów aplikacji* i kliknij ⚙.

   Zostanie otwarte okno właściwości zadania.

3. W sekcji **Pobieranie i instalowanie aktualizacji modułów aplikacji** zaznacz pole **Pobierz aktualizacje składników aplikacji**.

4. Wybierz aktualizacje modułów aplikacji, które chcesz zainstalować.

   - **Instaluj krytyczne i zatwierdzone aktualizacje**. Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security automatycznie instaluje krytyczne uaktualnienia, a także wszystkie inne uaktualnienia modułów aplikacji po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center.

   - **Instaluj tylko zatwierdzone aktualizacje**. Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security instaluje je po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center. Ta opcja jest wybrana domyślnie.

5. Zapisz swoje zmiany.

Używanie serwera proxy do aktualizacji

Konieczne może być określenie ustawień serwera proxy do pobrania aktualizacji baz danych i modułów aplikacji ze źródła uaktualnień. Jeśli istnieje kilka źródeł uaktualnień, ustawienia serwera proxy są stosowane do wszystkich źródeł. Jeśli serwer proxy nie jest potrzebny dla niektórych źródeł uaktualnień, możesz wyłączyć korzystanie z serwera proxy we właściwościach profilu. Kaspersky Endpoint Security będzie również korzystał z serwera proxy w celu uzyskania dostępu do sieci Kaspersky Security Network i serwerów aktywacji.

W celu skonfigurowania połączenia ze źródłami uaktualnień poprzez serwer proxy:

1. W oknie głównym Web Console kliknij ⚙.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Przejdź do sekcji **Konfiguracja dostępu do internetu**.

3. Zaznacz pole **Użyj serwera proxy**.

4. Skonfiguruj ustawienia połączenia z serwerem proxy: adres serwera proxy, port i ustawienia uwierzytelniania (nazwa użytkownika i hasło).

5. Zapisz swoje zmiany.

W celu wyłączenia korzystania z serwera proxy dla określonej grupy administracyjnej:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.

5. W sekcji **Serwer proxy** kliknij przycisk **Ustawienia**.

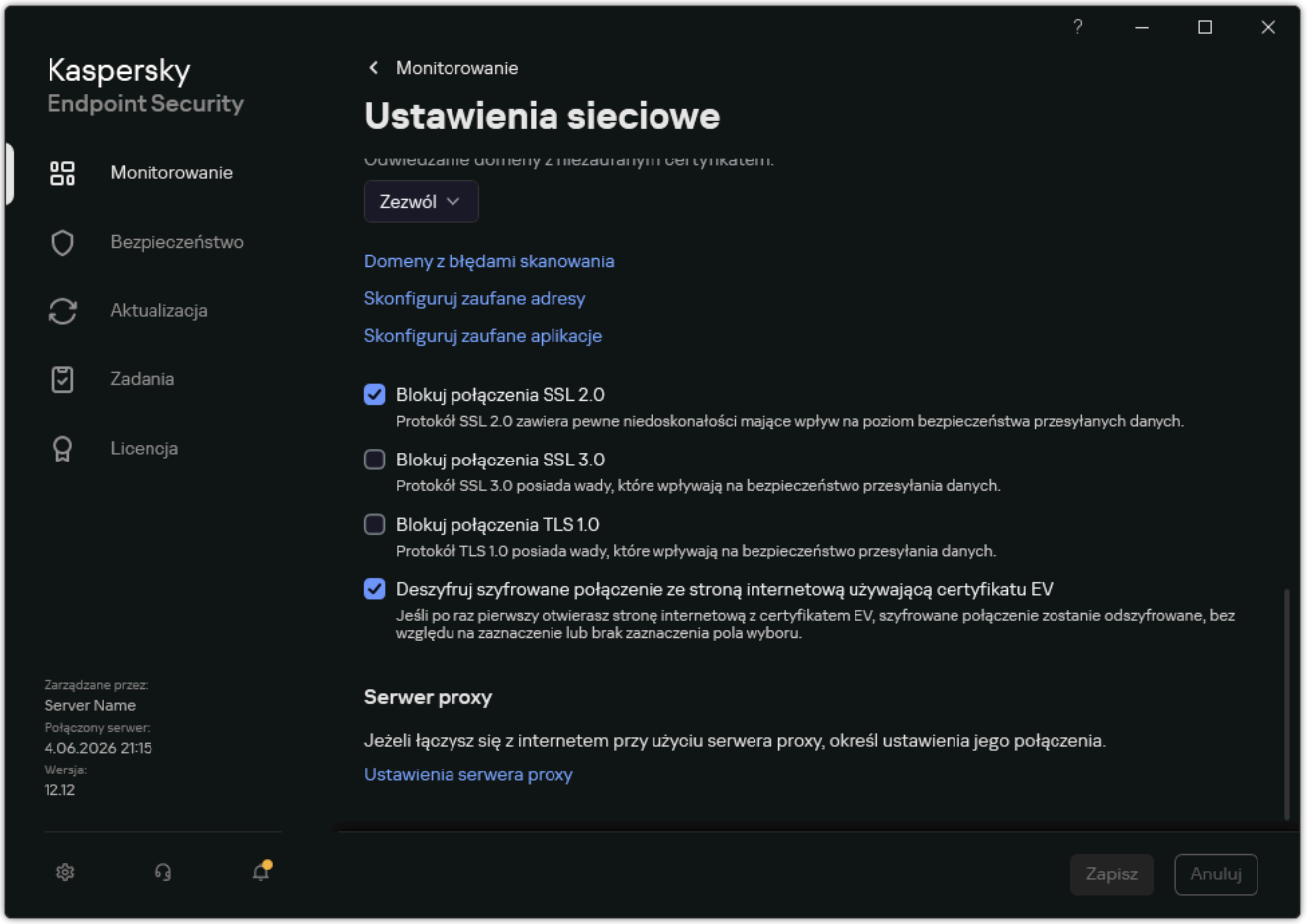
6. W otwartym oknie zaznacz pole **Nie wykorzystuj serwera proxy dla adresów lokalnych**.

7. Zapisz swoje zmiany.

W celu skonfigurowania ustawień serwera proxy w interfejsie aplikacji:

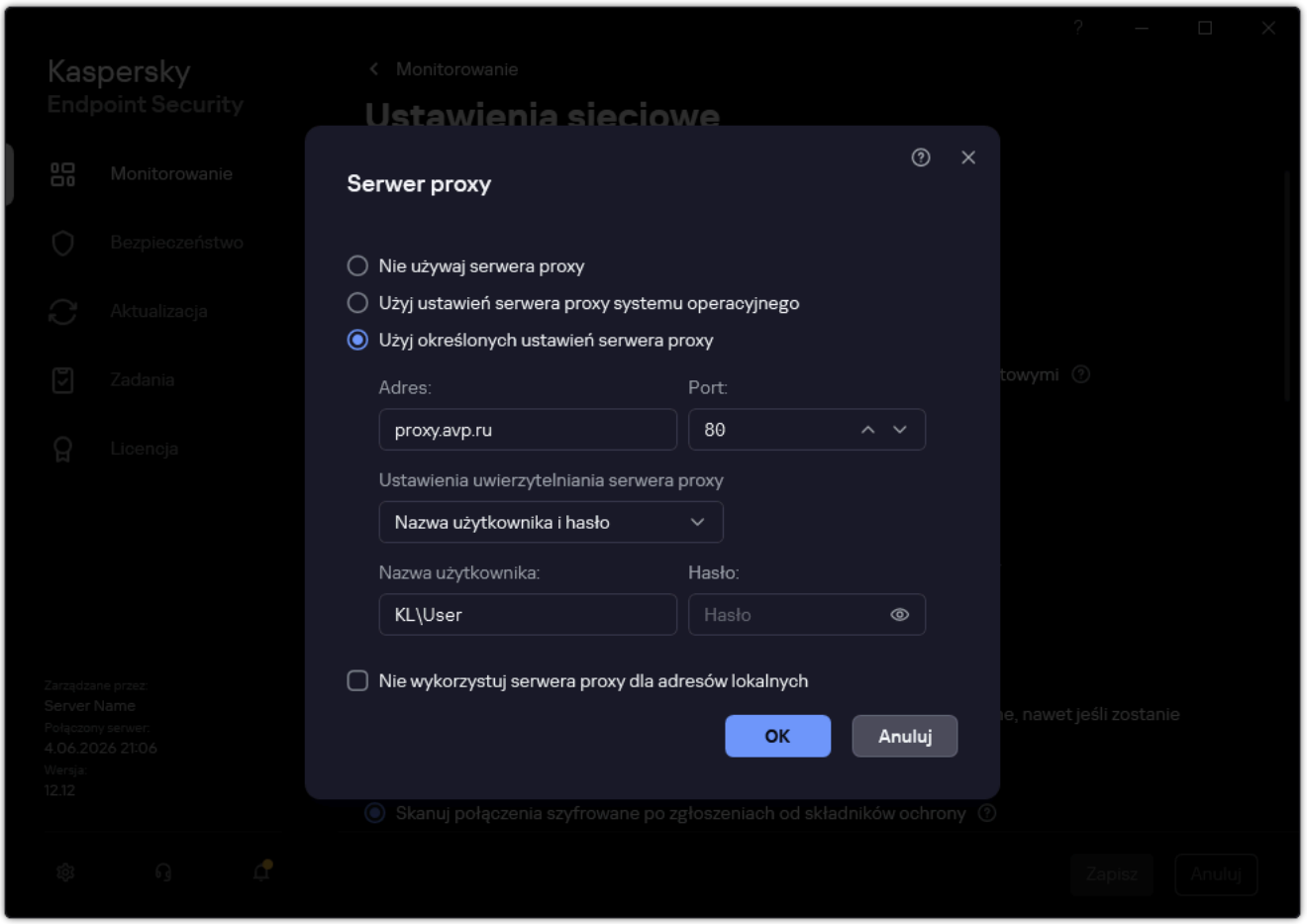
1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.



Ustawienia sieciowe aplikacji

3. W sekcji **Serwer proxy** kliknij odnośnik **Ustawienia serwera proxy**.



Ustawienia połączenia z serwerem proxy

4. W otwartym oknie, w celu określenia adresu serwera proxy wybierz jedną z następujących opcji:

   - **Użyj ustawień serwera proxy systemu operacyjnego**.

     Ta opcja jest wybrana domyślnie. Kaspersky Endpoint Security używa ustawień serwera proxy, które są zdefiniowane w ustawieniach systemu operacyjnego.

   - **Użyj określonych ustawień serwera proxy**.

     Jeśli wybrałeś tę opcję, skonfiguruj ustawienia połączenia z serwerem proxy: port i adres serwera proxy.

5. Wybierz sposób uwierzytelniania aplikacji na serwerze proxy. Domyślnie aplikacja używa uwierzytelniania NTLM domeny bieżącego użytkownika.

6. Jeśli chcesz wyłączyć korzystanie z serwera proxy podczas aktualizacji baz danych i modułów aplikacji z folderu współdzielonego, zaznacz pole **Nie wykorzystuj serwera proxy dla adresów lokalnych**.

7. Zapisz swoje zmiany.

W rezultacie Kaspersky Endpoint Security użyje serwera proxy do pobrania aktualizacji baz danych i modułów aplikacji. Kaspersky Endpoint Security będzie również korzystał z serwera proxy w celu uzyskania dostępu do serwerów KSN i serwerów aktywacji Kaspersky. Jeśli na serwerze proxy wymagana jest autoryzacja, ale dane uwierzytelniające konta użytkownika nie zostały wprowadzone poprawnie, Kaspersky Endpoint Security wyświetli monit o podanie nazwy użytkownika i hasła.

Wycofanie ostatniej aktualizacji

Opcja cofnięcia do poprzedniej wersji baz danych i modułów staje się dostępna po pierwszej aktualizacji baz danych i modułów aplikacji.

Przy każdym uruchomieniu procesu aktualizacji program Kaspersky Endpoint Security tworzy kopię zapasową bieżących baz danych i modułów aplikacji. Umożliwi to w razie czego cofnięcie baz danych i modułów aplikacji do ich poprzedniej wersji. Funkcja cofania ostatniej aktualizacji jest przydatna w sytuacji, gdy, na przykład, nowa wersja bazy danych powoduje fałszywy alarm, co skutkuje tym, że Kaspersky Endpoint Security blokuje bezpieczną aplikację.

Kaspersky Endpoint Security w trybie Light Agent nie obsługuje zadania *Wycofywanie aktualizacji*.

Jak w Konsoli administracyjnej (MMC) wycofać ostatnią aktualizację

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

1. Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Wycofywanie aktualizacji**.

Krok 2. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 3. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz zadania, na przykład ręcznie.

Krok 4. Definiowanie nazwy zadania

Wprowadź nazwę zadania.

Krok 7. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Jak wycofać ostatnią aktualizację w Web Console

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Wycofywanie aktualizacji**.

   c. W polu **Nazwa zadania** wprowadź krótki opis, na przykład, *Wycofywanie aktualizacji*.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.

5. Wybierz konto do uruchomienia zadania. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika.

6. Zakończ działanie Kreatora.

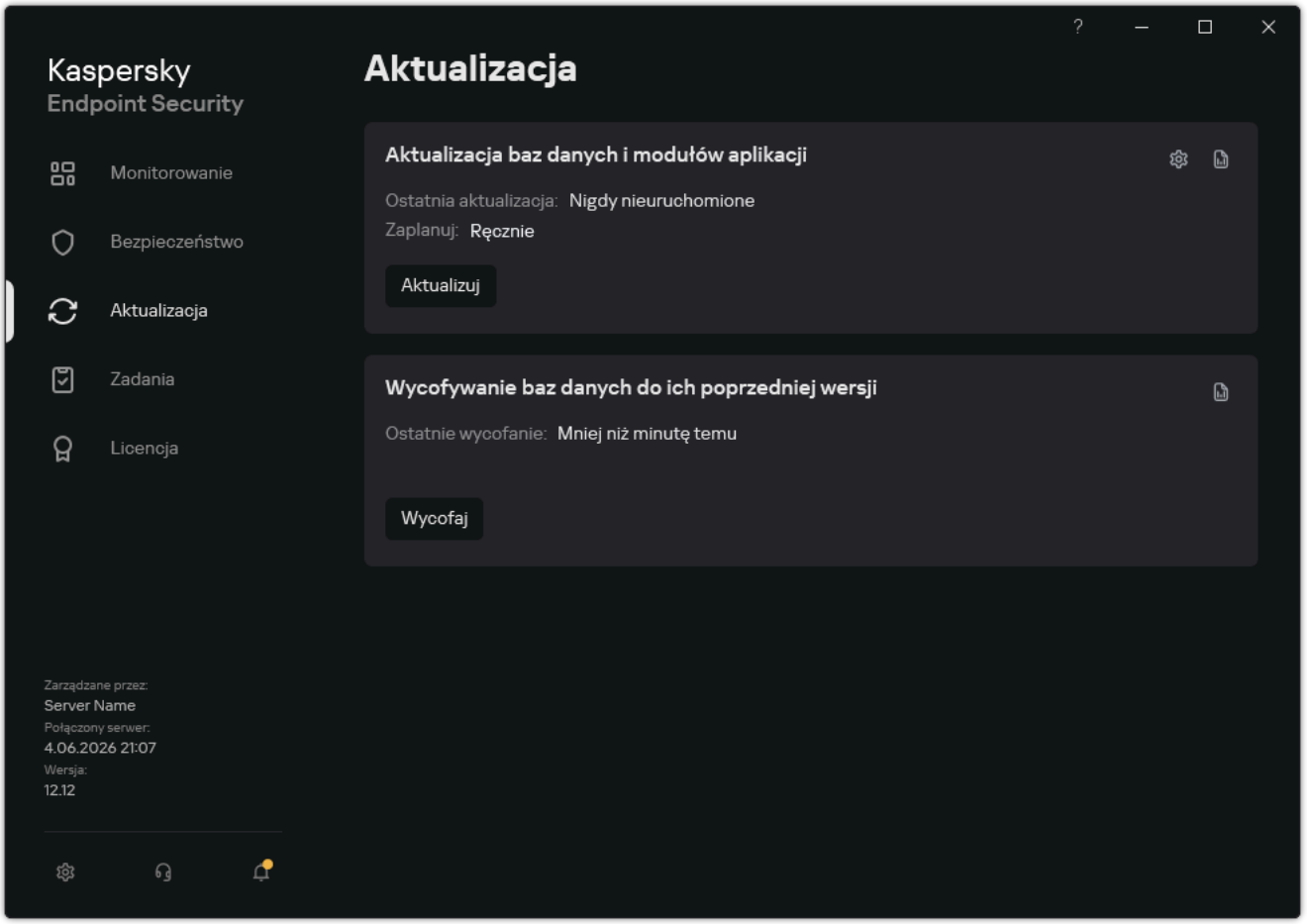
7. Nowe zadanie zostanie wyświetlone na liście zadań.

8. Zaznacz pole obok zadania.

9. Kliknij **Uruchom**.

Jak wycofać ostatnią aktualizację w interfejsie aplikacji

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.



Lokalne zadania aktualizacji

2. W sekcji **Wycofywanie baz danych do ich poprzedniej wersji** kliknij przycisk **Wycofaj**.

Kaspersky Endpoint Security rozpocznie wycofywanie ostatniej aktualizacji baz danych. Aplikacja wyświetli postęp wycofywania, rozmiar pobranych plików i źródło uaktualnień. Kliknij przycisk **Zatrzymaj aktualizację**, aby zatrzymać zadanie w dowolnym momencie.

Używanie technologii zaawansowanego leczenia

Aby pracować z aktywnymi zagrożeniami, Kaspersky Endpoint Security użyje technologii zaawansowanego leczenia. Zaawansowane leczenie działa inaczej dla stacji roboczych i serwerów. Możesz skonfigurować zaawansowane leczenie w ustawieniach zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania* i w ustawieniach aplikacji.

Jeśli program Kaspersky Endpoint Security nie może zatrzymać wykonania fragmentu szkodliwego oprogramowania, możesz użyć technologii zaawansowanego leczenia. W przypadku komputerów objętych polityką Zaawansowane leczenie jest domyślnie wyłączone, ponieważ ta technologia używa znaczącej ilości zasobów komputera. W przypadku komputerów nieobjętych tą polityką Zaawansowane leczenie jest domyślnie włączone.

Zaawansowane leczenie działa inaczej dla stacji roboczych i serwerów. Aby użyć technologii na serwerach, musisz włączyć natychmiastowe Zaawansowane leczenie we właściwościach zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*. To wymaganie wstępne nie jest konieczne do używania technologii na stacjach roboczych.

Jak włączyć lub wyłączyć technologię zaawansowanego leczenia w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.
4. W sekcji **Ogólne** zaznacz lub odznacz pole **Włącz technologię zaawansowanego leczenia**, aby włączyć lub wyłączyć technologię zaawansowanego leczenia.
5. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć technologię zaawansowanego leczenia w Web Console i Cloud Console?

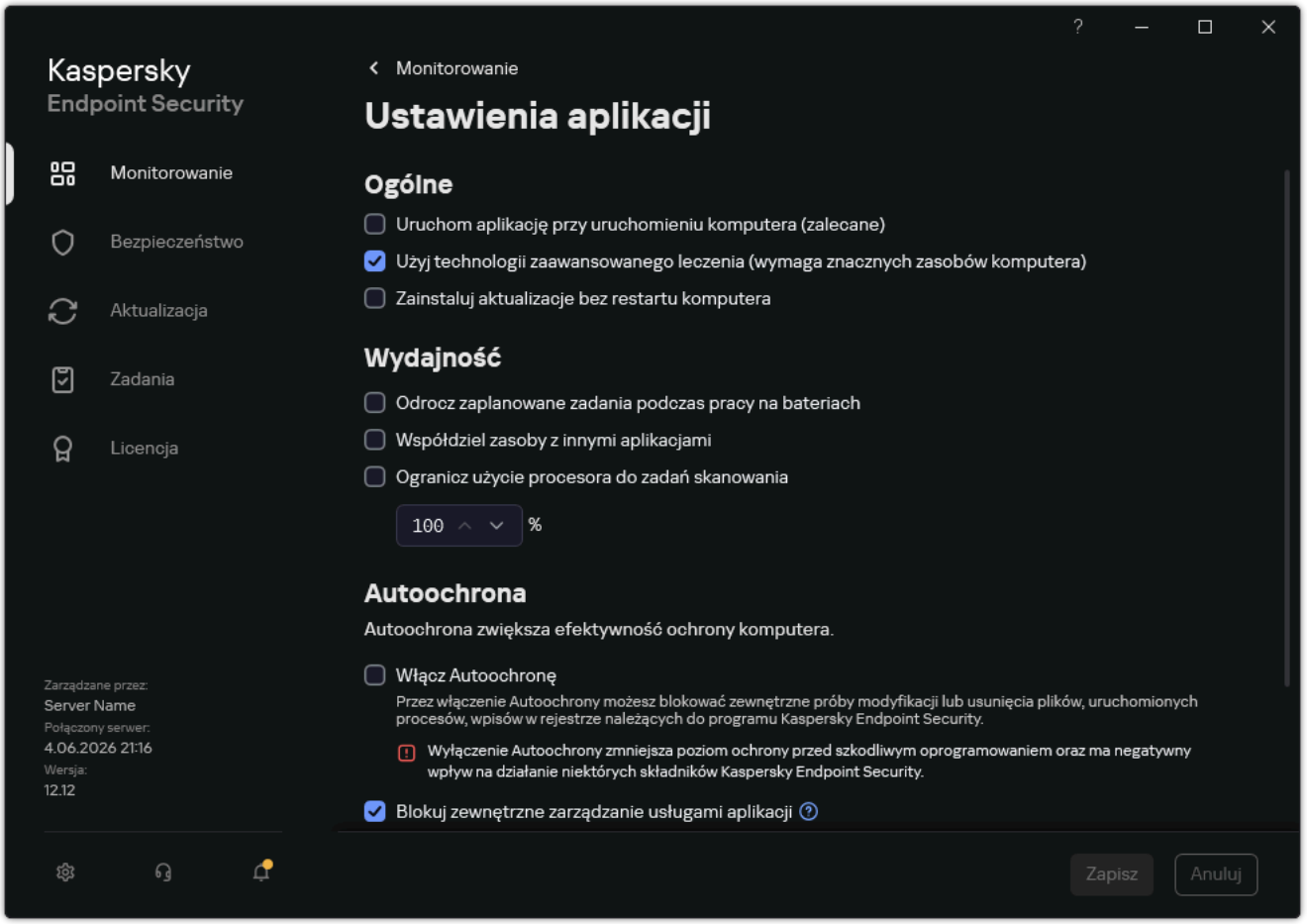
1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Ustawienia wykrywania**.
5. W sekcji **Technologia zaawansowanego leczenia** włącz lub wyłącz przełącznik **Technologia zaawansowanego leczenia WŁĄCZONA**, aby włączyć lub wyłączyć technologię Zaawansowane leczenie.
6. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć technologię zaawansowanego leczenia w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.



Ustawienia Kaspersky Endpoint Security for Windows

3. W sekcji **Ogólne** zaznacz lub odznacz pole **Użyj technologii zaawansowanego leczenia (wymaga znacznych zasobów komputera)**, aby włączyć lub wyłączyć technologię zaawansowanego leczenia.

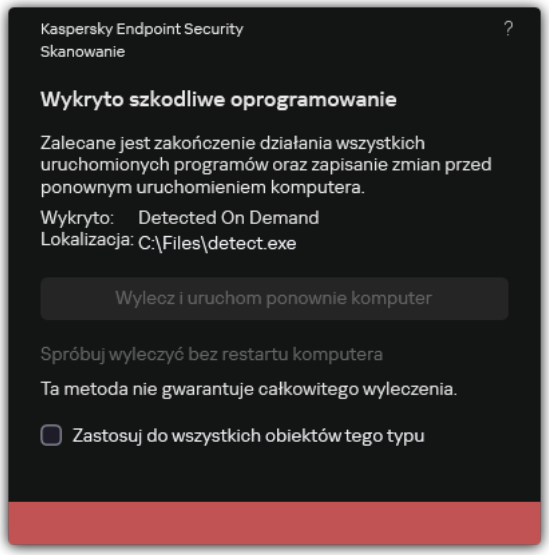
4. Zapisz swoje zmiany.

W trakcie przeprowadzania zaawansowanego leczenia użytkownik nie może korzystać z większości funkcji systemu operacyjnego. Po zakończeniu leczenia, komputer zostanie uruchomiony ponownie.

Leczenie aktywnych zagrożeń na stacjach roboczych

Aby pracować z aktywnymi zagrożeniami na stacjach roboczych, włącz technologię zaawansowanego leczenia w ustawieniach aplikacji. Następnie skonfiguruj doświadczenie użytkownika we właściwościach zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*. We właściwościach zadania dostępne jest pole **Uruchom natychmiast Zaawansowane leczenie**. Jeśli flaga jest ustawiona, Kaspersky Endpoint Security przeprowadzi leczenie bez informowania użytkownika. Po zakończeniu leczenia, komputer zostanie uruchomiony ponownie. Jeśli flaga nie jest ustawiona, Kaspersky Endpoint Security wyświetli komunikat o aktywnych zagrożeniach (patrz rysunek poniżej). Nie możesz zamknąć tego komunikatu bez przetworzenia pliku.

Zaawansowane leczenie podczas wykonywania zadania skanowania antywirusowego na komputerze jest wykonywane tylko wtedy, gdy funkcja Zaawansowane leczenie jest włączona we właściwościach zasady zastosowanej do tego komputera.



Powiadomienie dotyczące aktywnego zagrożenia

Leczenie aktywnych zagrożeń na serwerach

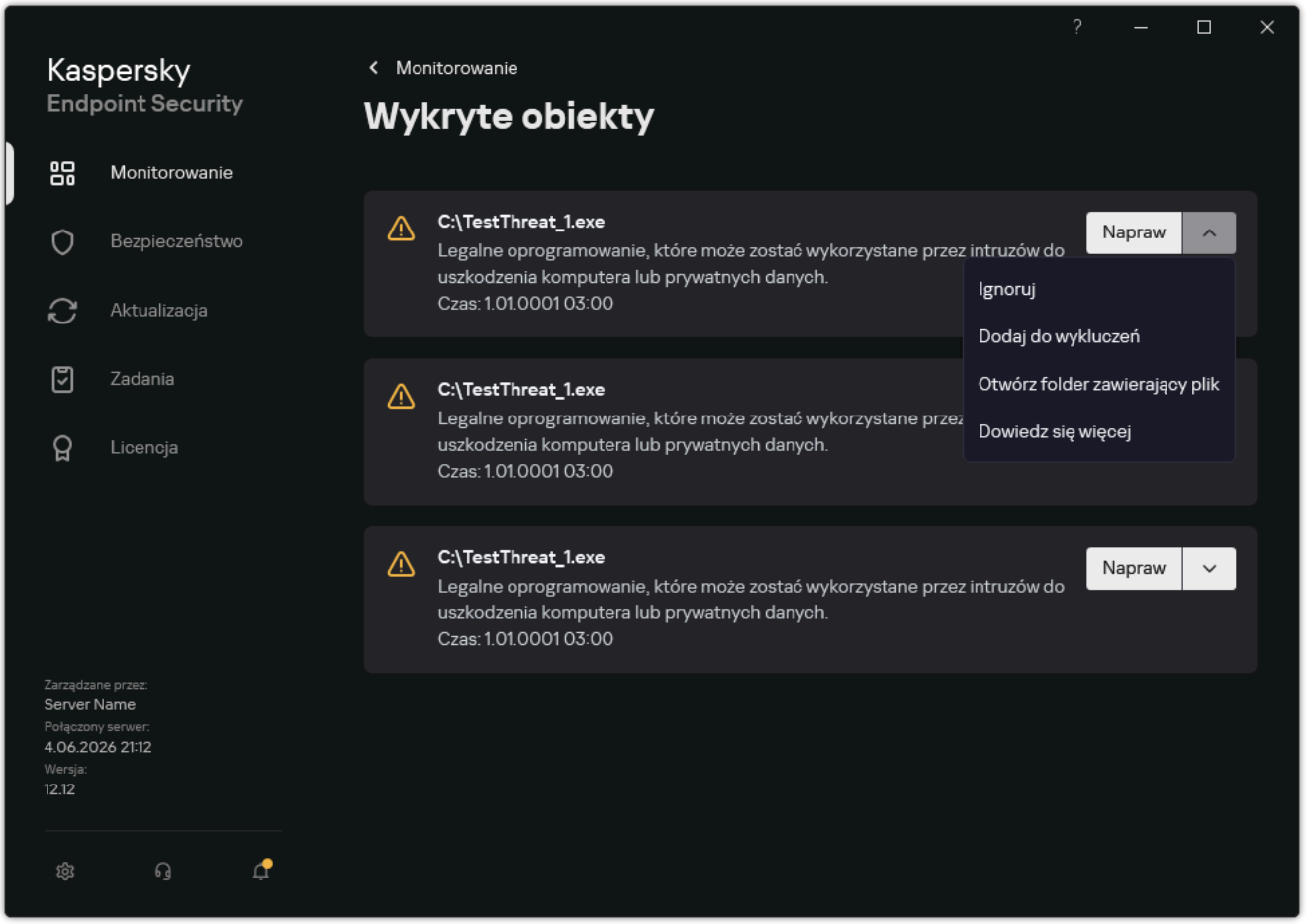
W celu pracy z aktywnymi zagrożeniami na serwerach musisz:

- włączyć technologię zaawansowanego leczenia w ustawieniach aplikacji;
- włączyć natychmiastowe zaawansowane leczenie we właściwościach zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows przeznaczonego dla serwerów, Kaspersky Endpoint Security nie wyświetli komunikatu. Dlatego nie możesz wybrać działania wyleczenia aktywnego zagrożenia. Aby wyleczyć zagrożenie, musisz włączyć technologię zaawansowanego leczenia w ustawieniach aplikacji oraz natychmiast włączyć Zaawansowane leczenie w ustawieniach zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Następnie musisz uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

Eliminowanie nieprzetworzonych zagrożeń

Kaspersky Endpoint Security zapisuje informacje o plikach, które z jakiegoś powodu nie zostały przetworzone. Informacje te są zapisywane w postaci zdarzeń na liście aktywnych zagrożeń (patrz rysunek poniżej).



Lista aktywnych zagrożeń

Zainfekowany plik zostaje uznany za *przetworzony*, jeśli Kaspersky Endpoint Security wyleczył plik lub usunął zagrożenie jako część skanowania komputera pod kątem wirusów i innych szkodliwych programów.

Kaspersky Endpoint Security przenosi plik na listę aktywnych zagrożeń, jeśli podczas skanowania komputera w poszukiwaniu wirusów i innych zagrożeń z jakiegoś powodu nie powiodło się wykonanie akcji na tym pliku, zgodnej z określonymi ustawieniami aplikacji.

Taka sytuacja może zajść w następujących przypadkach:

- Skanowany plik jest niedostępny (na przykład, znajduje się na dysku sieciowym lub wymiennym, do którego nie ma uprawnień zapisu).
- W ustawieniach zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania* działanie po wykryciu zagrożenia jest ustawione na **Poinformuj**. Następnie, gdy powiadomienie o zainfekowanym pliku zostało wyświetlone na ekranie, użytkownik wybrał **Ignoruj**.

Jeśli istnieją jakiekolwiek nieprzetworzone zagrożenia, Kaspersky Endpoint Security zmieni ikonę na . W oknie głównym aplikacji wyświetlane jest powiadomienie o zagrożeniu (patrz rysunek poniżej). W konsoli Kaspersky Security Center stan komputera zostanie zmieniony na *Krytyczny* – .

Jak przetworzyć zagrożenie w Konsoli administracyjnej (MMC)?

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Zaawansowane** → **Repozytoria** → **Aktywne zagrożenia**.

   Zostanie otwarta lista aktywnych zagrożeń.

2. Wybierz obiekt, który chcesz przetworzyć.

3. Wybierz sposób zarządzania zagrożeniem:

   - **Wylecz**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik.

   - **Usuń**. Jeżeli ta opcja jest zaznaczona, aplikacja usunie zainfekowany plik wykryty w aktywnym repozytorium zagrożeń. W tym przypadku aplikacja zachowuje wykryty plik w pamięci komputera. Aby wyeliminować zagrożenie z komputera, wybierz **Wylecz**.

Jak przetworzyć zagrożenie w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Operacje** → **Repozytoria** → **Aktywne zagrożenia**.

   Zostanie otwarta lista aktywnych zagrożeń.

2. Wybierz obiekt, który chcesz przetworzyć.

3. Wybierz sposób zarządzania zagrożeniem:

   - **Wylecz**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik.

   - **Usuń**. Jeżeli ta opcja jest zaznaczona, aplikacja usunie zainfekowany plik wykryty w aktywnym repozytorium zagrożeń. W tym przypadku aplikacja zachowuje wykryty plik w pamięci komputera. Aby wyeliminować zagrożenie z komputera, wybierz **Wylecz**.

Jak przetworzyć zagrożenie w interfejsie aplikacji?

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Istnieje ryzyko infekcji komputera**.

   Zostanie otwarta lista aktywnych zagrożeń.

2. Wybierz obiekt, który chcesz przetworzyć.

3. Wybierz sposób zarządzania zagrożeniem:

   - **Napraw**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik.

   - **Dodaj do wykluczeń**. Jeśli to działanie zostało wybrane, Kaspersky Endpoint Security sugeruje dodanie pliku do listy wykluczeń ze skanowania. Ustawienia wykluczenia są konfigurowane automatycznie. Jeśli dodanie wykluczenia nie jest dostępne, oznacza to, że administrator wyłączył dodawanie wykluczeń w ustawieniach zasady.

   - **Ignoruj**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security usunie wpis z listy aktywnych zagrożeń. Jeśli na liście nie ma aktywnych zagrożeń, stan komputera zostanie zmieniony na *OK*. Jeśli obiekt zostanie usunięty ponownie, Kaspersky Endpoint Security doda nowy wpis do listy aktywnych zagrożeń.

- **Otwórz folder zawierający plik**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security otworzy folder zawierający obiekt w menedżerze plików. Możesz ręcznie usunąć obiekt lub przenieś obiekt do folderu, który nie znajduje się w obszarze ochrony.

- **Dowiedz się więcej**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security otwiera stronę internetową bazy danych luk w zabezpieczeniach i zagrożeń Kaspersky.

Aby przetwarzać aktywne zagrożenia w konsoli Kaspersky Security Center, należy włączyć przesyłanie informacji o nieprzetworzonych plikach do Serwera administracyjnego. Przesyłanie danych jest domyślnie włączone.

Jak włączyć przesyłanie danych nieprzetworzonych plików w Konsoli administracyjnej (MMC)?

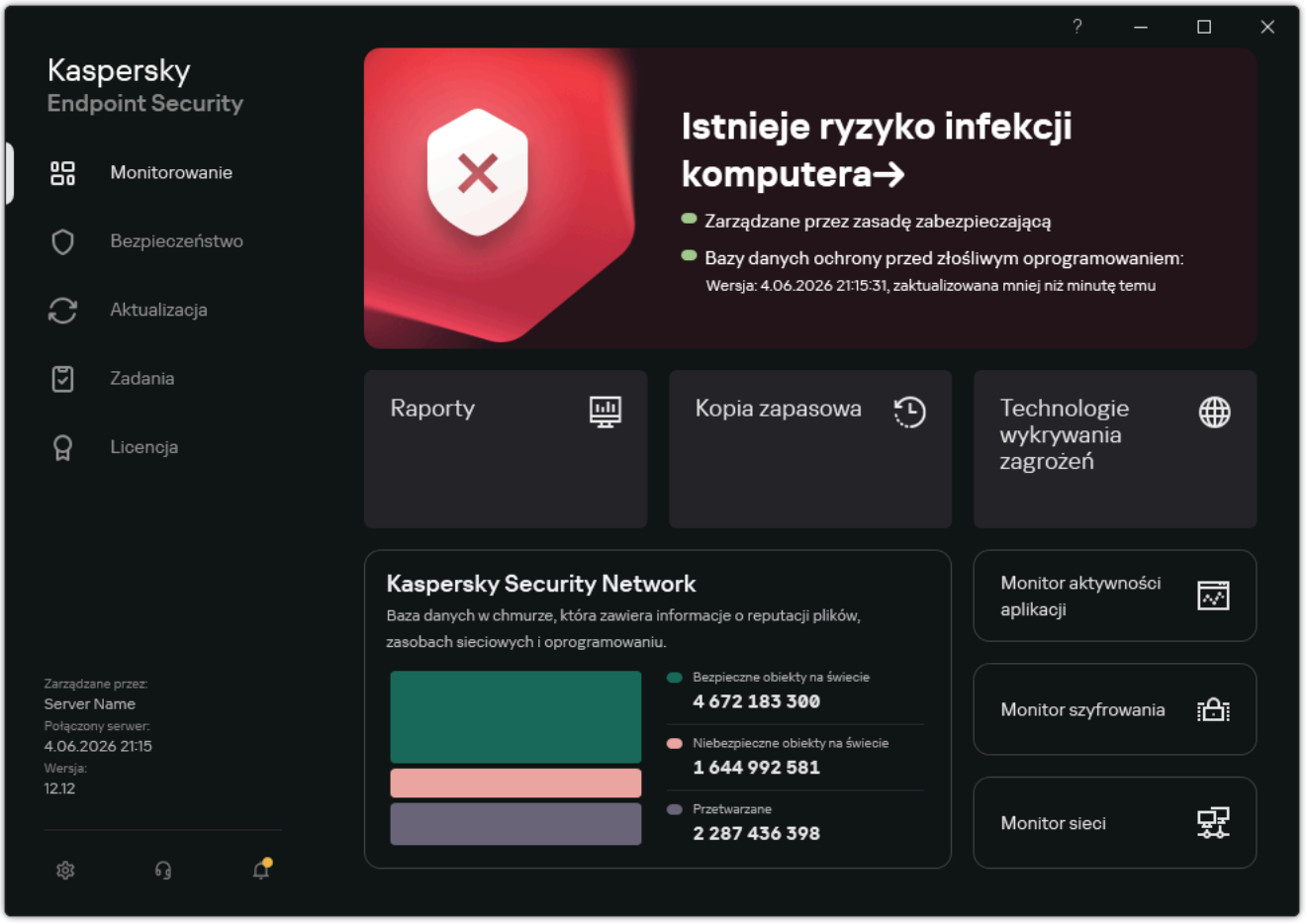
1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Raporty i Kopia zapasowa**.
4. W sekcji **Przesyłanie danych do Serwera administracyjnego** kliknij przycisk **Ustawienia**.
5. Zaznacz pole **Nieprzetworzone pliki**.
6. Zapisz swoje zmiany.

Jak włączyć przesyłanie danych nieprzetworzonych plików w Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Integracja KSC**.

5. W sekcji **Przesyłanie danych do Serwera administracyjnego** zaznacz pole **O nieprzetworzonych plikach**.

6. Zapisz swoje zmiany.



Okno główne aplikacji po wykryciu zagrożenia

Ochrona komputera

Ochrona plików

Komponent Ochrona plików pozwala zapobiegać infekcjom systemu plików komputera. Domyślnie komponent Ochrona plików znajduje się na stałe w pamięci RAM komputera i na bieżąco skanuje wszystkie otwierane, zapisywane i uruchamiane pliki. Ten komponent skanuje pliki na wszystkich dyskach komputera, także na dyskach podłączonych. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej.

Komponent skanuje pliki otwierane przez użytkownika lub aplikację. Jeśli zostanie wykryty szkodliwy plik, Kaspersky Endpoint Security blokuje operację na pliku. Następnie aplikacja leczy lub usuwa szkodliwy plik, w zależności od ustawień komponentu Ochrona plików.

Podczas próby uzyskania dostępu do pliku, którego zawartość znajduje się w chmurze OneDrive, Kaspersky Endpoint Security pobierze i przeskanuje zawartość pliku.

Włączanie i wyłączanie modułu Ochrona plików

Domyślnie moduł Ochrona plików jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. Dla modułu Ochrona plików program Kaspersky Endpoint Security można zastosować różne grupy ustawień. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane *poziomami ochrony*: **Wysoki**, **Zalecany**, **Niski**. Ustawienia poziomu ochrony **Zalecany** są uważane za optymalne ustawienia zalecane przez ekspertów z Kaspersky (patrz tabela poniżej). Możesz wybrać jeden z predefiniowanych poziomów ochrony lub ręcznie skonfigurować ustawienia poziomu ochrony. Jeśli zmieniłeś ustawienia poziomu ochrony, możesz zawsze powrócić do zalecanych ustawień poziomu ochrony.

Komponent Ochrona plików wykorzystuje dane otrzymane od innych komponentów aplikacji. Włączenie tych komponentów jest opcjonalne. Komponenty, które udostępniają dodatkowe dane, zawierają:

- Kaspersky Security Network.
- Ochrona przed włamaniami.
- Wykrywanie zachowań.

Jak włączyć lub wyłączyć komponent Ochrona plików w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
4. Użyj pola **Ochrona plików**, aby włączyć lub wyłączyć komponent.

5. Jeśli włączyłeś komponent, w sekcji **Poziom ochrony** wykonaj jedną z następujących czynności:

   - Jeśli chcesz zastosować jeden z predefiniowanych poziomów ochrony, wybierz go, korzystając z suwaka:

     - **Wysoki**. Jeśli wybrano ten poziom ochrony plików, moduł Ochrona plików będzie dokładnie kontrolować wszystkie otwierane, zapisywane i uruchamiane pliki. Komponent Ochrona plików skanuje wszystkie typy plików na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera. Moduł ten skanuje także archiwa, pakiety instalacyjne i osadzone obiekty OLE.

     - **Zalecany**. Ten poziomy ochrony plików jest zalecany przez specjalistów z Kaspersky Lab. Komponent Ochrona plików skanuje wszystkie formaty plików na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera, a także osadzonych obiektów OLE. Moduł Ochrona plików nie skanuje archiwów oraz pakietów instalacyjnych.

     - **Niski**. Ustawienia tego poziomu ochrony plików zapewniają maksymalną prędkość skanowania. Komponent Ochrona plików skanuje tylko pliki z określonymi rozszerzeniami na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera. Moduł Ochrona plików nie skanuje plików złożonych.

   - Jeśli chcesz skonfigurować niestandardowy poziom ochrony, kliknij przycisk **Ustawienia** i zdefiniuj własne ustawienia komponentu.

     Możesz przywrócić wartości predefiniowanych poziomów ochrony, klikając przycisk **Domyślny** w sekcji Domyślny.

6. W sekcji **Działanie po wykryciu zagrożenia** wybierz akcję, wykonywaną przez Kaspersky Endpoint Security po wykryciu szkodliwych obiektów:

   - **Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik.

   - **Wylecz; blokuj, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja zablokuje ten plik.

   - **Blokuj**. Jeśli wybrano tę opcję, aplikacja automatycznie zablokuje zainfekowany plik, bez podjęcia próby jego wyleczenia lub usunięcia.

   - **Poinformuj**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików.

   > Przed próbą wyleczenia lub usunięcia zainfekowanego pliku, aplikacja utworzy kopię zapasową pliku w przypadku, gdy potrzebujesz przywrócić plik lub jeśli może zostać wyleczony w przyszłości.

7. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć komponent Ochrona plików w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ochrona hosta** → **Ochrona plików**.

5. Użyj przełącznika **Ochrona plików WŁĄCZONA**, aby włączyć lub wyłączyć komponent.

6. Jeśli chcesz dodać nowy obiekt do obszaru ochrony:

   a. W menu **Ustawienia zaawansowane**, Wybierz zakładkę **Obszar ochrony**.

   b. Kliknij **Dodaj**.

   c. Spowoduje to otwarcie okna; w tym oknie wybierz obiekty, które chcesz dodać do obszaru ochrony.

   Użyj masek:

   - Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.

   - Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.

   - Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

   W dowolnym miejscu ścieżki pliku lub folderu można używać masek. Na przykład, jeśli chcesz, aby zakres skanowania obejmował folder Pobrane dla wszystkich kont użytkowników na komputerze, należy wprowadzić maskę `C:\Users\*\Downloads\`.

   Można wykluczyć obiekt z ochrony bez usuwania go z listy obiektów w obszarze ochrony. W tym celu ustaw przycisk przełącznika obok obiektu na pozycję wyłączenia.

   d. Zapisz swoje zmiany.

7. W sekcji **Działanie po wykryciu zagrożenia** wybierz akcję, wykonywaną przez Kaspersky Endpoint Security po wykryciu szkodliwych obiektów:

   - **Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik.

   - **Wylecz; blokuj, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja zablokuje ten plik.

   - **Zablokuj**. Jeśli wybrano tę opcję, aplikacja automatycznie zablokuje zainfekowany plik, bez podjęcia próby jego wyleczenia lub usunięcia.

   Przed próbą wyleczenia lub usunięcia zainfekowanego pliku, aplikacja utworzy kopię zapasową pliku w przypadku, gdy potrzebujesz przywrócić plik lub jeśli może zostać wyleczony w przyszłości.

8. W razie potrzeby edytuj zaawansowane ustawienia Ochrony plików.

9. Zapisz swoje zmiany.

Włączanie lub wyłączanie składnika Ochrony plików w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.

3. Użyj przełącznika **Ochrona plików**, aby włączyć lub wyłączyć komponent.

4. Jeśli włączyłeś komponent, w sekcji **Poziom ochrony** wykonaj jedną z następujących czynności:

   - Jeśli chcesz zastosować jeden z predefiniowanych poziomów ochrony, wybierz go, korzystając z suwaka:

     - **Wysoki**. Jeśli wybrano ten poziom ochrony plików, moduł Ochrona plików będzie dokładnie kontrolować wszystkie otwierane, zapisywane i uruchamiane pliki. Komponent Ochrona plików skanuje wszystkie typy plików na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera. Moduł ten skanuje także archiwa, pakiety instalacyjne i osadzone obiekty OLE.

     - **Zalecany**. Ten poziomy ochrony plików jest zalecany przez specjalistów z Kaspersky Lab. Komponent Ochrona plików skanuje wszystkie formaty plików na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera, a także osadzonych obiektów OLE. Moduł Ochrona plików nie skanuje archiwów oraz pakietów instalacyjnych.

     - **Niski**. Ustawienia tego poziomu ochrony plików zapewniają maksymalną prędkość skanowania. Komponent Ochrona plików skanuje tylko pliki z określonymi rozszerzeniami na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera. Moduł Ochrona plików nie skanuje plików złożonych.

   - Jeśli chcesz skonfigurować niestandardowy poziom ochrony, kliknij przycisk **Ustawienia zaawansowane** i zdefiniuj własne ustawienia składnika.

     Możesz przywrócić wartości predefiniowanych poziomów ochrony, klikając przycisk **Domyślny** w sekcji Przywróć zalecany poziom ochrony.

5. W sekcji **Działanie po wykryciu zagrożenia** wybierz akcję, wykonywaną przez Kaspersky Endpoint Security po wykryciu szkodliwych obiektów:

   - **Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik.

   - **Wylecz; blokuj, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja zablokuje ten plik.

   - **Blokuj**. Jeśli wybrano tę opcję, aplikacja automatycznie zablokuje zainfekowany plik, bez podjęcia próby jego wyleczenia lub usunięcia.

   - **Poinformuj**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików.

Przed próbą wyleczenia lub usunięcia zainfekowanego pliku, aplikacja utworzy kopię zapasową pliku w przypadku, gdy potrzebujesz przywrócić plik lub jeśli może zostać wyleczony w przyszłości.

6. Zapisz swoje zmiany.

Ustawienia Ochrony plików zalecane przez ekspertów z Kaspersky (zalecany poziom ochrony)

Parametr	Wartość	Opis
Typy plików	**Pliki skanowane według formatu**	Jeżeli wybierzesz tę opcję, aplikacja będzie skanować tylko infekowalne pliki. Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików.
Analiza heurystyczna	**Poziom niski**	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa. Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.
Skanuj tylko nowe i zmienione pliki	**Włączono**	Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.
Technologia iSwift	**Włączono**	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.
Użyj technologii iChecker	**Włączono**	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).
Skanuj pliki w formatach Microsoft Office	**Włączono**	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty. Aplikacja skanuje pliki w formacie Office, które są mniejsze niż 1 MB, niezależnie od tego, czy pole wyboru jest zaznaczone, czy nie.
Skanuj pliki formatu poczty elektronicznej	**Włączono**	Skanuje pliki w formacie e-mail. Aplikacja skanuje pliki MSG i EML. Pliki w formacie e-mail zawierają także obiekty OLE oraz pliki MHT. Kaspersky Endpoint Security skanuje pliki w formacie e-mail, które są mniejsze niż 1 MB, niezależnie od tego, czy pole wyboru jest zaznaczone, czy nie.
Tryb skanowania	**Tryb Inteligentny**	W tym trybie Ochrona plików skanuje obiekt w oparciu o analizę akcji podejmowanych na obiekcie. Na przykład, jeżeli wykorzystywany jest dokument Microsoft Office, Kaspersky Endpoint Security skanuje plik przy jego pierwszym otwieraniu i ostatnim zamykaniu. Wszystkie operacje wykonywane w międzyczasie, które nadpisują plik, nie są skanowane.
Działanie po wykryciu zagrożenia	**Wylecz; usuń, jeśli leczenie nie jest możliwe**	Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik.

Automatyczne wstrzymywanie Ochrony plików

Możesz skonfigurować moduł Ochrona plików tak, aby był automatycznie wstrzymywany o określonym czasie lub podczas pracy z określonymi aplikacjami.

Ochrona plików powinna zostać wstrzymana tylko w ostateczności, gdy powoduje konflikty z niektórymi aplikacjami. Jeśli podczas działania komponentu wystąpią jakiekolwiek konflikty, zalecane jest skontaktowanie się z pomocą techniczną Kaspersky. Eksperci z pomocy technicznej mogą w skonfigurowaniu komponentu Ochrona plików tak, aby mógł być uruchamiany jednocześnie z innymi aplikacjami na komputerze.

W celu skonfigurowania automatycznego wstrzymywania Ochrony plików:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij **Ustawienia zaawansowane**.
4. W sekcji **Wstrzymaj moduł Ochrona plików** kliknij odnośnik **Wstrzymaj moduł Ochrona plików**.
5. W otwartym oknie skonfiguruj ustawienia wstrzymania modułu Ochrona plików:
   a. Skonfiguruj terminarz automatycznego wstrzymania działania modułu Ochrona plików.
   b. Utwórz listę aplikacji, których działanie powinno wstrzymać działanie modułu Ochrona plików.
6. Zapisz swoje zmiany.

Zmienianie akcji wykonywanej na zainfekowanych plikach przez moduł Ochrona plików

Domyślnie, Ochrona plików automatycznie próbuje wyleczyć wszystkie zainfekowane pliki, które zostały wykryte. Jeśli leczenie nie powiedzie się, komponent Ochrona plików usuwa te pliki.

W celu zmiany akcji wykonywanej na zainfekowanych plikach przez moduł Ochrona plików:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. W sekcji **Działanie po wykryciu zagrożenia** wybierz żądaną opcję:
   - **Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik.
   - **Wylecz; blokuj, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja zablokuje ten plik.
   - **Blokuj**. Jeśli wybrano tę opcję, aplikacja automatycznie zablokuje zainfekowany plik, bez podjęcia próby jego wyleczenia lub usunięcia.

   Przed próbą wyleczenia lub usunięcia zainfekowanego pliku, aplikacja utworzy kopię zapasową pliku w przypadku, gdy potrzebujesz przywrócić plik lub jeśli może zostać wyleczony w przyszłości.
4. Zapisz swoje zmiany.

Tworzenie obszaru ochrony modułu Ochrona plików

Obszar ochrony oznacza obiekty, które są skanowane przez moduł, gdy jest on włączony. Obszary ochrony różnych modułów mają odmienne właściwości. Lokalizacja i typ skanowanych plików to właściwości obszaru ochrony modułu Ochrona plików. Domyślnie, komponent Ochrona plików skanuje tylko potencjalnie infekowalne pliki, które są uruchamiane z dysków twardych, dysków wymiennych i dysków sieciowych.

Podczas wybierania typu skanowanych plików należy pamiętać, że:

1. Istnieje małe prawdopodobieństwo wprowadzenia złośliwego kodu do plików niektórych formatów i jego późniejszej aktywacji (na przykład, formatu TXT). Istnieją jednak formaty plików zawierające kod wykonywalny (na przykład .exe, .dll). Kod wykonywalny może także znajdować się w plikach formatów, które nie są przeznaczone do tego celu (na przykład, format DOC). Ryzyko przeniknięcia i aktywacji szkodliwego kodu w takich plikach jest wysokie.

2. Cyberprzestępca może przesłać na Twój komputer wirusa lub inną szkodliwą aplikację w pliku wykonywalnym posiadającym rozszerzenie .txt. Jeśli wybierzesz opcję skanowania plików według rozszerzenia, aplikacja pominie ten plik podczas skanowania. Jeśli wybrano skanowanie plików według formatu, Kaspersky Endpoint Security analizuje nagłówek pliku niezależnie od jego rozszerzenia. Jeśli analiza wykryje, że plik posiada format pliku wykonywalnego (na przykład, EXE), aplikacja przeskanuje ten plik.

W celu utworzenia obszaru ochrony:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.

3. Kliknij **Ustawienia zaawansowane**.

4. W sekcji **Typy plików** określ typy plików, które mają być skanowane przez moduł Ochrona plików:

   - **Wszystkie pliki**. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanować wszystkie pliki bez wyjątku (wszystkie formaty i rozszerzenia).

   - **Pliki skanowane według formatu**. Jeżeli wybierzesz tę opcję, aplikacja będzie skanować tylko infekowalne pliki. Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików.

   - **Pliki skanowane według rozszerzenia**. Jeżeli wybierzesz tę opcję, aplikacja będzie skanować tylko infekowalne pliki. Format pliku będzie określany w oparciu o jego rozszerzenie.

5. Kliknij odnośnik **Edytuj obszar ochrony**.

6. W otwartym oknie wybierz obiekty, które chcesz dodać do obszaru ochrony lub wykluczyć z niego.

   Obiekty, które domyślnie znajdują się w obszarze ochrony, nie mogą zostać zmodyfikowane ani usunięte.

7. Jeśli chcesz dodać nowy obiekt do obszaru ochrony:

   a. Kliknij **Dodaj**.

      Zostanie otwarte drzewo folderów.

   b. W polu **Ścieżka** wprowadź ścieżkę do folderu lub pliku.

      Użyj masek:

      - Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.

      - Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.

      - Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

      W dowolnym miejscu ścieżki pliku lub folderu można używać masek. Na przykład, jeśli chcesz, aby zakres skanowania obejmował folder Pobrane dla wszystkich kont użytkowników na komputerze, należy wprowadzić maskę `C:\Users\*\Downloads\`.

      Obiekt **Ten komputer** na liście zasobów plikowych komputera zawiera następujące obiekty: **Wszystkie dyski twarde**, **Wszystkie dyski sieciowe** and **Wszystkie dyski wymienne**.

   Możesz wykluczyć obiekt ze skanowań bez usuwania go z listy obiektów w obszarze skanowania. W tym celu odznacz pole obok obiektu.

8. Zapisz swoje zmiany.

Używanie metod skanowania

Kaspersky Endpoint Security używa techniki skanowania nazywanej Uczenie maszynowe oraz analizy przy użyciu sygnatur. Podczas analizy sygnatur Kaspersky Endpoint Security porównuje wykryty obiekt z wpisami w swojej bazie danych. W oparciu o zalecenia ekspertów z Kaspersky, uczenie maszynowe i analiza sygnatur jest zawsze włączona.

Aby zwiększyć efektywność ochrony, możesz użyć analizy heurystycznej. Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.

W celu skonfigurowania użycia analizy heurystycznej w działaniu modułu Ochrona plików:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij **Ustawienia zaawansowane**.
4. Jeśli chcesz, żeby aplikacja korzystała z analizy heurystycznej do ochrony przed zagrożeniami plikowymi, w sekcji **Analiza heurystyczna** zaznacz pole **Metody skanowania**. Następnie użyj suwaka, aby ustawić poziom analizy heurystycznej: **Poziom niski**, **Poziom średni** lub **Poziom szczegółowy**.
5. Zapisz swoje zmiany.

Używanie technologii skanowania w działaniu modułu Ochrona plików

W celu skonfigurowania korzystania z technologii skanowania w trakcie działania Ochrony plików:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij **Ustawienia zaawansowane**.
4. W sekcji **Technologie skanowania** zaznacz pola obok nazw technologii, której chcesz użyć do ochrony przed zagrożeniami plikowymi:

   - **Technologia iSwift**. Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.

   - **Użyj technologii iChecker**. Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).

5. Zapisz swoje zmiany.

Optymalizowanie skanowania plików

Możesz zoptymalizować skanowanie plików wykonywane przez składnik Ochrona plików, zmniejszając czas skanowania i zwiększając szybkość działania programu Kaspersky Endpoint Security. Można to uzyskać poprzez skanowanie tylko nowych plików i tych plików, które zostały zmodyfikowane od ostatniego skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.

Możesz także włączyć korzystanie z technologii iChecker i iSwift, co zoptymalizuje prędkość skanowania plików poprzez wykluczenie plików, które nie zostały zmodyfikowane od ostatniego skanowania.

W celu zoptymalizowania skanowania plików:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij **Ustawienia zaawansowane**.
4. W sekcji **Optymalizacja** zaznacz pole **Skanuj tylko nowe i zmienione pliki**.
5. Zapisz swoje zmiany.

Skanowanie plików złożonych

Popularną techniką ukrywania wirusów i innego szkodliwego oprogramowania jest osadzanie ich w plikach złożonych, takich jak archiwa czy bazy danych. W celu wykrycia ukrytych w ten sposób wirusów i innego szkodliwego oprogramowania, plik złożony musi zostać rozpakowany, co może spowolnić skanowanie. Możesz ograniczyć typy skanowanych plików złożonych, dzięki czemu skanowanie będzie szybsze.

Metoda używana do przetwarzania zainfekowanego pliku złożonego (leczenie lub usuwanie) zależy od typu pliku.

Ochrona plików wyleczy pliki złożone w formatach ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR i ICE i usunie pliki we wszystkich pozostałych formatach (za wyjątkiem pocztowych baz danych).

W celu skonfigurowania skanowania plików złożonych:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij **Ustawienia zaawansowane**.
4. W sekcji **Skanuj pliki złożone** określ, które pliki złożone mają być skanowane: archiwa, pakiety dystrybucyjne, poczta lub pliki w formatach pakietu Office.

5. Jeśli skanowanie tylko nowych i zmodyfikowanych plików zostało wyłączone, skonfiguruj ustawienia każdego typu pliku złożonego: skanuj wszystkie pliki tego typu lub tylko nowe pliki.

   Jeśli skanowanie tylko nowych i zmodyfikowanych plików zostało włączone, Kaspersky Endpoint Security skanuje tylko nowe i zmodyfikowane pliki wszystkich typów plików złożonych.

6. Skonfiguruj zaawansowane ustawienia skanowania plików złożonych.

   - **Nie rozpakowuj dużych plików złożonych**.

     Jeżeli to pole jest zaznaczone, Kaspersky Endpoint Security nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość.

     Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security skanuje pliki złożone o wszystkich rozmiarach.

     > Kaspersky Endpoint Security skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

   - **Rozpakowywanie plików złożonych w tle**.

     Jeśli pole jest zaznaczone, Kaspersky Endpoint Security oferuje dostęp do plików złożonych, które mają większy rozmiar niż wartość określona przed skanowaniem tych plików. W tym przypadku Kaspersky Endpoint Security rozpakowuje i skanuje pliki złożone w tle.

     Kaspersky Endpoint Security oferuje dostęp do plików złożonych, których rozmiar jest mniejszy niż ta wartość dopiero po rozpakowaniu i przeskanowaniu tych plików.

     Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security oferuje dostęp do plików złożonych dopiero po rozpakowaniu i przeskanowaniu plików dowolnego rozmiaru.

7. Zapisz swoje zmiany.

Zmienianie trybu skanowania

Tryb skanowania odnosi się do warunku wyzwalającego skanowanie pliku przez moduł Ochrona plików. Domyślnie program Kaspersky Endpoint Security skanuje pliki w trybie smart. W tym trybie skanowania Ochrona plików decyduje czy skanować pliki po przeanalizowaniu operacji wykonywanych na pliku przez użytkownika, aplikację w imieniu użytkownika (z poziomu konta, które zostało użyte przy logowaniu lub z poziomu innego konta użytkownika), bądź przez system operacyjny. Na przykład, jeżeli wykorzystywany jest dokument programu Microsoft Office Word, Kaspersky Endpoint Security skanuje plik przy jego pierwszym otwieraniu i ostatnim zamykaniu. Wszystkie operacje wykonywane w międzyczasie, które nadpisują plik, nie są skanowane.

W celu zmiany trybu skanowania plików:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.

3. Kliknij **Ustawienia zaawansowane**.

4. W sekcji **Tryb skanowania** wybierz żądany tryb:

   - **Tryb Inteligentny**. W tym trybie Ochrona plików skanuje obiekt w oparciu o analizę akcji podejmowanych na obiekcie. Na przykład, jeżeli wykorzystywany jest dokument Microsoft Office, Kaspersky Endpoint Security skanuje plik przy jego pierwszym otwieraniu i ostatnim zamykaniu. Wszystkie operacje wykonywane w międzyczasie, które nadpisują plik, nie są skanowane.

   - **Podczas dostępu i modyfikacji**. W tym trybie moduł Ochrona plików skanuje obiekty za każdym razem, gdy są otwierane lub modyfikowane.

   - **Podczas dostępu**. W tym trybie moduł Ochrona plików skanuje obiekty podczas ich otwierania.

   - **Podczas wykonywania**. W tym trybie moduł Ochrona plików skanuje obiekty jedynie podczas ich uruchamiania.

5. Zapisz swoje zmiany.

Skanowanie kontenerów

Kontener jest odizolowanym środowiskiem, w którym aplikacja może działać bez bezpośredniej interakcji z systemem operacyjnym. Używanie kontenerów wiąże się z następującymi ryzykami:

- Hakerzy mogą wykorzystać luki w zabezpieczeniach konteneryzacji w celu naruszenia bezpieczeństwa aplikacji znajdujących się w kontenerze.

- Hakerzy mogą wykorzystać niezabezpieczoną konfigurację środowiska kontenerowego w celu uzyskania nieautoryzowanego dostępu do danych na komputerze lub naruszenia integralności systemu.

- Udany atak na kontener może umożliwić hakerowi uzyskanie dostępu do danych na komputerze.

- Hakerzy mogą wykorzystywać luki w zabezpieczeniach sieci w celu przechwytywania ruchu sieciowego.

Kaspersky Endpoint Security skanuje pliki nie tylko na dyskach, ale również wewnątrz kontenerów. Oznacza to, że Kaspersky Endpoint Security jest zewnętrznym narzędziem służącym do wykrywania złośliwej aktywności wewnątrz kontenerów. Pozwala to utrzymać wydajność kontenerów i zapobiega konfliktom z innymi aplikacjami wewnątrz kontenera. Instalacja Kaspersky Endpoint Security wewnątrz kontenera nie jest obsługiwana.

Oprócz zapewnienia bezpieczeństwa kontenerów Kaspersky Endpoint Security umożliwia zarządzanie aplikacjami wewnątrz kontenerów przy użyciu Kontroli aplikacji. Kontrolę aplikacji konfiguruje się dla kontenerów w taki sam sposób jak dla aplikacji zainstalowanych na komputerze. Monitorowanie integralności systemu obsługuje także kontenery.

Wymagania dotyczące kontenerów

- Kontener musi być kontenerem Docker. Inne narzędzia do konteneryzacji nie są obsługiwane.

- Kontener musi działać w trybie izolacji procesu. Tryb izolacji Hyper-V nie jest obsługiwany.

- Kontener musi być umieszczony na serwerze z systemem Windows Server 2016, 2019 lub 2022 (Docker Host).
- Kontener musi zawierać obraz systemu Windows (Docker Image). Systemy Windows 10 i 11 nie są obsługiwane. Obrazy systemu Linux nie są obsługiwane.

Działanie podejmowane w przypadku wykrycia zagrożenia

W razie wykrycia zagrożenia wewnątrz kontenera aplikacja zastosuje czynność wybraną dla komponentu Ochrona plików. Skanowanie kontenerów ma dodatkowe ustawienia (zobacz poniższe instrukcje). W przypadku wykrycia zagrożenia aplikacja zablokuje złośliwą aktywność i wykona wybraną akcję (na przykład podejmie próbę wyleczenia obiektu). Kaspersky Endpoint Security może zatrzymać kontener, jeśli wykrytego obiektu nie da się wyleczyć. Domyślnie funkcja zatrzymywania kontenerów jest wyłączona.

Jak skonfigurować skanowanie kontenerów w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
4. Kliknij **Ustawienia**.
5. Spowoduje to otwarcie okna. Wybierz w nim zakładkę **Dodatkowe**.
6. W sekcji **Skanowanie operacji na plikach wykonywanych w kontenerach Windows** skonfiguruj ustawienia skanowania kontenerów:
   - **Zatrzymaj kontener, jeśli dezynfekcja się nie powiedzie**. Aplikacja może nie mieć wystarczających uprawnień do odczytu i zapisu wykrytego obiektu. W takim przypadku wyleczenie lub usunięcie wykrytego obiektu będzie niemożliwe. Jeśli to pole wyboru jest zaznaczone, aplikacja blokuje wykryty obiekt i wstrzymuje kontener. Jeśli to pole wyboru nie jest zaznaczone, aplikacja tylko blokuje wykryty obiekt.
   - **Nie skanuj operacji na plikach wykonywanych w kontenerach Windows**. Jeśli to pole wyboru jest zaznaczone, aplikacja skanuje kontener tylko podczas jego uruchamiania. Jeśli to pole wyboru nie jest zaznaczone, aplikacja będzie stale skanować kontener w czasie rzeczywistym.
7. Zapisz swoje zmiany.

Jak skonfigurować skanowanie kontenerów w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Ochrona plików**.
5. W menu **Ustawienia zaawansowane**, Wybierz zakładkę **Wydajność**.

6. W sekcji **Optymalizacja skanowania** skonfiguruj ustawienia skanowania kontenerów:

   - **Wstrzymaj kontener, jeśli dezynfekcja się nie powiedzie**. Aplikacja może nie mieć wystarczających uprawnień do odczytu i zapisu wykrytego obiektu. W takim przypadku wyleczenie lub usunięcie wykrytego obiektu będzie niemożliwe. Jeśli to pole wyboru jest zaznaczone, aplikacja blokuje wykryty obiekt i wstrzymuje kontener. Jeśli to pole wyboru nie jest zaznaczone, aplikacja tylko blokuje wykryty obiekt.

   - **Nie skanuj operacji na plikach wykonywanych w kontenerach Windows**. Jeśli to pole wyboru jest zaznaczone, aplikacja skanuje kontener tylko podczas jego uruchamiania. Jeśli to pole wyboru nie jest zaznaczone, aplikacja będzie stale skanować kontener w czasie rzeczywistym.

7. Zapisz swoje zmiany.

Jak skonfigurować skanowanie kontenerów w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.

3. W sekcji **Skanowanie operacji na plikach wykonywanych w kontenerach Windows** skonfiguruj ustawienia skanowania kontenerów:

   - **Zatrzymaj kontener, jeśli dezynfekcja się nie powiedzie**. Aplikacja może nie mieć wystarczających uprawnień do odczytu i zapisu wykrytego obiektu. W takim przypadku wyleczenie lub usunięcie wykrytego obiektu będzie niemożliwe. Jeśli to pole wyboru jest zaznaczone, aplikacja blokuje wykryty obiekt i wstrzymuje kontener. Jeśli to pole wyboru nie jest zaznaczone, aplikacja tylko blokuje wykryty obiekt.

   - **Nie skanuj operacji na plikach wykonywanych w kontenerach Windows**. Jeśli to pole wyboru jest zaznaczone, aplikacja skanuje kontener tylko podczas jego uruchamiania. Jeśli to pole wyboru nie jest zaznaczone, aplikacja będzie stale skanować kontener w czasie rzeczywistym.

4. Zapisz swoje zmiany.

Ochrona przed włamaniami

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Ochrona przed włamaniami uniemożliwia aplikacjom wykonywanie działań niebezpiecznych dla systemu operacyjnego i zapewnia kontrolę dostępu do zasobów systemu operacyjnego i danych osobowych. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network.

Komponent kontroluje działanie aplikacji za pomocą *uprawnień aplikacji*. Uprawnienia aplikacji obejmują następujące parametry dostępu:

- Dostęp do zasobów systemu operacyjnego (na przykład opcje automatycznego uruchamiania, klucze rejestru)
- Dostęp do danych osobowych (takich jak pliki i aplikacje)

Aktywność sieciowa aplikacji jest kontrolowana przez Zaporę sieciową za pomocą *reguł sieciowych*.

Podczas pierwszego uruchomienia aplikacji Ochrona przed włamaniami wykonuje następujące działania:

1. Sprawdza bezpieczeństwo aplikacji przy użyciu pobranych antywirusowych baz danych.
2. Sprawdza bezpieczeństwo aplikacji w Kaspersky Security Network.

   Zalecane jest uczestniczenie w Kaspersky Security Network, aby zapewnić bardziej efektywne działanie komponentu Ochrona przed włamaniami.

3. Umieszcza aplikację w jednej z grup zaufania: *Zaufane*, *Niskie ograniczenia*, *Wysokie ograniczenia*, *Niezaufane*.

   Grupa zaufania określa uprawnienia, do których program Kaspersky Endpoint Security odnosi się podczas kontrolowania aktywności aplikacji. Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera.

   Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania dla składników Zapora sieciowa i Ochrona przed włamaniami. Nie można zmienić grupy zaufania tylko dla Zapory sieciowej lub Ochrony przed włamaniami.

   Jeśli odmówiłeś uczestnictwa w KSN lub nie ma sieci, Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od ustawień modułu Ochrona przed włamaniami. Po otrzymaniu reputacji aplikacji od KSN, grupę zaufania można zmienić automatycznie.

4. Blokuje działania aplikacji w zależności od grupy zaufania. Na przykład, aplikacje z grupy *Wysokie ograniczenia* mają zablokowany dostęp do modułów systemu operacyjnego.

Przy następnym uruchomieniu aplikacji, Kaspersky Endpoint Security sprawdzi integralność aplikacji. Jeżeli aplikacja nie została zmieniona, moduł użyje dla niej bieżących uprawnień aplikacji. Jeżeli aplikacja została zmodyfikowana, Kaspersky Endpoint Security analizuje aplikację tak, jakby była uruchamiana po raz pierwszy.

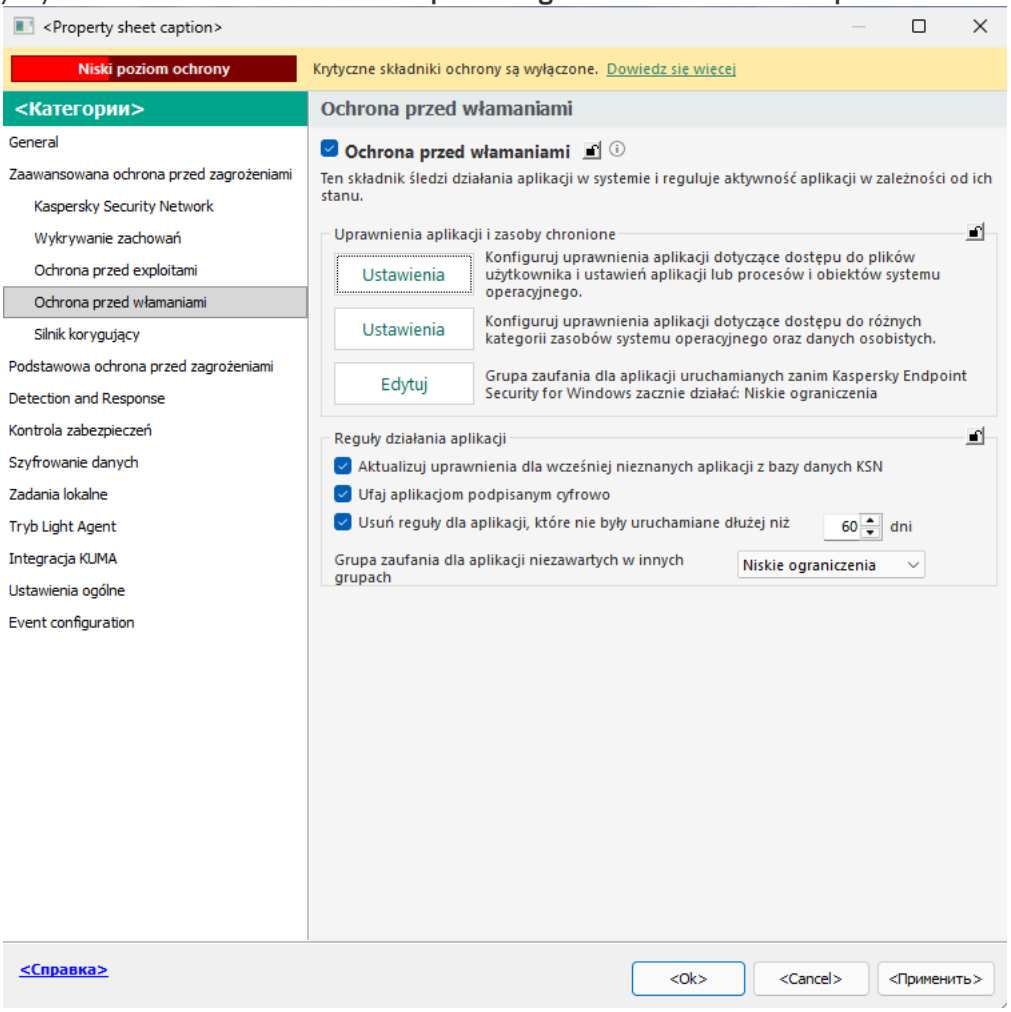
Włączanie i wyłączanie modułu Ochrona przed włamaniami

Domyślnie moduł Ochrona przed włamaniami jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky.

Jak włączyć lub wyłączyć komponent Ochrona przed włamaniami w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.



Ustawienia modułu Ochrona przed włamaniami

4. Użyj pola **Ochrona przed włamaniami**, aby włączyć lub wyłączyć komponent.

5. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć komponent Ochrona przed włamaniami w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ochrona hosta → Ochrona przed włamaniami**.

5. Użyj przełącznika **Ochrona przed włamaniami WŁĄCZONA**, aby włączyć lub wyłączyć komponent.

6. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć komponent Ochrona przed włamaniami w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.

3. Użyj przełącznika **Ochrona przed włamaniami**, aby włączyć lub wyłączyć komponent.

4. Zapisz swoje zmiany.

Jeśli komponent Ochrona przed włamaniami jest włączona, Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera. Następnie Kaspersky Endpoint Security zablokuje działania aplikacji w zależności od grupy zaufania.

Zarządzanie grupami zaufania aplikacji

Przy pierwszym uruchomieniu aplikacji moduł Ochrona przed włamaniami sprawdza jej bezpieczeństwo i umieszcza w grupie zaufania.

W pierwszym kroku skanowania aplikacji Kaspersky Endpoint Security przeszukuje wewnętrzną bazę danych znanych aplikacji w poszukiwaniu odpowiadającego jej wpisu i jednocześnie wysyła żądanie do bazy danych Kaspersky Security Network (jeśli dostępne jest połączenie internetowe). W oparciu o wyniki przeszukiwania wewnętrznej bazy danych i bazy danych Kaspersky Security Network, aplikacja zostaje umieszczona w grupie zaufania. Przy każdym kolejnym uruchomieniu aplikacji program Kaspersky Endpoint Security wysyła nowe zapytanie do bazy danych KSN i umieszcza aplikację w innej grupie zaufania, jeśli reputacja aplikacji w bazie danych KSN uległa zmianie.

Możesz wybrać grupę zaufania, w której program Kaspersky Endpoint Security musi automatycznie umieszczać wszystkie nieznane aplikacje. Aplikacje uruchomione przed uruchomieniem programu Kaspersky Endpoint Security są automatycznie umieszczane w grupie zaufania ustawionej w ustawieniach komponentu Ochrona przed włamaniami.

Dla aplikacji, które zostały uruchomione przed Kaspersky Endpoint Security, kontrolowana jest tylko aktywność sieciowa. Kontrola odbywa się zgodnie z regułami sieciowymi określonymi w ustawieniach Zapory sieciowej.

Zmiana grupy zaufania aplikacji

Przy pierwszym uruchomieniu aplikacji moduł Ochrona przed włamaniami sprawdza jej bezpieczeństwo i umieszcza w grupie zaufania.

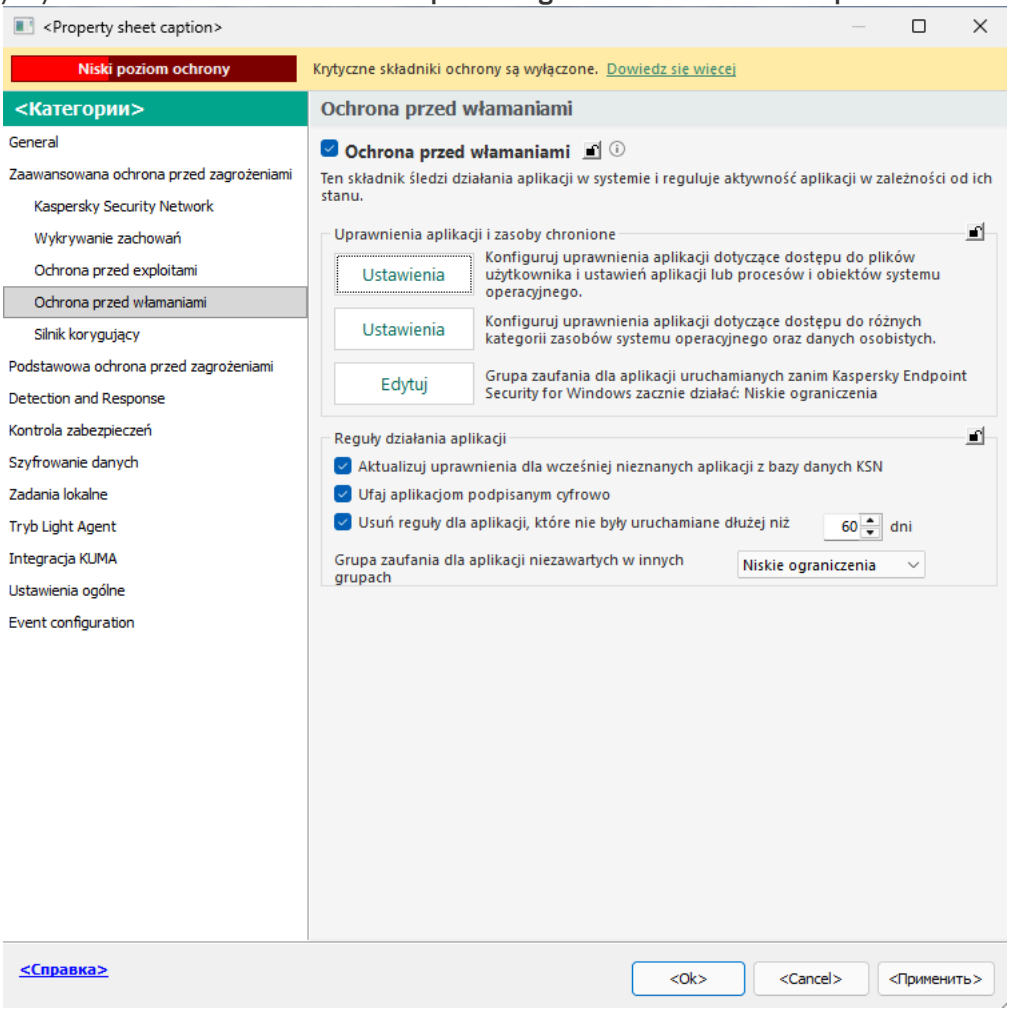
Specjaliści z Kaspersky nie zalecają przenoszenia aplikacji z automatycznie przydzielonej grupy zaufania do innej grupy zaufania. Zamiast tego możesz zmodyfikować uprawnienia dla pojedynczej aplikacji (jeśli to konieczne).

Jak zmienić grupę zaufania aplikacji w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.



Ustawienia modułu Ochrona przed włamaniami

4. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij przycisk **Ustawienia**.

   To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.

5. Wybierz zakładkę **Uprawnienia aplikacji**.

6. Kliknij **Dodaj**.

7. W otwartym oknie wprowadź kryteria wyszukiwania aplikacji, której grupę zaufania chcesz zmienić.

   Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

8. Kliknij **Odśwież**.

   Kaspersky Endpoint Security wyszuka aplikację na skonsolidowanej liście aplikacji zainstalowanych na zarządzanych komputerach. Kaspersky Endpoint Security wyświetli listę aplikacji spełniających Twoje kryteria wyszukiwania.

9. Wybierz żądaną aplikację.

10. Z listy rozwijalnej **Dodaj wybraną aplikację do grupy zaufania** wybierz żądaną grupę zaufania dla aplikacji.

11. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak zmienić grupę zaufania aplikacji w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Ochrona przed włamaniami**.
5. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij odnośnik **Uprawnienia aplikacji i zasoby chronione**.

   To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
6. Wybierz zakładkę **Uprawnienia aplikacji**.

   W lewej części okna zobaczysz listę grup zaufania, a w prawej części okna zobaczysz i ich właściwości.
7. Kliknij **Dodaj**.

   To spowoduje uruchomienie Kreatora dodawania aplikacji do grupy zaufania.
8. Wybierz odpowiednią grupę zaufania dla aplikacji.
9. Wybierz typ **Aplikacja**. Przejdź do następnego kroku.

   Jeśli chcesz zmienić grupę zaufania dla kilku aplikacji, wybierz typ **Grupa** i określ nazwę grupy zaufania.
10. Z otwartej listy aplikacji wybierz aplikacje, dla których chcesz zmienić grupę zaufania.

    Użyj filtra. Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.
11. Zakończ działanie Kreatora.

    Aplikacja zostanie dodana do grupy zaufania.
12. Zapisz swoje zmiany.

Jak zmienić grupę zaufania aplikacji w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. Kliknij **Zarządzanie aplikacjami**.

   Spowoduje to otwarcie listy zainstalowanych aplikacji.
4. Wybierz żądaną aplikację.
5. Z menu kontekstowego aplikacji wybierz **Ograniczenia** → **<grupa zaufania>**.
6. Zapisz swoje zmiany.

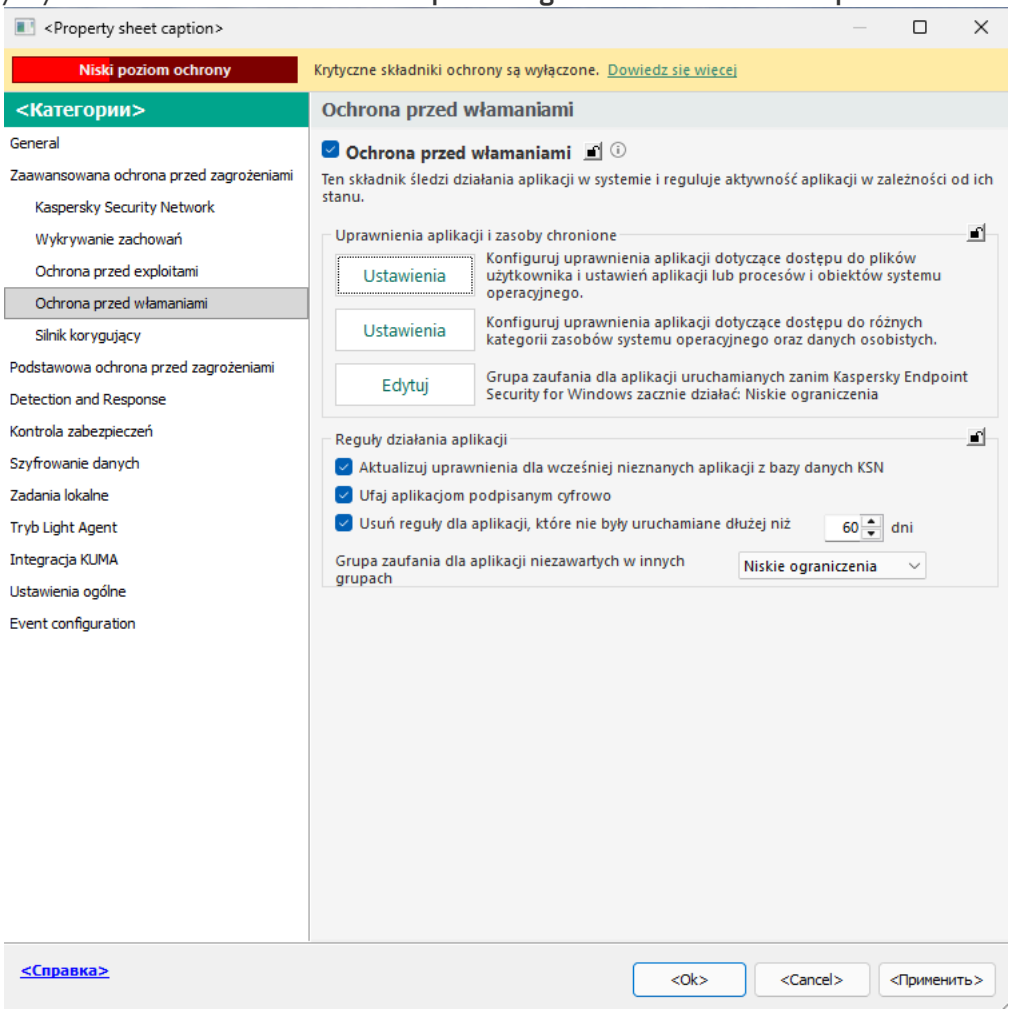
W wyniku tego działania aplikacja zostanie umieszczona w innej grupie zaufania. Następnie Kaspersky Endpoint Security zablokuje działania aplikacji w zależności od grupy zaufania. Status *(określona przez użytkownika)* zostanie przypisany do aplikacji. Jeśli reputacja aplikacji została zmieniona w Kaspersky Security Network, Ochrona przed włamaniami pozostawi tę grupę zaufania aplikacji niezmienioną.

Konfigurowanie uprawnień grupy zaufania

Optymalne uprawnienia aplikacji są domyślnie tworzone dla różnych grup zaufania. Ustawienia uprawnień dla grup aplikacji, które nie znajdują się w grupie zaufania, dziedziczą wartości z ustawień uprawnień grupy zaufania.

Jak zmienić uprawnienia grupy zaufania w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.



Ustawienia modułu Ochrona przed włamaniami

4. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij przycisk **Ustawienia**.

   To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
5. Przejdź do zakładki **Uprawnienia aplikacji**.
6. Wybierz żądaną grupę zaufania.

7. Z menu kontekstowego grupy zaufania wybierz **Uprawnienia grupy**.

   Spowoduje to otwarcie właściwości grupy zaufania.

8. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz **Pliki i rejestr systemu**.
   - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz **Uprawnienia**.

   Aktywność sieciowa aplikacji jest kontrolowana przez Zaporę sieciową za pomocą *reguł sieciowych*.

9. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania kliknij je prawym klawiszem myszy, aby otworzyć menu kontekstowe i wybrać odpowiednią opcję: **Dziedzicz**, **Zezwól** (✓) lub **Blokuj** (⊘).

10. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** (✓ / ⊘).

    Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.

11. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak zmienić uprawnienia grupy zaufania w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Ochrona przed włamaniami**.
5. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij odnośnik **Uprawnienia aplikacji i zasoby chronione**.

   To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.

6. Przejdź do zakładki **Uprawnienia aplikacji**.

   W lewej części okna zobaczysz listę grup zaufania, a w prawej części okna zobaczysz i ich właściwości.

7. W lewej części okna wybierz odpowiednią grupę zaufania.
8. W prawej części okna, z listy rozwijalnej wykonaj jedną z następujących czynności:

   - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz **Pliki i rejestr systemu**.
   - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz **Uprawnienia**.

   Aktywność sieciowa aplikacji jest kontrolowana przez Zaporę sieciową za pomocą *reguł sieciowych*.

9. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania wybierz odpowiednią opcję: **Dziedzicz**, **Zezwól** (), **Zablokuj** ().

10. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** (/).

    Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.

11. Zapisz swoje zmiany.

Jak zmienić uprawnienia grupy zaufania w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.

3. Kliknij **Zarządzanie aplikacjami**.

   Spowoduje to otwarcie listy zainstalowanych aplikacji.

4. Wybierz żądaną grupę zaufania.

5. Z menu kontekstowego grupy zaufania wybierz **Szczegóły i reguły**.

   Spowoduje to otwarcie właściwości grupy zaufania.

6. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz **Pliki i rejestr systemu**.
   - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz **Uprawnienia**.

   Aktywność sieciowa aplikacji jest kontrolowana przez Zaporę sieciową za pomocą *reguł sieciowych*.

7. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania kliknij je prawym klawiszem myszy, aby otworzyć menu kontekstowe i wybrać odpowiednią opcję: **Dziedzicz**, **Zezwól** () lub **Blokuj** ().

8. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** ().

   Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.

9. Zapisz swoje zmiany.

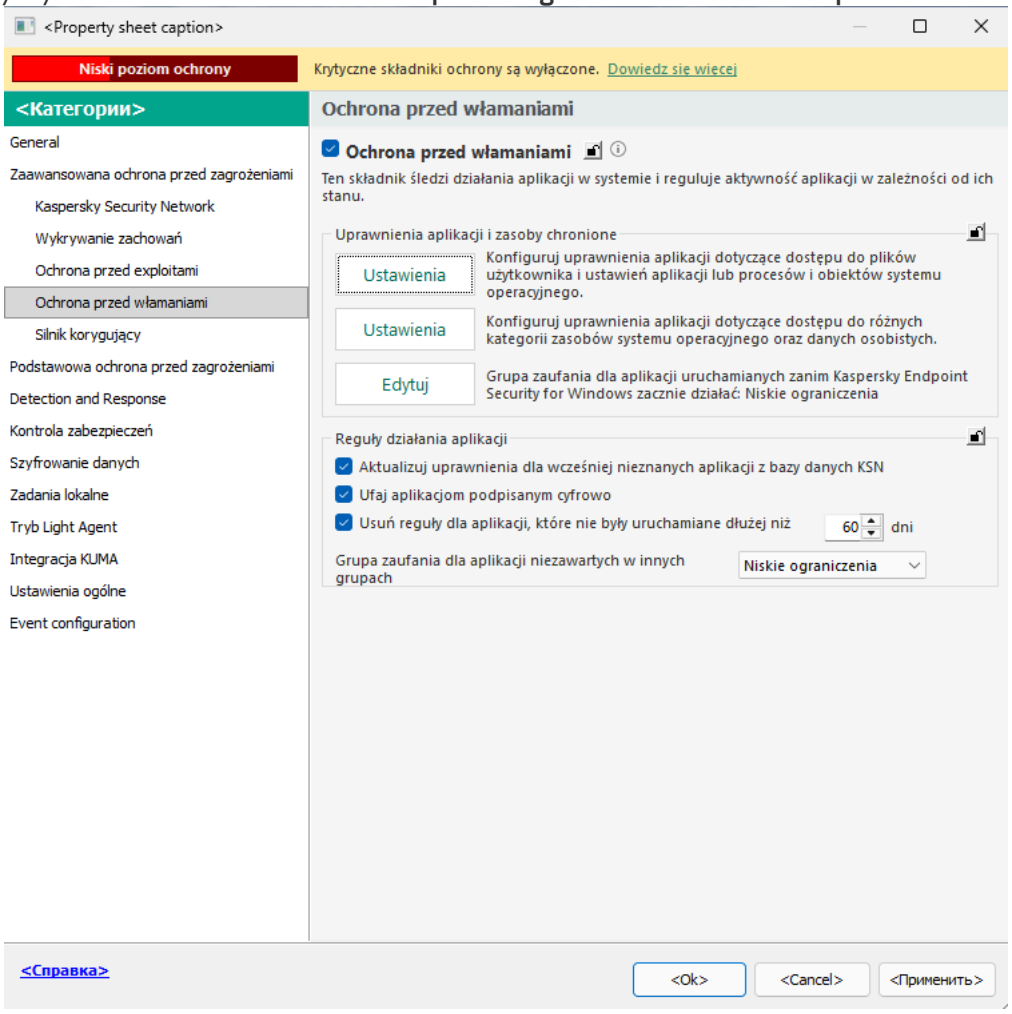
Uprawnienia grupy zaufania zostaną zmienione. Następnie Kaspersky Endpoint Security zablokuje działania aplikacji w zależności od grupy zaufania. Stan (*Ustawienia niestandardowe*) zostanie przypisany do grupy zaufania.

Wybieranie grupy zaufania dla aplikacji uruchamianych przed Kaspersky Endpoint Security

Dla aplikacji, które zostały uruchomione przed Kaspersky Endpoint Security, kontrolowana jest tylko aktywność sieciowa. Kontrola odbywa się zgodnie z regułami sieciowymi określonymi w ustawieniach Zapory sieciowej. Aby określić, które reguły sieciowe muszą być stosowane do monitorowania aktywności sieciowej dla tych aplikacji, należy wybrać grupę zaufania.

Jak wybrać grupę zaufania dla aplikacji uruchomionych przed Kaspersky Endpoint Security w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.



Ustawienia modułu Ochrona przed włamaniami

4. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij przycisk **Edytuj**.
5. Dla ustawienia **Grupa zaufania dla aplikacji uruchomionych przed Kaspersky Endpoint Security** wybierz odpowiednią grupę zaufania.
6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak wybrać grupę zaufania dla aplikacji uruchomionych przed Kaspersky Endpoint Security w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Ochrona przed włamaniami**.
5. Dla ustawienia **Grupa zaufania dla aplikacji uruchomionych przed Kaspersky Endpoint Security** wybierz odpowiednią grupę zaufania.
6. Zapisz swoje zmiany.

Jak wybrać grupę zaufania dla aplikacji uruchomionych przed Kaspersky Endpoint Security w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. W sekcji **Grupa zaufania dla aplikacji uruchamianych zanim Kaspersky Endpoint Security zacznie działać** wybierz odpowiednią grupę zaufania.
4. Zapisz swoje zmiany.

W wyniku tego działania aplikacja, która jest uruchamiana przed Kaspersky Endpoint Security, zostanie umieszczona w innej grupie zaufania. Następnie Kaspersky Endpoint Security zablokuje działania aplikacji w zależności od grupy zaufania.

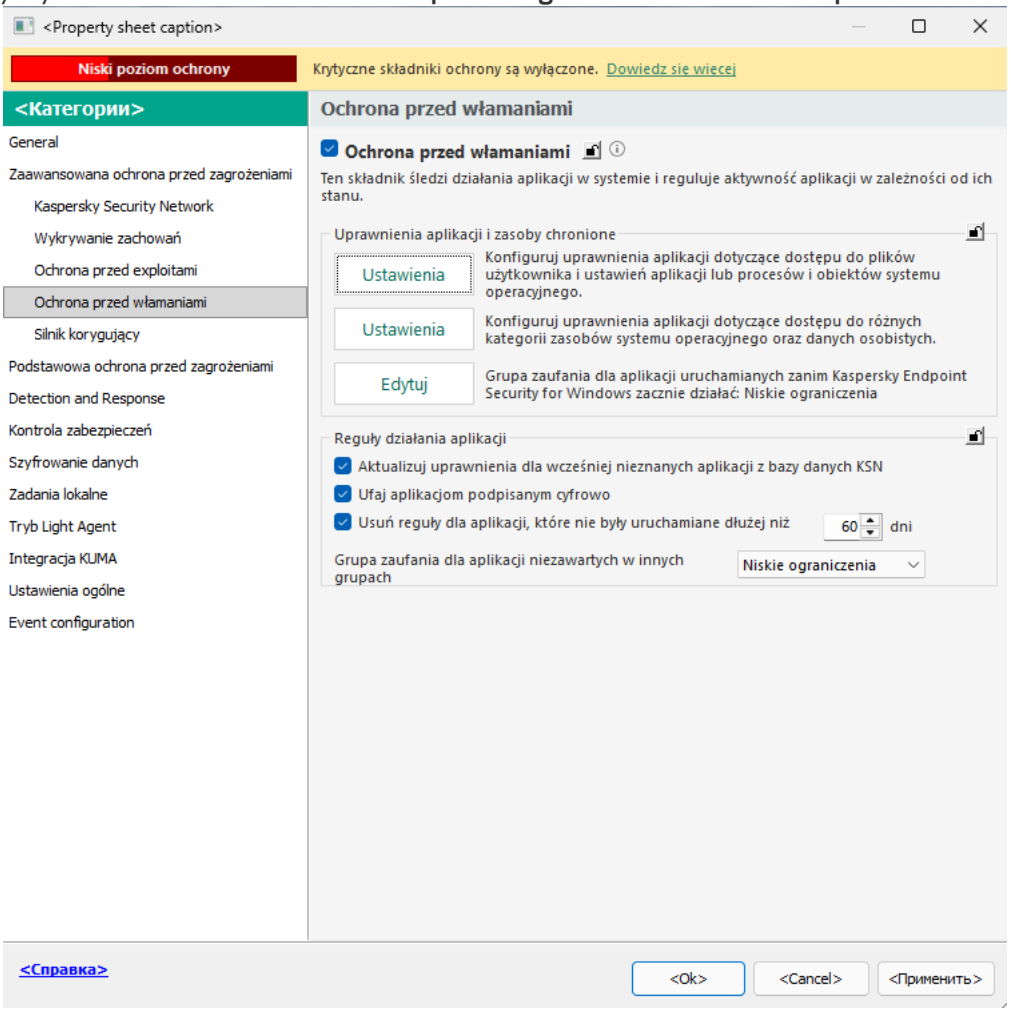
Wybieranie grupy zaufania dla nieznanych aplikacji

Podczas pierwszego uruchomienia aplikacji komponent Ochrona przed włamaniami określa grupę zaufania dla aplikacji. Jeśli nie masz dostępu do internetu lub jeśli Kaspersky Security Network nie zawiera informacji o tej aplikacji, domyślnie Kaspersky Endpoint Security umieści aplikację w grupie *Niskie ograniczenia*. Jeśli informacje o wcześniej nieznanej aplikacji zostały wykryte w KSN, Kaspersky Endpoint Security zaktualizuje uprawnienia tej aplikacji. Następnie możesz ręcznie edytować uprawnienia aplikacji.

Jak wybrać grupę zaufania dla nieznanych aplikacji w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.



Ustawienia modułu Ochrona przed włamaniami

4. W sekcji **Reguły działania aplikacji** użyj listy rozwijalnej **Grupa zaufania dla aplikacji niezawartych w innych grupach**, aby wybrać żądaną grupę zaufania.

   Jeśli uczestnictwo w Kaspersky Security Network jest włączone, Kaspersky Endpoint Security wysyła do KSN pytanie odnośnie reputacji aplikacji za każdym razem, gdy jest ona uruchamiana. W oparciu o uzyskaną odpowiedź, aplikacja może zostać przeniesiona do grupy zaufania, która jest inna niż ta określona w ustawienia komponentu Ochrona przed włamaniami.

5. Użyj pola **Aktualizuj uprawnienia dla wcześniej nieznanych aplikacji z bazy danych KSN**, aby skonfigurować automatyczną aktualizację uprawnień nieznanych aplikacji.

6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak wybrać grupę zaufania dla nieznanych aplikacji w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ochrona hosta → Ochrona przed włamaniami**.

5. W sekcji **Reguły działania aplikacji** użyj listy rozwijalnej **Grupa zaufania dla aplikacji niezawartych w innych grupach**, aby wybrać żądaną grupę zaufania.

   Jeśli uczestnictwo w Kaspersky Security Network jest włączone, Kaspersky Endpoint Security wysyła do KSN pytanie odnośnie reputacji aplikacji za każdym razem, gdy jest ona uruchamiana. W oparciu o uzyskaną odpowiedź, aplikacja może zostać przeniesiona do grupy zaufania, która jest inna niż ta określona w ustawienia komponentu Ochrona przed włamaniami.

6. Użyj pola **Aktualizuj uprawnienia dla wcześniej nieznanych aplikacji z bazy danych KSN**, aby skonfigurować automatyczną aktualizację uprawnień nieznanych aplikacji.

7. Zapisz swoje zmiany.

Jak wybrać grupę zaufania dla nieznanych aplikacji w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.

3. W sekcji **Reguły działania aplikacji** wybierz odpowiednią grupę zaufania.

   Jeśli uczestnictwo w Kaspersky Security Network jest włączone, Kaspersky Endpoint Security wysyła do KSN pytanie odnośnie reputacji aplikacji za każdym razem, gdy jest ona uruchamiana. W oparciu o uzyskaną odpowiedź, aplikacja może zostać przeniesiona do grupy zaufania, która jest inna niż ta określona w ustawienia komponentu Ochrona przed włamaniami.

4. Użyj pola **Uaktualnij reguły dla wcześniej nieznanych aplikacji z KSN**, aby skonfigurować automatyczną aktualizację uprawnień nieznanych aplikacji.

5. Zapisz swoje zmiany.

Wybieranie grupy zaufania dla cyfrowo podpisanych aplikacji

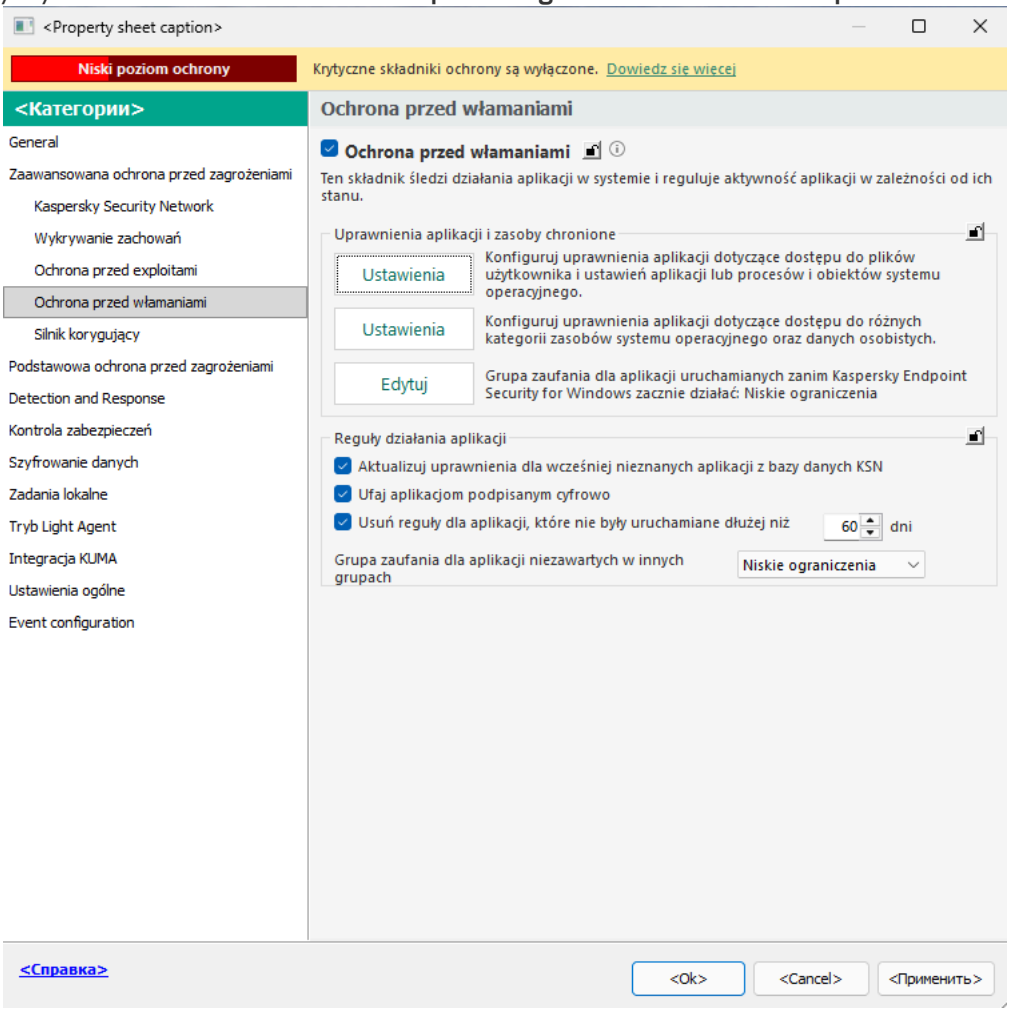
Kaspersky Endpoint Security zawsze umieszcza aplikacje podpisane certyfikatami firmy Microsoft lub certyfikatami firmy Kaspersky w grupie *Zaufane*.

Jak wybrać grupę zaufania dla cyfrowo podpisanych aplikacji w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.



Ustawienia modułu Ochrona przed włamaniami

4. W sekcji **Reguły działania aplikacji** użyj pola wyboru **Ufaj aplikacjom podpisanym cyfrowo**, aby włączyć lub wyłączyć automatyczne przypisywanie do grupy zaufania Zaufane dla aplikacji zawierających podpis cyfrowy zaufanych producentów.

   Zaufani producenci to producenci oprogramowania, którzy zostali umieszczeni w grupie zaufania przez Kaspersky. Możesz także ręcznie dodać certyfikat producenta do zaufanych certyfikatów systemowych.

   Jeśli pole nie jest zaznaczone, Ochrona przed włamaniami nie uważa aplikacji posiadających podpis cyfrowy za zaufane i wykorzystuje inne parametry do określenia ich grupy zaufania.

5. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak wybrać grupę zaufania dla cyfrowo podpisanych aplikacji w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ochrona hosta → Ochrona przed włamaniami**.

5. W sekcji **Reguły działania aplikacji** użyj pola wyboru **Ufaj aplikacjom podpisanym cyfrowo**, aby włączyć lub wyłączyć automatyczne przypisywanie do grupy zaufania Zaufane dla aplikacji zawierających podpis cyfrowy zaufanych producentów.

Zaufani producenci to producenci oprogramowania, którzy zostali umieszczeni w grupie zaufania przez Kaspersky. Możesz także ręcznie dodać certyfikat producenta do zaufanych certyfikatów systemowych.

Jeśli pole nie jest zaznaczone, Ochrona przed włamaniami nie uważa aplikacji posiadających podpis cyfrowy za zaufane i wykorzystuje inne parametry do określenia ich grupy zaufania.

6. Zapisz swoje zmiany.

Jak wybrać grupę zaufania dla cyfrowo podpisanych aplikacji w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.
3. W sekcji **Reguły działania aplikacji** użyj pola wyboru **Ufaj aplikacjom podpisanym cyfrowo**, aby włączyć lub wyłączyć automatyczne przypisywanie do grupy zaufania Zaufane dla aplikacji zawierających podpis cyfrowy zaufanych producentów.

   Zaufani producenci to producenci oprogramowania, którzy zostali umieszczeni w grupie zaufania przez Kaspersky. Możesz także ręcznie dodać certyfikat producenta do zaufanych certyfikatów systemowych.

   Jeśli pole nie jest zaznaczone, Ochrona przed włamaniami nie uważa aplikacji posiadających podpis cyfrowy za zaufane i wykorzystuje inne parametry do określenia ich grupy zaufania.

4. Zapisz swoje zmiany.

Zarządzanie uprawnieniami aplikacji

Domyślnie, aktywność aplikacji jest kontrolowana w oparciu o uprawnienia aplikacji, które są definiowane dla określonej grupy zaufania, do której Kaspersky Endpoint Security przypisał aplikację przy jej pierwszym uruchomieniu. Jeżeli jest to konieczne, możesz zmodyfikować uprawnienia aplikacji dla całej grupy zaufania, dla pojedynczej aplikacji lub grupy aplikacji znajdujących się w grupie zaufania.

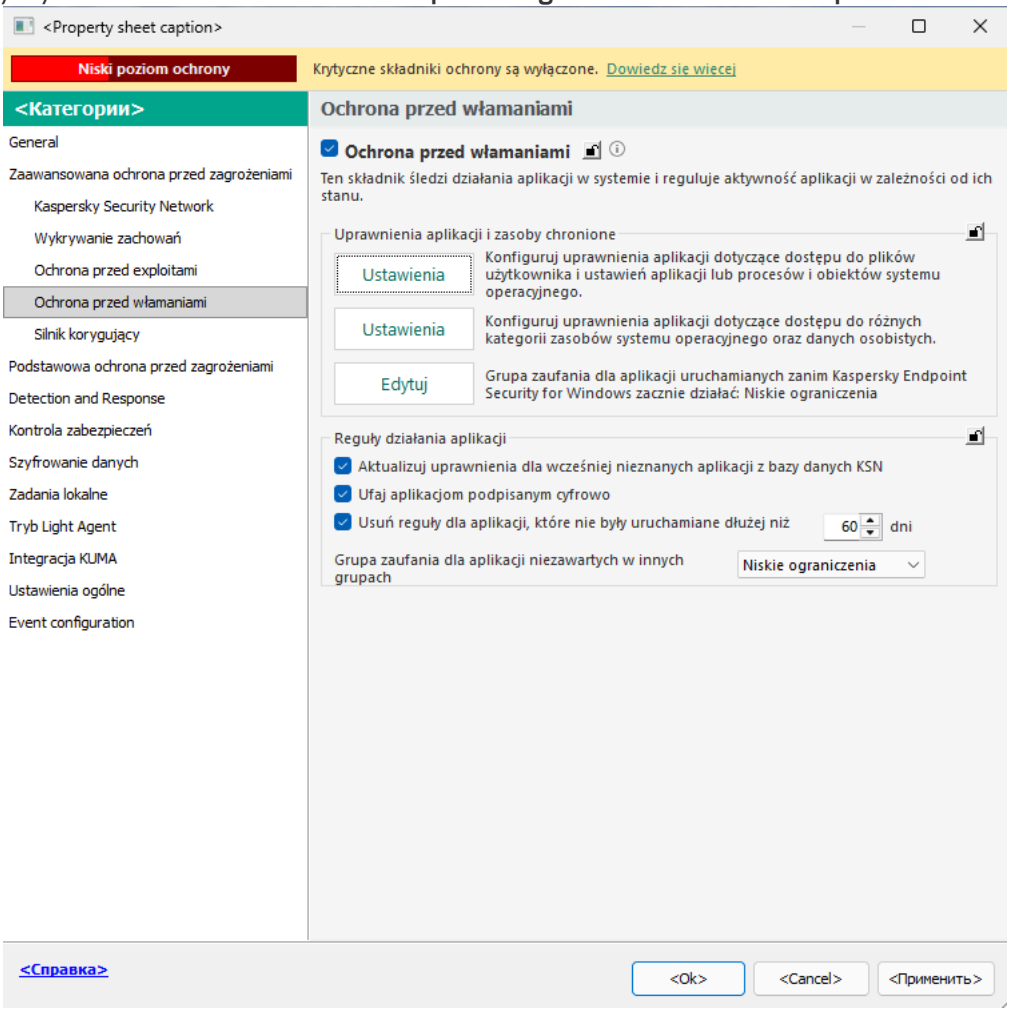
Ręcznie zdefiniowane uprawnienia aplikacji posiadają wyższy priorytet niż uprawnienia aplikacji, które zostały zdefiniowane dla grupy zaufania. Innymi słowy, jeśli ręcznie zdefiniowane uprawnienia aplikacji różnią się od uprawnień aplikacji zdefiniowanych dla grup zaufania, komponent Ochrona przed włamaniami kontroluje aktywność aplikacji zgodnie z ręcznie zdefiniowanymi uprawnieniami aplikacji.

Reguły, które tworzysz dla aplikacji, są dziedziczone przez aplikacje potomne. Na przykład, jeśli zablokujesz całą aktywność sieciową dla cmd.exe, cała aktywność sieciowa zostanie także zablokowana dla notepad.exe, gdy zostanie uruchomiony przy użyciu cmd.exe. Jeśli aplikacja nie jest potomną aplikacją, z której jest uruchamiana, reguły nie są dziedziczone.

Jak zmienić uprawnienia aplikacji w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.



Ustawienia modułu Ochrona przed włamaniami

4. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij przycisk **Ustawienia**.

   To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.

5. Przejdź do zakładki **Uprawnienia aplikacji**.

6. Kliknij **Dodaj**.

7. W otwartym oknie wprowadź kryteria wyszukiwania aplikacji, której uprawnienia chcesz zmienić.

   Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

8. Kliknij **Odśwież**.

   Kaspersky Endpoint Security wyszuka aplikację na skonsolidowanej liście aplikacji zainstalowanych na zarządzanych komputerach. Kaspersky Endpoint Security wyświetli listę aplikacji spełniających Twoje kryteria wyszukiwania.

9. Wybierz żądaną aplikację.

10. Z listy rozwijalnej **Dodaj wybraną aplikację do grupy zaufania** wybierz **Grupy domyślne** i kliknij **OK**.

    Aplikacja zostanie dodana do domyślnej grupy.

11. Wybierz odpowiednią aplikację, a następnie wybierz **Uprawnienia aplikacji** z menu kontekstowego aplikacji.

    Spowoduje to otwarcie właściwości aplikacji.

12. Wykonaj jedną z poniższych czynności:

    - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz **Pliki i rejestr systemu**.
    - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz **Uprawnienia**.

    Aktywność sieciowa aplikacji jest kontrolowana przez Zaporę sieciową za pomocą *reguł sieciowych*.

13. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania kliknij je prawym klawiszem myszy, aby otworzyć menu kontekstowe i wybrać odpowiednią opcję: **Dziedzicz**, **Zezwól** (✓) lub **Blokuj** (⊘).

14. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** (✓ / ⊘).

    Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.

15. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak zmienić uprawnienia aplikacji w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Ochrona przed włamaniami**.
5. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij odnośnik **Uprawnienia aplikacji i zasoby chronione**.

   To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
6. Przejdź do zakładki **Uprawnienia aplikacji**.

   W lewej części okna zobaczysz listę grup zaufania, a w prawej części okna zobaczysz i ich właściwości.
7. Kliknij **Dodaj**.

   To spowoduje uruchomienie Kreatora dodawania aplikacji do grupy zaufania.
8. Wybierz odpowiednią grupę zaufania dla aplikacji.
9. Wybierz typ **Aplikacja**. Przejdź do następnego kroku.

   Jeśli chcesz zmienić grupę zaufania dla kilku aplikacji, wybierz typ **Grupa** i określ nazwę grupy zaufania.
10. Z otwartej listy aplikacji wybierz aplikacje, dla których chcesz zmienić uprawnienia aplikacji.

    Użyj filtra. Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.
11. Zakończ działanie Kreatora.

    Aplikacja zostanie dodana do grupy zaufania.

12. W lewej części okna wybierz odpowiednią aplikację.

13. W prawej części okna, z listy rozwijalnej wykonaj jedną z następujących czynności:

    - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz **Pliki i rejestr systemu**.
    - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz **Uprawnienia**.

    Aktywność sieciowa aplikacji jest kontrolowana przez Zaporę sieciową za pomocą *reguł sieciowych*.

14. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania wybierz odpowiednią opcję: **Dziedzicz**, **Zezwól** (), **Zablokuj** ().

15. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** (/).

    Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.

16. Zapisz swoje zmiany.

Jak zmienić uprawnienia aplikacji w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.

3. Kliknij **Zarządzanie aplikacjami**.

   Spowoduje to otwarcie listy zainstalowanych aplikacji.

4. Wybierz żądaną aplikację.

5. Z menu kontekstowego aplikacji wybierz **Szczegóły i reguły**.

   Spowoduje to otwarcie właściwości aplikacji.

6. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz **Pliki i rejestr systemu**.
   - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz **Uprawnienia**.

7. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania kliknij je prawym klawiszem myszy, aby otworzyć menu kontekstowe i wybrać odpowiednią opcję: **Dziedzicz**, **Zezwól** () lub **Blokuj** ().

8. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** ().

   Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.

9. Wybierz zakładkę **Wykluczenia** i skonfiguruj zaawansowane ustawienia aplikacji (patrz tabela poniżej).

10. Zapisz swoje zmiany.

Zaawansowane ustawienia aplikacji

Parametr	Opis
Nie skanuj plików otwieranych przez aplikację	Wszystkie pliki, które są otwierane przez aplikację, zostają wykluczone ze skanowania wykonywanego przez program Kaspersky Endpoint Security. Na przykład, jeśli używasz aplikacji do tworzenia kopii zapasowej plików, ta funkcja pomaga w zmniejszeniu zużycia zasobów przez Kaspersky Endpoint Security.
Nie monitoruj aktywności aplikacji	Kaspersky Endpoint Security nie będzie monitorował aktywności sieciowej i plikowej aplikacji w systemie operacyjnym. Możesz skonfigurować monitorowanie aktywności aplikacji dla różnych komponentów Kaspersky Endpoint Security: • **Nie monitoruj komponentów zabezpieczeń i kontroli**. Aktywność aplikacji jest monitorowana przez następujące komponentów: Wykrywanie zachowań, Ochrona przed exploitami, Ochrona przed włamaniami, Silnik korygujący i Zapora sieciowa. • **Nie monitoruj Managed Detection and Response oraz Endpoint Detection and Response**. Aktywność aplikacji jest monitorowana przez wbudowanego agenta MDR I wbudowanego agenta EDR (KATA). • **Nie przechwytuj interaktywnych danych wejściowych konsoli dla Endpoint Detection and Response**. Kaspersky Endpoint Security nie wysyła danych telemetrycznych dotyczących zarządzania aplikacją na konsoli. Dane telemetryczne są używane przez Kaspersky Anti Targeted Attack Platform (EDR).
Nie dziedzicz ograniczeń nadrzędnego procesu (aplikacji)	Ograniczenia skonfigurowane dla procesu nadrzędnego nie będą stosowane przez program Kaspersky Endpoint Security do procesu podrzędnego. Proces nadrzędny jest uruchamiany przez aplikację, dla której skonfigurowano uprawnienia aplikacji (Ochrona przed włamaniami) i reguły sieciowe dla aplikacji (Zapora sieciowa).
Nie monitoruj aktywności aplikacji potomnych	Kaspersky Endpoint Security nie będzie monitorował aktywności plikowej i sieciowej aplikacji, które są uruchamiane przez tę aplikację. Możesz zastosować wykluczenie cyklicznie. Aby aplikacja nie monitorowała aktywności całego łańcucha aplikacji podrzędnych.
Zezwól na interakcję z interfejsem Kaspersky Endpoint Security	Autoochrona Kaspersky Endpoint Security blokuje wszystkie próby zarządzania usługami aplikacji ze zdalnego komputera. Jeśli pole jest zaznaczone, aplikacja do zdalnej administracji może zarządzać ustawieniami Kaspersky Endpoint Security poprzez interfejs Kaspersky Endpoint Security.
Nie skanuj szyfrowanego ruchu sieciowego / Nie skanuj całego ruchu sieciowego	Ruch sieciowy zainicjowany przez aplikację zostanie wykluczony ze skanowania wykonywanego przez Kaspersky Endpoint Security. Ze skanowania można wykluczyć cały ruch sieciowy lub tylko zaszyfrowany ruch sieciowy. Ze skanowania możesz także wykluczyć pojedyncze adresy IP i numery portów. Kaspersky Endpoint Security w wersji 14.0 lub wcześniejszej nie obsługuje wykluczania ruchu sieciowego, jeśli dla zaufanej aplikacji zamiast ścieżki określono skrót.

Ochrona zasobów systemu operacyjnego i danych osobowych

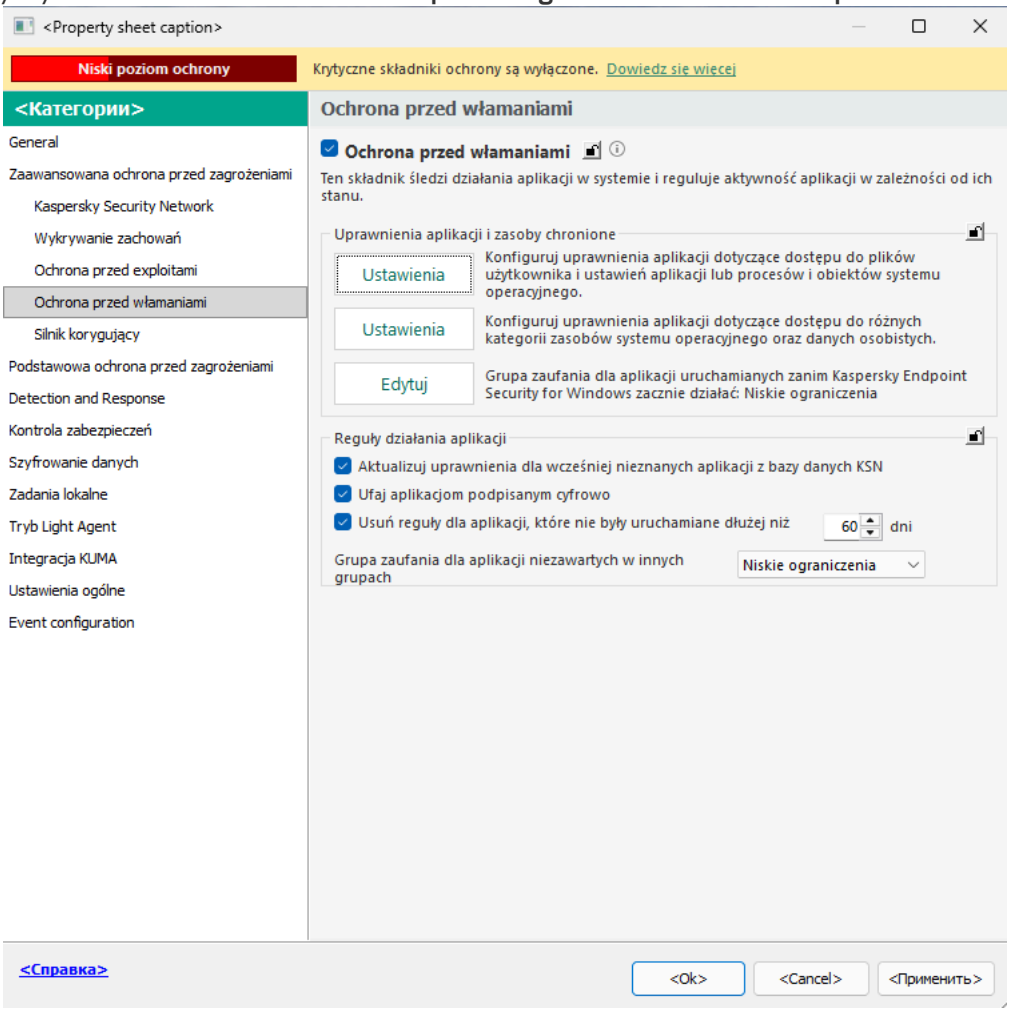
Komponent Ochrona przed włamaniami zarządza uprawnieniami aplikacji do podejmowania działań na różnych kategoriach zasobów systemu operacyjnego i danych osobistych. Specjaliści z Kaspersky utworzyli listę predefiniowanych kategorii chronionych zasobów. Na przykład, kategoria *System operacyjny* zawiera podkategorię *Ustawienia startowe*, która wyświetla wszystkie klucze rejestru skojarzone z automatycznym uruchamianiem aplikacji. Nie możesz zmieniać ani usuwać predefiniowanych kategorii chronionych zasobów ani chronionych zasobów znajdujących się w tych kategoriach.

Jak dodawać chronione zasoby w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.



Ustawienia modułu Ochrona przed włamaniami

4. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij przycisk **Ustawienia**.

   To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.

5. Przejdź do zakładki **Chronione zasoby**.

   W lewej części okna zostanie wyświetlona lista chronionych zasobów oraz odpowiednie uprawnienia dostępu do tych zasobów w zależności od określonej grupy zaufania.

6. Wybierz kategorię chronionych zasobów, do których chcesz dodać nowy chroniony zasób.

   Jeśli chcesz dodać podkategorię, kliknij **Dodaj → Kategoria**.

7. Kliknij przycisk **Dodaj**. Z listy rozwijalnej wybierz typ zasobu, który chcesz dodać: **Plik lub folder** lub **Klucz rejestru**.

8. W otwartym oknie wybierz plik, folder lub klucz rejestru.

   Możesz przejrzeć uprawnienia aplikacji do uzyskania dostępu do dodanych zasobów. Aby to zrobić, w lewej części okna wybierz dodany zasób, a Kaspersky Endpoint Security wyświetli uprawnienia dostępu dla każdej grupy zaufania. Możesz także wyłączyć kontrolę aktywności aplikacji na zasobach, używając pola obok nowego zasobu.

9. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak dodać chroniony zasób w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Ochrona przed włamaniami**.
5. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij odnośnik **Uprawnienia aplikacji i zasoby chronione**.

   To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
6. Przejdź do zakładki **Chronione zasoby**.

   W lewej części okna zostanie wyświetlona lista chronionych zasobów oraz odpowiednie uprawnienia dostępu do tych zasobów w zależności od określonej grupy zaufania.
7. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zasobu.
8. W sekcji **Nazwa grupy** wybierz kategorię chronionych zasobów, do których chcesz dodać nowy chroniony zasób.

   Jeśli chcesz dodać podkategorię, wybierz opcję **Kategoria chronionych zasobów**.
9. Wybierz typ zasobu, który chcesz dodać: **Plik lub folder** lub **Klucz rejestru**.
10. Wybierz plik, folder lub klucz rejestru.
11. Zakończ działanie Kreatora.

    Możesz przejrzeć uprawnienia aplikacji do uzyskania dostępu do dodanych zasobów. Aby to zrobić, w lewej części okna wybierz dodany zasób, a Kaspersky Endpoint Security wyświetli uprawnienia dostępu dla każdej grupy zaufania. Możesz także użyć pola w kolumnie **Stan**, aby wyłączyć kontrolę aktywności aplikacji na zasobach.
12. Zapisz swoje zmiany.

Jak dodać chroniony zasób w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. Kliknij **Zarządzaj zasobami**.

   Zostanie otwarta lista chronionych zasobów.
4. Wybierz kategorię chronionych zasobów, do których chcesz dodać nowy chroniony zasób.

   Jeśli chcesz dodać podkategorię, kliknij **Dodaj** → **Kategoria**.
5. Kliknij przycisk **Dodaj**. Z listy rozwijalnej wybierz typ zasobu, który chcesz dodać: **Plik lub folder** lub **Klucz rejestru**.

6. W otwartym oknie wybierz plik, folder lub klucz rejestru.

   Możesz przejrzeć uprawnienia aplikacji do uzyskania dostępu do dodanych zasobów. Aby to zrobić, w lewej części okna wybierz dodany zasób, a Kaspersky Endpoint Security wyświetli listę aplikacji i uprawnienia dostępu dla każdej aplikacji. Możesz wyłączyć kontrolę aktywności aplikacji na zasobach, używając przycisku **Włącz kontrolę** w kolumnie **Stan**.

7. Zapisz swoje zmiany.

Kaspersky Endpoint Security będzie kontrolował dostęp do dodanych zasobów systemu operacyjnego i do danych osobowych. Kaspersky Endpoint Security kontroluje dostęp aplikacji do zasobów w oparciu o grupę zaufania przypisaną do aplikacji. Możesz także zmienić grupę zaufania aplikacji.

Usuwanie informacji o nieużywanych aplikacjach

Kaspersky Endpoint Security używa uprawnień aplikacji do kontrolowania aktywności aplikacji. Uprawnienia aplikacji są określone przez ich grupę zaufania. Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, gdy aplikacja jest uruchamiania po raz pierwszy. Możesz ręcznie zmienić grupę zaufania aplikacji. Możesz także ręcznie skonfigurować uprawnienia poszczególnych aplikacji. Kaspersky Endpoint Security przechowuje następujące informacje o aplikacji: grupę zaufania aplikacji i uprawnienia aplikacji.

Kaspersky Endpoint Security automatycznie usuwa informacje o nieużywanych aplikacjach, aby zaoszczędzić zasoby komputera. Kaspersky Endpoint Security usuwa informacje o aplikacji zgodnie z następującymi regułami:

- Jeśli grupa zaufania i uprawnienia aplikacji zostały określone automatycznie, Kaspersky Endpoint Security usunie informacje o tej aplikacji po 30 dniach. Nie jest możliwa zmiana okresu przechowywania informacji o aplikacji ani wyłączenie automatycznego usuwania.

- Jeśli ręcznie umieścisz aplikację w grupie zaufania lub skonfigurujesz jej uprawnienia dostępu, Kaspersky Endpoint Security usunie informacje o tej aplikacji po 60 dniach (domyślny okres przechowywania). Możesz zmienić okres przechowywania informacji o aplikacji lub wyłączyć automatyczne usuwanie (patrz instrukcje poniżej).

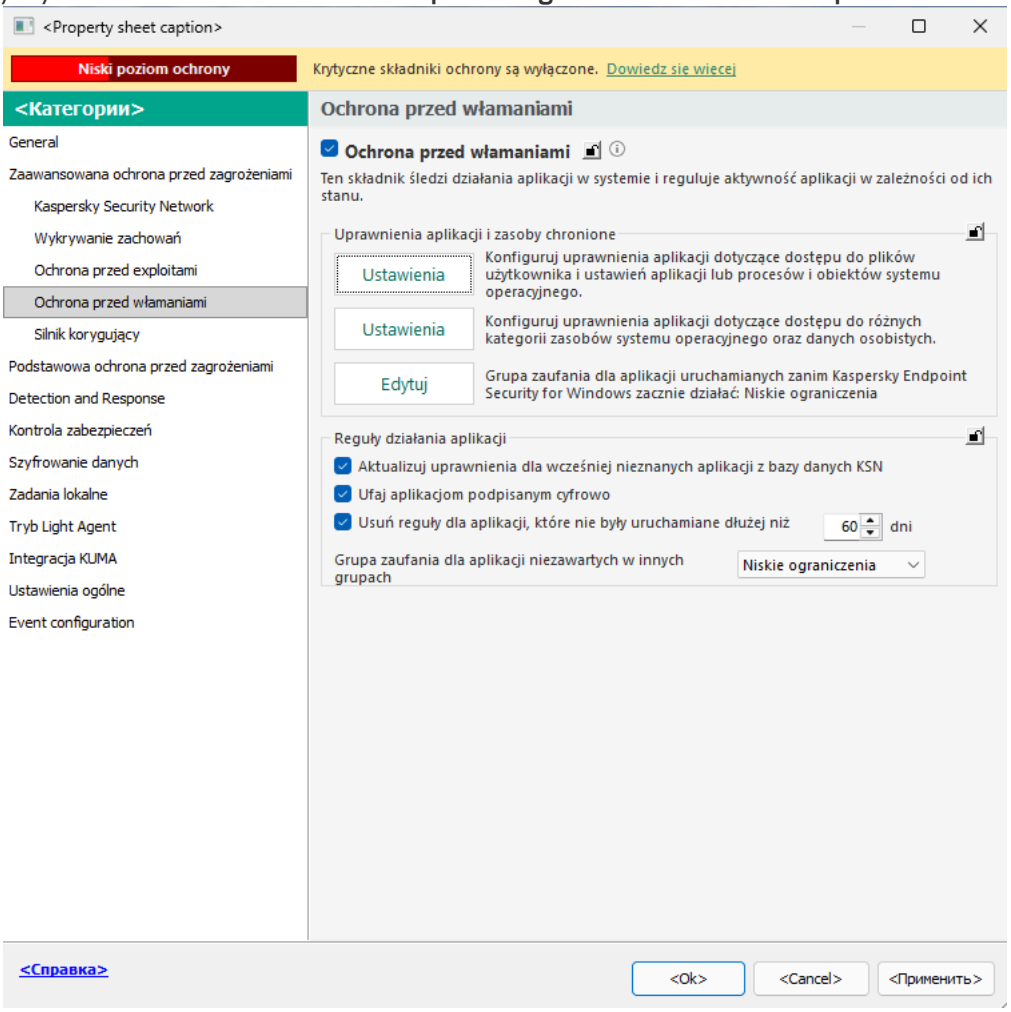
Po uruchomieniu aplikacji, której informacje zostały usunięte, Kaspersky Endpoint Security analizuje aplikację tak, jakby była uruchamiana po raz pierwszy.

Jak skonfigurować automatyczne usuwanie informacji o nieużywanych aplikacjach w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed włamaniami**.



Ustawienia modułu Ochrona przed włamaniami

4. W sekcji **Reguły działania aplikacji** wykonaj jedną z następujących czynności:

   - Jeśli chcesz skonfigurować automatyczne usuwanie, zaznacz pole wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni** i wprowadź liczbę dni.

     Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu zostaną usunięte przez Kaspersky Endpoint Security po upływie określonej liczbie dni. Informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone, zostaną również usunięte przez Kaspersky Endpoint Security po 30 dniach.

   - Jeśli chcesz wyłączyć automatyczne usuwanie, usuń zaznaczenie pola wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni**.

     Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu będą przechowywane przez Kaspersky Endpoint Security na czas nieokreślony, bez żadnych ograniczeń czasu przechowywania. Kaspersky Endpoint Security usunie tylko informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone po 30 dniach.

5. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak skonfigurować automatyczne usuwanie informacji o nieużywanych aplikacjach w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ochrona hosta** → **Ochrona przed włamaniami**.

5. W sekcji **Reguły działania aplikacji** wykonaj jedną z następujących czynności:

   - Jeśli chcesz skonfigurować automatyczne usuwanie, zaznacz pole wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż (dni, 1 do 90)** i wprowadź liczbę dni.

     Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu zostaną usunięte przez Kaspersky Endpoint Security po upływie określonej liczbie dni. Informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone, zostaną również usunięte przez Kaspersky Endpoint Security po 30 dniach.

   - Jeśli chcesz wyłączyć automatyczne usuwanie, usuń zaznaczenie pola wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż (dni, 1 do 90)**.

     Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu będą przechowywane przez Kaspersky Endpoint Security na czas nieokreślony, bez żadnych ograniczeń czasu przechowywania. Kaspersky Endpoint Security usunie tylko informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone po 30 dniach.

6. Zapisz swoje zmiany.

Jak skonfigurować automatyczne usuwanie informacji o nieużywanych aplikacjach w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.

3. W sekcji **Reguły działania aplikacji** wykonaj jedną z następujących czynności:

   - Jeśli chcesz skonfigurować automatyczne usuwanie, zaznacz pole wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni (od 1 do 90)** i wprowadź liczbę dni.

     Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu zostaną usunięte przez Kaspersky Endpoint Security po upływie określonej liczbie dni. Informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone, zostaną również usunięte przez Kaspersky Endpoint Security po 30 dniach.

   - Jeśli chcesz wyłączyć automatyczne usuwanie, usuń zaznaczenie pola wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni (od 1 do 90)**.

     Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu będą przechowywane przez Kaspersky Endpoint Security na czas nieokreślony, bez żadnych ograniczeń czasu przechowywania. Kaspersky Endpoint Security usunie tylko informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone po 30 dniach.

4. Zapisz swoje zmiany.

Monitorowanie Ochrony przed włamaniami

Możesz otrzymać raporty z działania komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.

Aby monitorować działania komponentu Ochrona przed włamaniami, musisz włączyć zapisywanie do raportu. Na przykład, możesz włączyć przekazywanie raportów dla pojedynczych aplikacji w ustawieniach komponentu Ochrona przed włamaniami.

Podczas konfigurowania monitorowania Ochrony przed włamaniami należy wziąć pod uwagę potencjalne obciążenie sieci, gdy przekazywane są zdarzenia do Kaspersky Security Center. Możesz też włączyć zapisywanie raportów tylko w dzienniku lokalnym programu Kaspersky Endpoint Security.

Ochrona dostępu do audio i wideo

Funkcje ochrony sygnału audio i ochrony dostępu do kamery internetowej nie są obsługiwane na komputerach opartych na architekturze ARM.

Cyberprzestępcy mogą używać specjalnych programów w celu podjęcia próby uzyskania dostępu do urządzeń, które nagrywają audio i wideo (takich jak mikrofony lub kamery internetowe). Kaspersky Endpoint Security kontroluje, kiedy aplikacje uzyskują dostęp do strumienia audio i do strumienia wideo oraz chronią dane przed nieautoryzowanym przechwytywaniem.

Domyślnie Kaspersky Endpoint Security zezwala na odbieranie strumieni audio i wideo tylko dla aplikacji z grupy *Zaufane*. Aplikacje z grup *Niskie ograniczenia*, *Wysokie ograniczenia* i *Niezaufane* nie mogą odbierać strumienia audio i wideo z urządzeń. Możesz ręcznie zezwolić aplikacjom na uzyskiwanie dostępu do strumienia audio i strumienia wideo.

Specjalne funkcje ochrony strumienia audio

W przypadku ochrony strumienia audio należy mieć na uwadze następujące kwestie:

- Aby ta funkcjonalność mogła działać, należy włączyć moduł Ochrona przed włamaniami.
- Jeśli aplikacja zaczęła odbierać strumień audio przed uruchomieniem Ochrony przed włamaniami, Kaspersky Endpoint Security zezwoli aplikacji na odbieranie strumienia audio i nie wyświetli żadnego komunikatu.
- Jeśli po rozpoczęciu odbierania przez aplikację strumienia audio przeniosłeś ją go grupy *Niezaufane* lub *Wysokie ograniczenia*, Kaspersky Endpoint Security zezwoli aplikacji na odbieranie strumienia audio i nie wyświetli żadnego komunikatu.
- Po zmianie ustawień dostępu aplikacji do urządzeń rejestrujących dźwięk (na przykład, jeśli dla aplikacji zablokowano możliwość odbierania strumienia audio), ta aplikacja musi zostać uruchomiona ponownie, aby zatrzymać dla niej odbieranie strumienia audio.
- Kontrola dostępu urządzeń rejestrujących dźwięk do strumienia audio nie zależy od ustawień dostępu aplikacji do kamery internetowej.
- Kaspersky Endpoint Security chroni dostęp tylko do wbudowanych i zewnętrznych mikrofonów. Inne urządzenia rejestrujące dźwięk nie są obsługiwane.

- Kaspersky Endpoint Security nie może zagwarantować ochrony strumienia audio pochodzącego z takich urządzeń, jak aparaty DSLR (lustrzanki), kamery wideo oraz kamery sportowe.
- Jeśli uruchamiasz aplikacje rejestrujące dźwięk i obraz lub aplikacje do odtwarzania dźwięku i obrazu pierwszy raz od momentu zainstalowania Kaspersky Endpoint Security, działanie tych aplikacji może zostać przerwane. Jest to konieczne do włączenia funkcji kontrolującej dostęp aplikacji do urządzeń rejestrujących dźwięk. Usługi systemu kontrolujące sprzęt audio zostają uruchomione ponownie, gdy Kaspersky Endpoint Security jest uruchamiany po raz pierwszy.

Specjalne funkcje ochrony dostępu do kamery internetowej

Funkcja ochrony dostępu do kamery internetowej posiada następujące cechy i ograniczenia:

- Aplikacja kontroluje obraz wideo i nieruchome obrazy pochodzące z przetworzenia danych kamery internetowej.
- Aplikacja kontroluje strumień audio, jeśli jest on częścią strumienia wideo otrzymanego z kamery internetowej.
- Aplikacja kontroluje jedynie kamery podłączone do portów USB lub IEEE1394, które są wyświetlane w Menedżerze urządzeń systemu Windows jako Urządzenia do obrazowania.
- Kaspersky Endpoint Security obsługuje następujące kamery internetowe:
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310
  - Logitech Webcam C210
  - Logitech Webcam Pro 9000
  - Logitech HD Webcam C525
  - Microsoft LifeCam VX-1000
  - Microsoft LifeCam VX-2000
  - Microsoft LifeCam VX-3000
  - Microsoft LifeCam VX-800
  - Microsoft LifeCam Cinema

  Kaspersky nie gwarantuje obsługi kamer internetowych, które nie znajdują się na tej liście.

Ochrona przed atakami BadUSB

Niektóre wirusy modyfikują oprogramowanie wbudowane urządzeń USB w celu zmylenia systemu operacyjnego do wykrywania urządzenia USB jako klawiatury. W wyniku tego działania wirus może wykonać polecenia z poziomu konta użytkownika, na przykład, w celu pobrania szkodliwego oprogramowania.

Komponent Ochrona przed atakami BadUSB zapobiega podłączeniu do komputera zainfekowanych urządzeń USB emulujących klawiaturę.

Po podłączeniu urządzenia USB do komputera i zidentyfikowaniu go przez system operacyjny jako klawiatury, aplikacja wyświetli pytanie o wprowadzenie kodu numerycznego, wygenerowanego przez aplikację, z poziomu tej klawiatury lub Klawiatury ekranowej, jeśli jest dostępna (patrz rysunek poniżej). Ta procedura jest znana jako autoryzacja klawiatury.

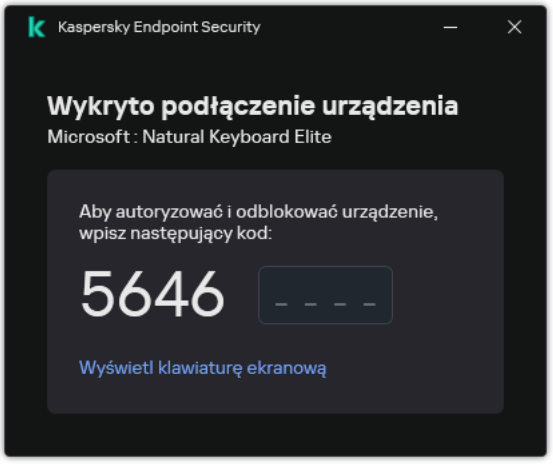
Jeśli kod został wpisany poprawnie, aplikacja zapisuje parametry identyfikujące – VID/PID klawiatury oraz numer portu, do którego została podłączona – na liście uprawnionych klawiatur. Po ponownym podłączeniu klawiatury lub po ponownym uruchomieniu systemu nie ma konieczności powtarzania procesu autoryzacji klawiatury.

Jeśli autoryzowana klawiatura zostanie podłączona do innego portu USB, aplikacja ponownie wyświetli prośbę o przeprowadzenie autoryzacji tej klawiatury.

Jeśli kod numeryczny zostanie wprowadzony niepoprawnie, aplikacja wygeneruje nowy kod. Możesz skonfigurować liczbę prób wprowadzenia kodu numerycznego. Jeśli kod numeryczny zostanie wprowadzony niepoprawnie kilka razy lub okno autoryzacji klawiatury jest zamknięte (patrz rysunek poniżej), aplikacja zablokuje wprowadzenie z poziomu tej klawiatury. Po upłynięciu czasu blokowania urządzenia USB lub ponownym uruchomieniu systemu operacyjnego, aplikacja ponownie wyświetli pytanie o przeprowadzenie autoryzacji klawiatury.

Aplikacja zezwoli na użycie zautoryzowanej klawiatury, a zablokuje klawiaturę, która nie została zautoryzowana.

Komponent Ochrona przed atakami BadUSB nie jest domyślnie instalowany. Jeśli potrzebujesz składnika Ochrona przed atakami BadUSB, możesz dodać ten składnik we właściwościach pakietu instalacyjnego przed zainstalowaniem aplikacji lub zmienić dostępne składniki aplikacji po zainstalowaniu aplikacji.



Autoryzacja klawiatury

Włączanie i wyłączanie Ochrony przed atakami BadUSB

Urządzenia USB, rozpoznawane przez system operacyjny jako klawiatury i podłączone do komputera przed zainstalowaniem modułu Ochrona przed atakami BadUSB, zostają uznane za zautoryzowane po zainstalowaniu modułu Ochrona przed atakami BadUSB.

Jak włączyć lub wyłączyć Ochronę przed atakami BadUSB w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona przed atakami BadUSB**.
4. Użyj pola **Ochrona przed atakami BadUSB**, aby włączyć lub wyłączyć komponent.
5. W sekcji **Autoryzacja urządzenia USB po jego podłączeniu** dostosuj ustawienia ochrony do wprowadzenia kodu autoryzacyjnego:
   - **Maksymalna liczba prób autoryzacji urządzenia USB**. Automatyczne blokowanie urządzenia USB, jeśli kod autoryzacyjny jest wprowadzany niepoprawnie określoną liczbę. Ważne wartości to 1 do 10. Na przykład, jeśli zezwolisz na pięć prób wprowadzenia kodu autoryzacyjnego, aplikacja zablokuje urządzenie USB po piątej nieudanej próbie. Kaspersky Endpoint Security wyświetla czas blokowania dla urządzenia USB. Po upływie tego czasu możliwe będzie podjęcie pięciu prób wprowadzenia kodu autoryzacyjnego.
   - **Limit czasu po osiągnięciu maksymalnej liczby prób (minuty)**. Czas trwania blokady urządzenia USB po określonej liczbie nieudanych prób wprowadzenia kodu autoryzacyjnego. Ważne wartości to 1 do 180 (minuty).
6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć Ochronę przed atakami BadUSB w Web Console i Cloud Console?

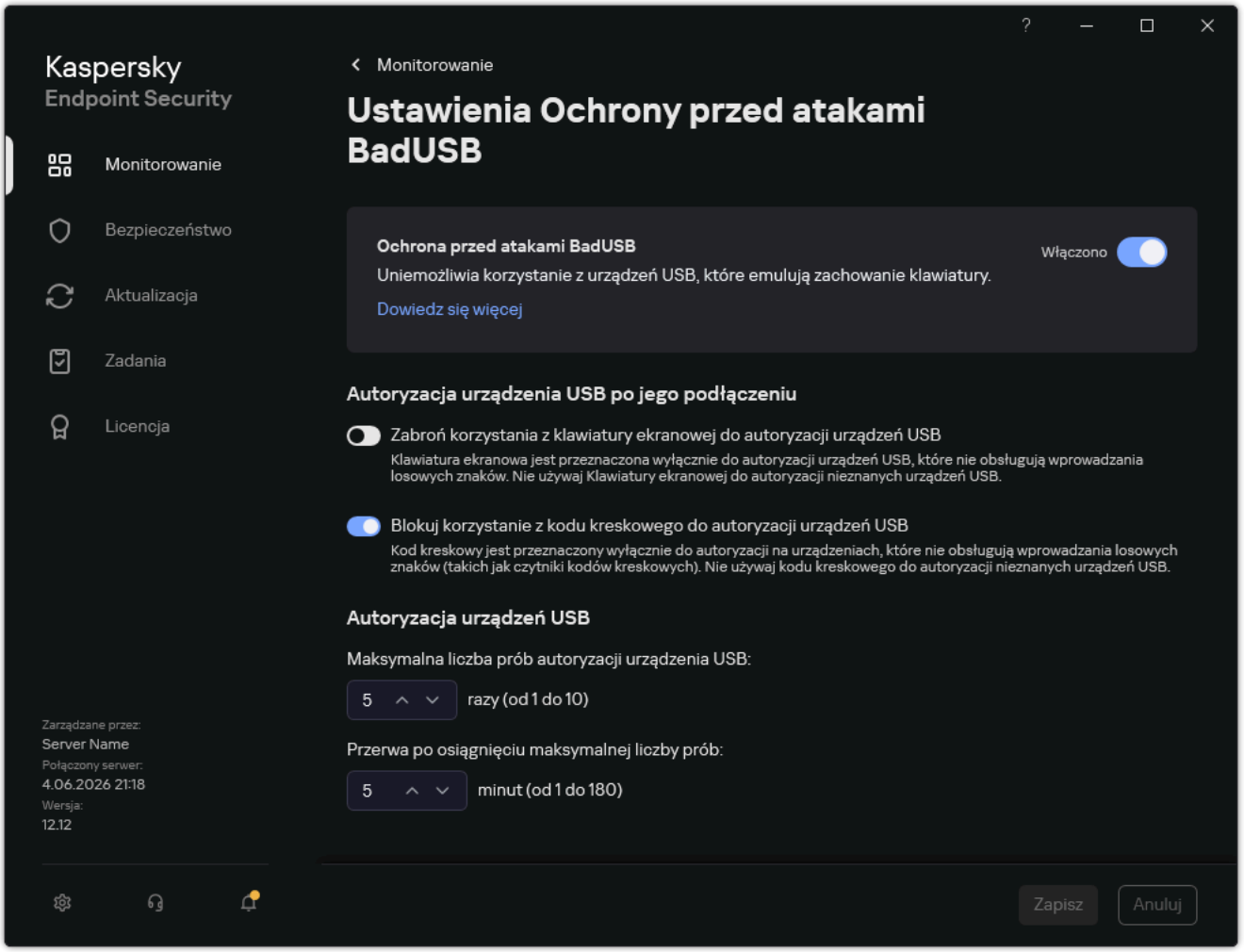
1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta → Ochrona przed atakami BadUSB**.
5. Użyj przełącznika **Ochrona przed atakami BadUSB WŁĄCZONA**, aby włączyć lub wyłączyć komponent.
6. W sekcji **Autoryzacja urządzeń USB** dostosuj ustawienia ochrony do wprowadzenia kodu autoryzacyjnego:
   - **Maksymalna liczba prób autoryzacji urządzenia USB**. Automatyczne blokowanie urządzenia USB, jeśli kod autoryzacyjny jest wprowadzany niepoprawnie określoną liczbę. Ważne wartości to 1 do 10. Na przykład, jeśli zezwolisz na pięć prób wprowadzenia kodu autoryzacyjnego, aplikacja zablokuje urządzenie USB po piątej nieudanej próbie. Kaspersky Endpoint Security wyświetla czas blokowania dla urządzenia USB. Po upływie tego czasu możliwe będzie podjęcie pięciu prób wprowadzenia kodu autoryzacyjnego.
   - **Limit czasu po osiągnięciu maksymalnej liczby prób (min)**. Czas trwania blokady urządzenia USB po określonej liczbie nieudanych prób wprowadzenia kodu autoryzacyjnego. Ważne wartości to 1 do 180 (minuty).
7. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć Ochronę przed atakami BadUSB w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona przed atakami BadUSB**.



Ustawienia komponentu Ochrona przed atakami BadUSB

3. Użyj przełącznika **Ochrona przed atakami BadUSB**, aby włączyć lub wyłączyć komponent.

4. W sekcji **Autoryzacja urządzenia USB po jego podłączeniu** dostosuj ustawienia ochrony do wprowadzenia kodu autoryzacyjnego:

   - **Maksymalna liczba prób autoryzacji urządzenia USB**. Automatyczne blokowanie urządzenia USB, jeśli kod autoryzacyjny jest wprowadzany niepoprawnie określoną liczbę. Ważne wartości to 1 do 10. Na przykład, jeśli zezwolisz na pięć prób wprowadzenia kodu autoryzacyjnego, aplikacja zablokuje urządzenie USB po piątej nieudanej próbie. Kaspersky Endpoint Security wyświetla czas blokowania dla urządzenia USB. Po upływie tego czasu możliwe będzie podjęcie pięciu prób wprowadzenia kodu autoryzacyjnego.

   - **Przerwa po osiągnięciu maksymalnej liczby prób**. Czas trwania blokady urządzenia USB po określonej liczbie nieudanych prób wprowadzenia kodu autoryzacyjnego. Ważne wartości to 1 do 180 (minuty).

5. Zapisz swoje zmiany.

W wyniku tego działania, jeśli Ochrona przed atakami BadUSB jest włączona, Kaspersky Endpoint Security wymaga autoryzacji podłączonego urządzenia USB zidentyfikowanego przez system operacyjny jako klawiatura. Użytkownik może użyć niezautoryzowaną klawiaturę dopiero po jej zautoryzowaniu.

Korzystanie z Klawiatury ekranowej do autoryzacji urządzeń USB

Klawiatura ekranowa powinna być używana tylko do autoryzacji urządzeń USB, które nie obsługują wprowadzania losowych znaków (np. czytniki kodów kreskowych). Nie jest zalecane korzystanie z klawiatury ekranowej do autoryzacji nieznanych urządzeń USB.

Jak zezwolić na korzystanie lub zabronić korzystania z klawiatury ekranowej w celu autoryzacji w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona przed atakami BadUSB**.
4. Aby zablokować użycie lub zezwolić na użycie klawiatury ekranowej do autoryzacji, użyj pola **Zabroń korzystania z klawiatury ekranowej do autoryzacji urządzeń USB**.
5. Zapisz swoje zmiany.

Jak zezwolić na korzystanie lub zabronić korzystania z klawiatury ekranowej w celu autoryzacji w Web Console i Cloud Console?

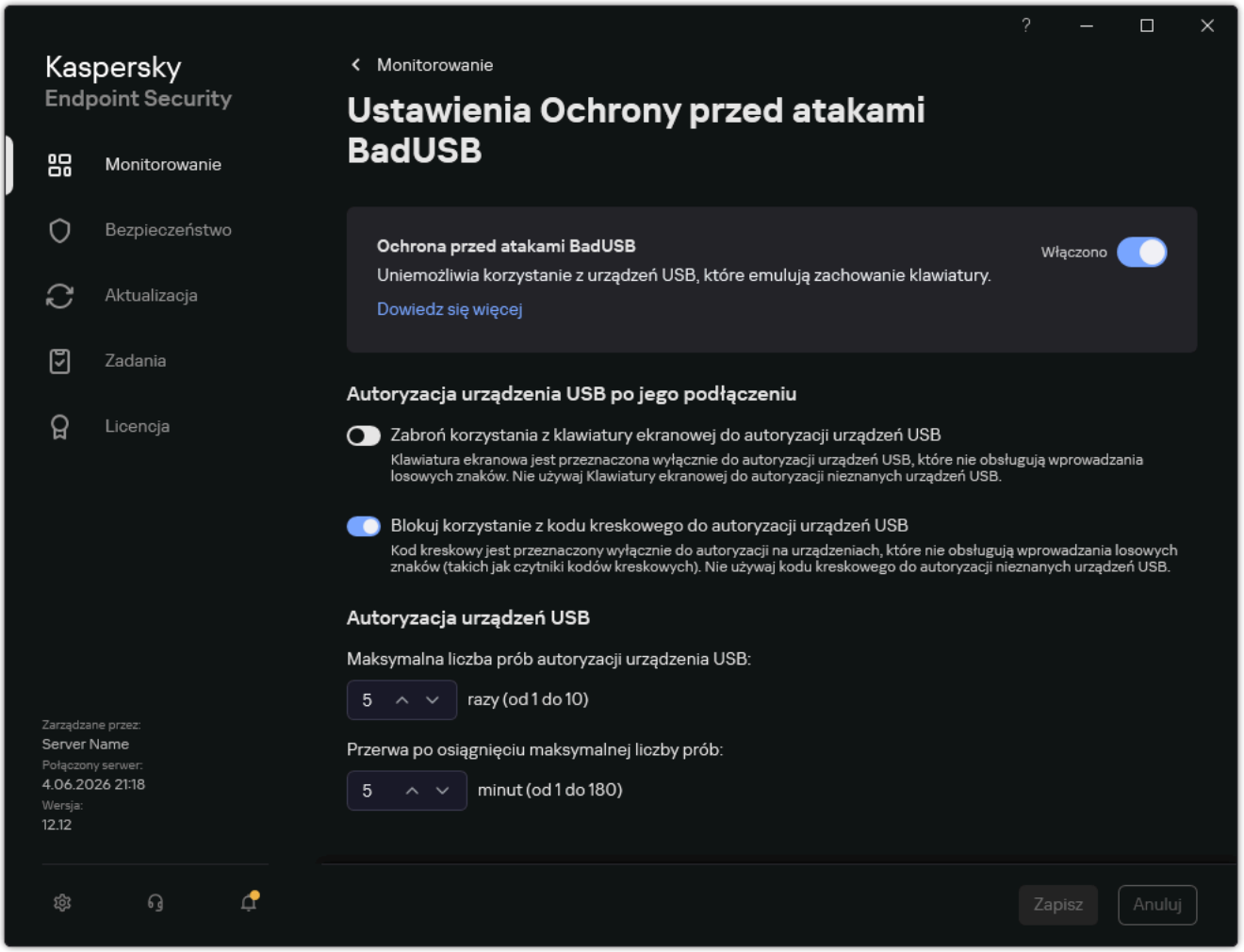
1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta → Ochrona przed atakami BadUSB**.
5. Aby zablokować użycie lub zezwolić na użycie klawiatury ekranowej do autoryzacji, użyj pola **Zabroń korzystania z klawiatury ekranowej do autoryzacji urządzeń USB**.
6. Zapisz swoje zmiany.

Jak zezwolić na korzystanie lub zabronić korzystania z klawiatury ekranowej w celu autoryzacji w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

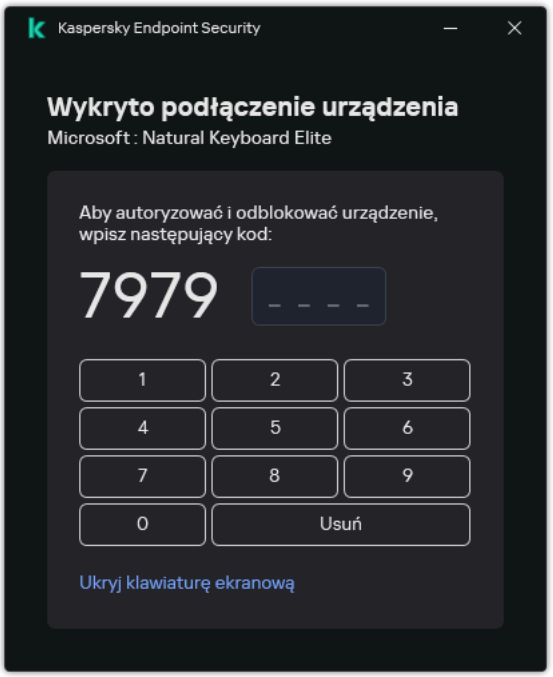
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona przed atakami BadUSB**.



Ustawienia komponentu Ochrona przed atakami BadUSB

3. Aby zablokować użycie lub zezwolić na użycie klawiatury ekranowej do autoryzacji, użyj pola **Zabroń korzystania z klawiatury ekranowej do autoryzacji urządzeń USB**.

4. Zapisz swoje zmiany.



Autoryzacja urządzeń USB

Autoryzacja czytnika kodów kreskowych

Po podłączeniu czytnika kodów kreskowych do komputera komponent Ochrona przed atakami BadUSB identyfikuje to urządzenie jako urządzenie wejściowe i wyświetla monit o przeprowadzenie autoryzacji. Aby autoryzować czytnik kodów kreskowych, należy zeskanować kod kreskowy wyświetlany na ekranie. Aplikacja generuje kod kreskowy w formacie Code39 obsługiwanym przez większość czytników kodów kreskowych i kodów QR.

Kaspersky Endpoint Security obsługuje również inną metodę autoryzacji czytnika kodów kreskowych. Jeśli używasz urządzenia z ekranem dotykowym, możesz wpisać kod za pomocą klawiatury ekranowej. Aby to zrobić, musisz zezwolić na używanie klawiatury ekranowej. Metoda ta jest wygodna np. w przypadku stacjonarnych czytników kodów kreskowych wbudowanych w kasy fiskalne. Inne metody autoryzacji czytnika kodów kreskowych są zabronione.

Domyślnie aplikacja nie używa kodu kreskowego do autoryzacji urządzeń USB.

Jak zezwolić na autoryzację urządzenia USB za pomocą kodu kreskowego w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W drzewie konsoli wybierz **Zasady**.

3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

4. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona przed atakami BadUSB**.

5. Aby zablokować użycie lub zezwolić na użycie kodów kreskowych do autoryzacji, użyj pola **Blokuj korzystanie z kodu kreskowego do autoryzacji urządzeń USB**.

6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak zezwolić na autoryzację urządzenia USB za pomocą kodu kreskowego w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ochrona hosta** → **Ochrona przed atakami BadUSB**.

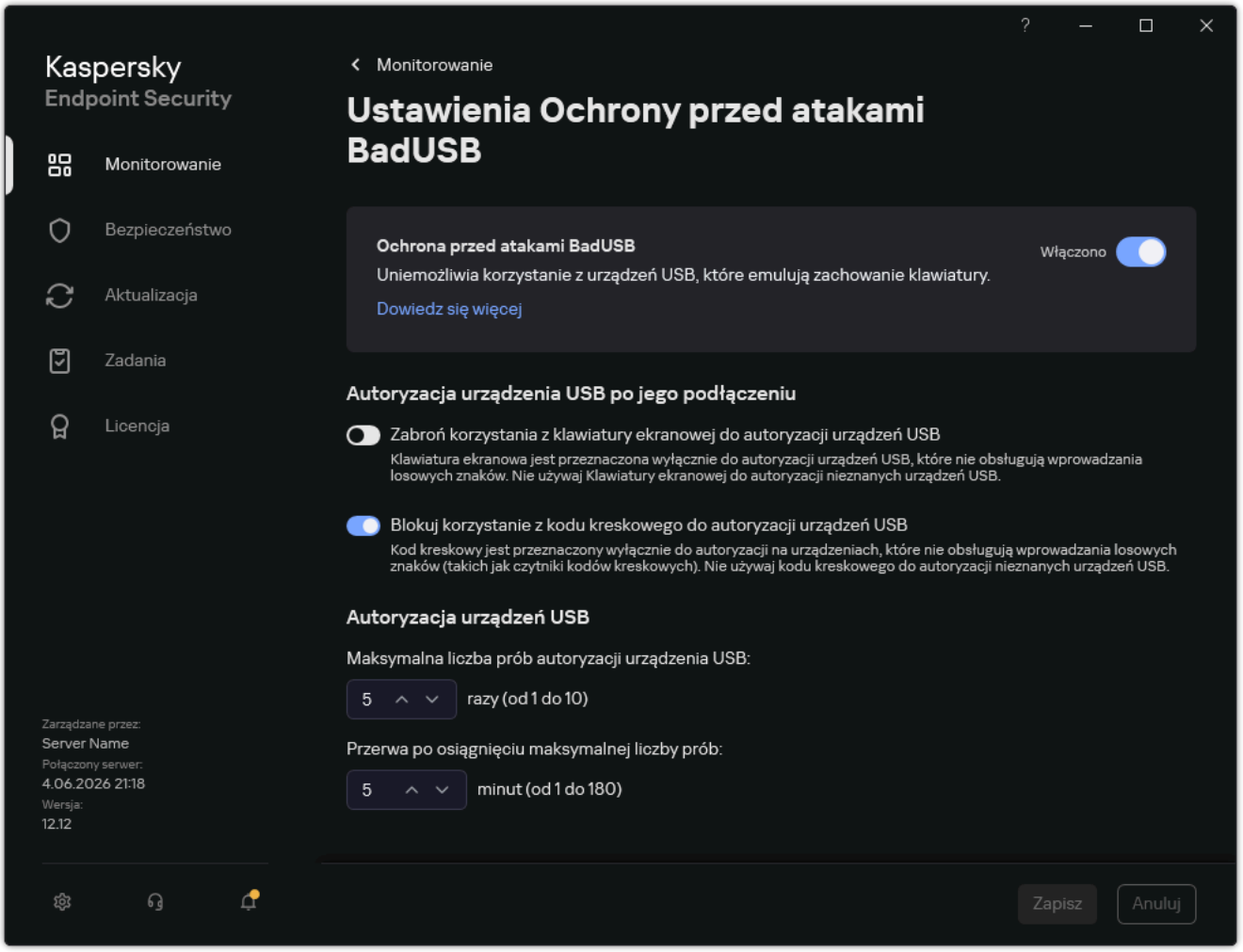
5. Aby zablokować użycie lub zezwolić na użycie kodów kresowych do autoryzacji, użyj przełącznika **Blokuj korzystanie z kodu kreskowego do autoryzacji urządzeń USB**.

6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak zezwolić na autoryzację urządzenia USB za pomocą kodu kreskowego w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .

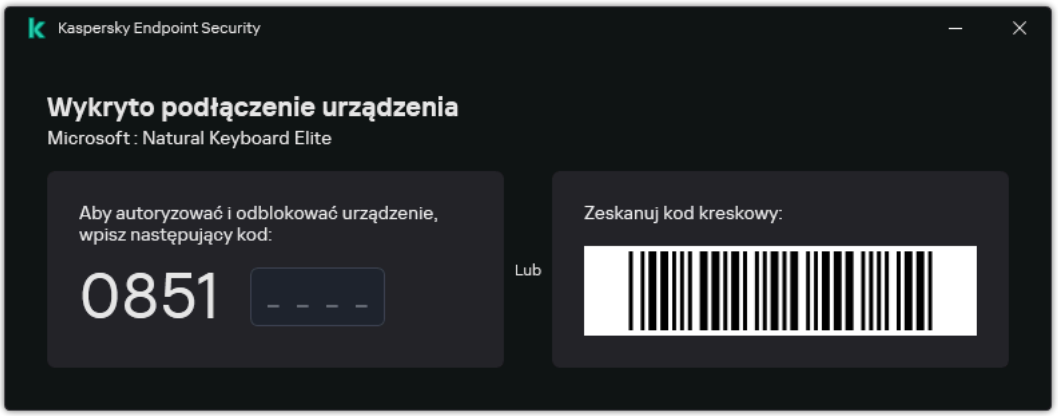
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona przed atakami BadUSB**.



Ustawienia komponentu Ochrona przed atakami BadUSB

3. Aby zablokować użycie lub zezwolić na użycie kodów kresowych do autoryzacji, użyj przełącznika **Blokuj korzystanie z kodu kreskowego do autoryzacji urządzeń USB**.

4. Zapisz swoje zmiany.

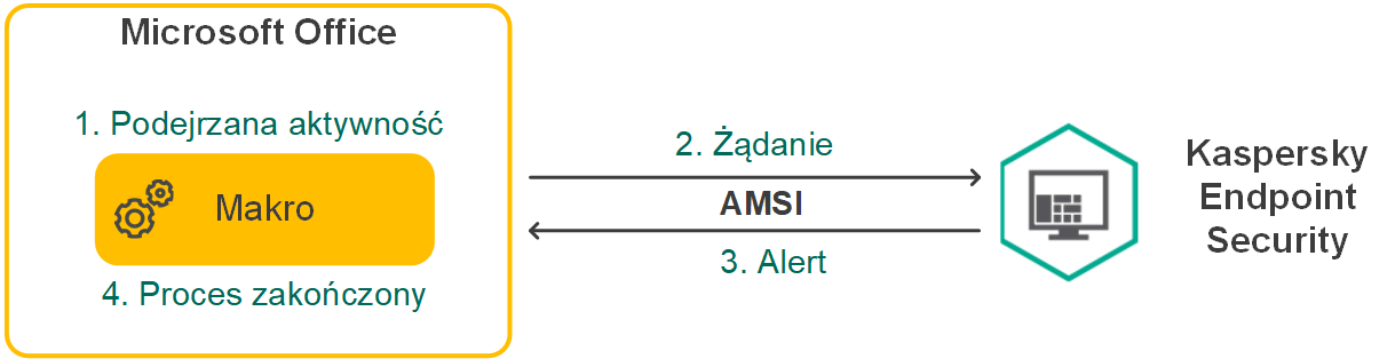


Autoryzacja czytnika kodów kreskowych

Ochrona AMSI

Komponent Ochrona AMSI jest przeznaczony do obsługi Antimalware Scan Interface firmy Microsoft. *Antimalware Scan Interface (AMSI)* umożliwia aplikacjom firm trzecich z obsługą AMSI wysyłanie obiektów (na przykład, skryptów PowerShell) do Kaspersky Endpoint Security w celu przeprowadzenia dodatkowego skanowania i otrzymania wyników ze skanowania tych obiektów. Aplikacje firm trzecich mogą obejmować, na przykład, aplikacje Microsoft Office (patrz rysunek poniżej). Więcej informacji na temat AMSI znajdziesz w dokumentacji firmy Microsoft.

Ochrona AMSI może tylko wykrywać zagrożenia i informować aplikację firmy trzeciej o wykrytym zagrożeniu. Aplikacja zewnętrzna, po odebraniu powiadomienia o zagrożeniu, nie zezwala na wykonanie szkodliwych działań (na przykład kończy proces).



Przykład działania AMSI

Komponent Ochrona AMSI może odrzucić żądanie z aplikacji firmy trzeciej, na przykład, jeśli ta aplikacja przekracza maksymalną liczbę żądań w określonym przedziale czasu. Kaspersky Endpoint Security wyśle informacje o odrzuconym żądaniu z aplikacji firmy trzeciej do Serwera administracyjnego. Komponent Ochrona AMSI nie zablokuje żądań od tych aplikacji firm trzecich, dla których jest włączona trwała integracja z komponentem Ochrona AMSI.

Ochrona AMSI jest dostępny dla następujących systemów operacyjnych dla stacji roboczych i serwerów:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise wielosesyjny
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter (w tym tryb Server Core)
- Windows Server 2019 Essentials / Standard / Datacenter (w tym tryb Server Core)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (w tym tryb Server Core)
- Windows Server 2025 Standard / Datacenter

Włączanie i wyłączanie Ochrony AMSI

Domyślnie Ochrona AMSI jest włączona i działa w trybie zalecanym przez Kaspersky (patrz tabela poniżej).

Jak włączyć lub wyłączyć Ochronę AMSI w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Skaner AMSI**.
4. Użyj pola **Skaner AMSI**, aby włączyć lub wyłączyć komponent.
5. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

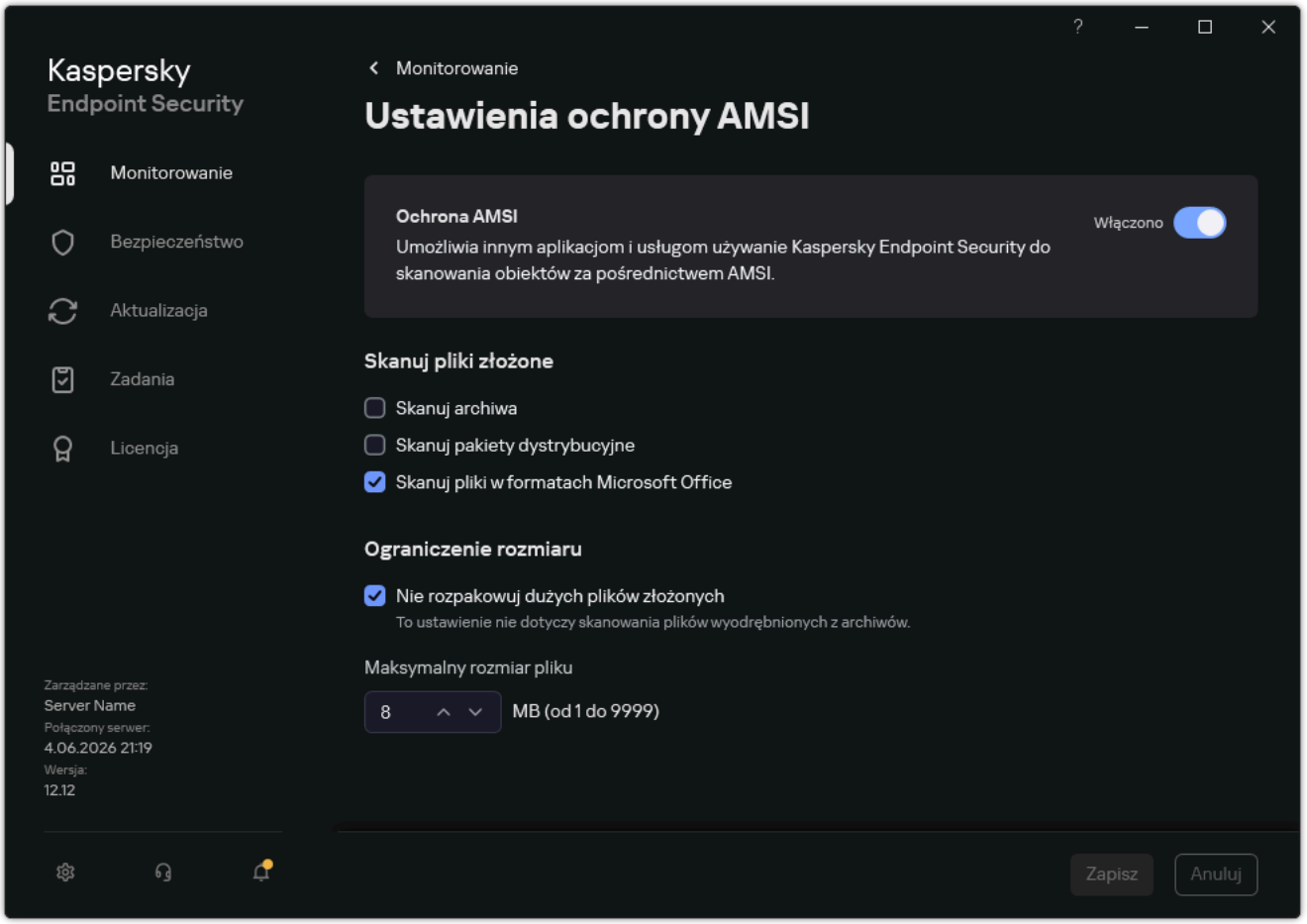
Jak włączyć lub wyłączyć Ochronę AMSI w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Ochrona AMSI**.
5. Użyj przełącznika **Ochrona AMSI WŁĄCZONA**, aby włączyć lub wyłączyć komponent.
6. Zapisz swoje zmiany. Aby zastosować zasady na komputerach, zamknij kłódki .

Jak włączyć lub wyłączyć Ochronę AMSI w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona AMSI**.



Ustawienia Ochrony AMSI

3. Użyj przełącznika **Ochrona AMSI**, aby włączyć lub wyłączyć komponent.

4. Zapisz swoje zmiany.

Ustawienia Ochrony AMSI zalecane przez ekspertów Kaspersky

Parametr	Wartość	Opis
Skanuj archiwa	**Wyłączono**	Skanowanie ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE i innych archiwów. Aplikacja skanuje archiwa nie tylko według rozszerzenia, ale także według formatu. Podczas sprawdzania archiwów aplikacja przeprowadzi cykliczne rozpakowywanie. Pozwala to na wykrywanie zagrożeń w archiwach wielopoziomowych (archiwach wewnątrz archiwów).
Skanuj pakiety dystrybucyjne	**Wyłączono**	Skanowanie pakietów dystrybucyjnych aplikacji firm trzecich.
Skanuj pliki w formatach Microsoft Office	**Włączono**	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty. Aplikacja skanuje pliki w formacie Office, które są mniejsze niż 1 MB, niezależnie od tego, czy pole wyboru jest zaznaczone, czy nie.
Nie rozpakowuj dużych plików złożonych	**Maksymalny rozmiar pliku 8 MB**	Jeżeli to pole jest zaznaczone, aplikacja nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość. Jeśli pole nie jest zaznaczone, aplikacja skanuje pliki złożone o wszystkich rozmiarach. Aplikacja skanuje pliki o dużych rozmiarach, które zostają wypakowane z archiwów niezależnie od tego, czy pole jest zaznaczone.

Optymalizacja skanowania plików przez Ochronę AMSI

Możesz zoptymalizować skanowanie plików, zmniejszając czas skanowania i zwiększając szybkość działania programu Kaspersky Endpoint Security. Możesz wybrać pliki złożone, które mają zostać zeskanowane: archiwa, pakiety dystrybucyjne lub pliki w formatach biurowych. Możesz również ograniczyć rozmiar plików złożonych, które mają zostać zeskanowane. Komponent Ochrona AMSI nie będzie rozpakowywać plików złożonych, których rozmiar jest większy niż określona wartość.

Popularną techniką ukrywania wirusów i innego szkodliwego oprogramowania jest osadzanie ich w plikach złożonych, takich jak archiwa. W celu wykrycia ukrytych w ten sposób wirusów i innego szkodliwego oprogramowania, plik złożony musi zostać rozpakowany, co może spowolnić skanowanie. Możesz ograniczyć typy skanowanych plików złożonych, dzięki czemu skanowanie będzie szybsze.

Jak zoptymalizować skanowanie plików przez Ochronę AMSI w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Skaner AMSI**.
4. W sekcji **Skanowanie plików złożonych** określ, które pliki złożone mają być skanowane: archiwa, pakiety dystrybucyjne lub pliki w formatach pakietu Office.
5. W sekcji **Ograniczenie rozmiaru** wykonaj jedną z następujących czynności:
   - Aby moduł Ochrona AMSI nie rozpakowywał dużych plików złożonych, zaznacz pole wyboru **Nie rozpakowuj dużych plików złożonych** i określ żądaną wartość. Komponent Ochrona AMSI nie będzie rozpakowywać plików złożonych, których rozmiar jest większy niż określona wartość.
   - Aby moduł Ochrona AMSI rozpakowywał duże pliki złożone, usuń zaznaczenie z pola **Nie rozpakowuj dużych plików złożonych**.

   Komponent Ochrona AMSI skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.
6. Zapisz swoje zmiany. Aby zastosować zasady na komputerach, zamknij kłódki .

Jak zoptymalizować skanowanie plików przez Ochronę AMSI w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta → Ochrona AMSI**.
5. W sekcji **Skanowanie plików złożonych** określ, które pliki złożone mają być skanowane: archiwa, pakiety dystrybucyjne lub pliki w formatach pakietu Office.

6. W sekcji **Optymalizacja skanowania** wykonaj jedną z następujących czynności:

   - Aby moduł Ochrona AMSI nie rozpakowywał dużych plików złożonych, zaznacz pole wyboru **Limity rozmiaru włączone** i określ żądaną wartość. Komponent Ochrona AMSI nie będzie rozpakowywać plików złożonych, których rozmiar jest większy niż określona wartość.

   - Aby moduł Ochrona AMSI rozpakowywał duże pliki złożone, usuń zaznaczenie z pola **Limity rozmiaru włączone**.

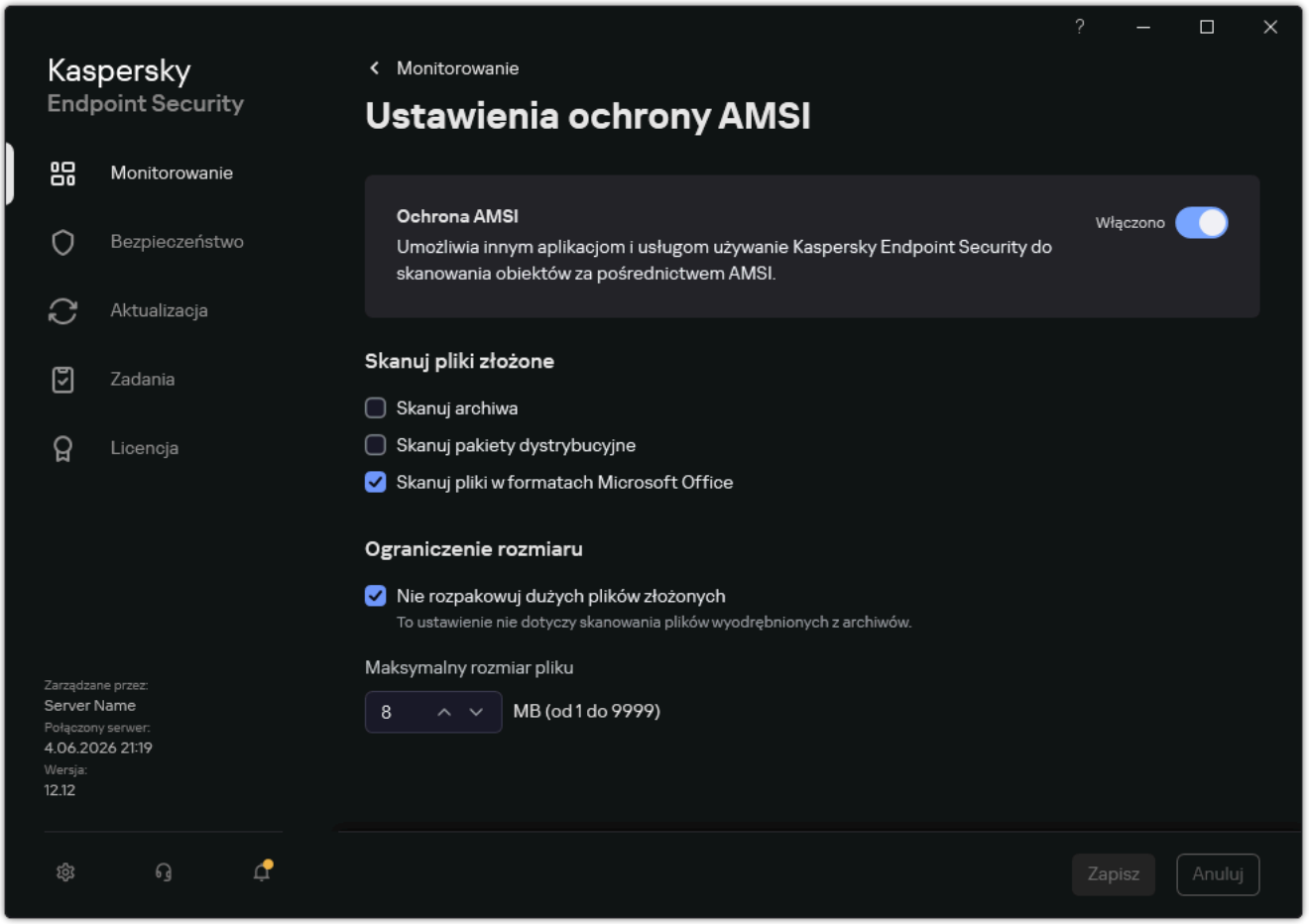
   Komponent Ochrona AMSI skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Limity rozmiaru włączone** jest zaznaczone.

7. Zapisz swoje zmiany. Aby zastosować zasady na komputerach, zamknij kłódki.

Jak zoptymalizować skanowanie plików przez Ochronę AMSI w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona AMSI**.



Ustawienia Ochrony AMSI

3. W sekcji **Skanuj pliki złożone** określ, które pliki złożone mają być skanowane: archiwa, pakiety dystrybucyjne lub pliki w formatach pakietu Office.

4. W sekcji **Ograniczenie rozmiaru** wykonaj jedną z następujących czynności:

   - Aby moduł Ochrona AMSI nie rozpakowywał dużych plików złożonych, zaznacz pole wyboru **Nie rozpakowuj dużych plików złożonych** i określ żądaną wartość. Komponent Ochrona AMSI nie będzie rozpakowywać plików złożonych, których rozmiar jest większy niż określona wartość.

   - Aby moduł Ochrona AMSI rozpakowywał duże pliki złożone, usuń zaznaczenie z pola **Nie rozpakowuj dużych plików złożonych**.

   Komponent Ochrona AMSI skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

5. Zapisz swoje zmiany.

Ochrona WWW

Komponent Ochrona WWW zapobiega pobieraniu szkodliwych plików z internetu, a także blokuje szkodliwe i phishingowe strony internetowe. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej.

Kaspersky Endpoint Security skanuje ruch HTTP, HTTPS i FTP. Kaspersky Endpoint Security skanuje adresy internetowe i adresy IP.

Aby móc korzystać z Ochrony WWW, należy wykonać początkową konfigurację aplikacji:

- Do monitorowania ruchu HTTPS, włącz skanowanie połączeń szyfrowanych (domyślnie włączone).

- Wybierz porty, które musi monitorować Kaspersky Endpoint Security (domyślnie aplikacja monitoruje wszystkie porty).

- Wybierz aplikacje, których ruch ma być monitorowany za pomocą Kaspersky Endpoint Security. Większość przeglądarek znajduje się już na liście aplikacji zalecanych przez Kaspersky. Jeśli Twojej przeglądarki nie ma na liście, dodaj ją ręcznie.

- Zalecamy wstrzyknąć skrypt interakcji ze stroną internetową do ruchu sieciowego (domyślnie wstrzykiwanie skryptów jest wyłączone). Ten skrypt umożliwia rejestrację zdarzeń Ochrony WWW dla dziennika zdarzeń aplikacji, dziennika zdarzeń systemu operacyjnego i raportów.

Gdy użytkownik próbuje otworzyć złośliwą lub phishingową stronę internetową, Kaspersky Endpoint Security zablokuje dostęp i wyświetli ostrzeżenie.

Włączanie i wyłączanie modułu Ochrona WWW

Domyślnie moduł Ochrona WWW jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. Dla modułu Ochrona WWW aplikacja można zastosować różne grupy ustawień. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane *poziomami ochrony*: **Wysoki**, **Zalecany**, **Niski**. Ustawienia **Zalecany** poziomu ochrony ruchu sieciowego są uważane za optymalne ustawienia zalecane przez ekspertów z Kaspersky (patrz poniższa tabela). Możesz wybrać jeden z predefiniowanych poziomów ochrony ruchu sieciowego, odbieranego lub wysyłanego przez protokoły HTTP i FTP, lub skonfigurować niestandardowy poziom ochrony ruchu sieciowego. Jeśli zmienisz ustawienia poziomu ochrony ruchu sieciowego, możesz zawsze powrócić do zalecanych ustawień poziomu ochrony.

Możesz wybrać lub skonfigurować poziom ochrony tylko w Konsoli administracyjnej (MMC) lub lokalnym interfejsie aplikacji. Nie możesz wybrać lub skonfigurować poziomu ochrony w konsoli Web Console lub Cloud Console.

Jak włączyć lub wyłączyć komponent Ochrona WWW w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.
4. Użyj pola **Ochrona WWW**, aby włączyć lub wyłączyć komponent.
5. Jeśli włączyłeś komponent, w sekcji **Poziom ochrony** wykonaj jedną z następujących czynności:
   - Jeśli chcesz zastosować jeden z predefiniowanych poziomów ochrony, wybierz go, korzystając z suwaka:
     - **Wysoki**. Poziom ochrony, zgodnie z którym Ochrona WWW przeprowadza maksymalne skanowanie ruchu sieciowego, odbieranego przez komputer poprzez protokoły HTTP i FTP. Ochrona WWW szczegółowo skanuje wszystkie obiekty ruchu sieciowego, używając pełnego zestawu baz danych aplikacji, a także przeprowadza najbardziej szczegółową analizę heurystyczną.
     - **Zalecany**. Jest to poziom ochrony zapewniający optymalna równowagę pomiędzy wydajnością aplikacji a ochroną ruchu sieciowego. Ochrona WWW wykonuje analizę heurystyczną na średnim poziomie. Ten poziom ochrony ruchu sieciowego jest zalecany przez specjalistów z Kaspersky. Wartości ustawień dla zalecanego poziomu ochrony są dostępne w poniższej tabeli.
     - **Niski**. Ustawienia tego poziomu ochrony ruchu sieciowego zapewniają maksymalną prędkość skanowania ruchu sieciowego. Ochrona WWW wykonuje analizę heurystyczną na niskim poziomie.
   - Jeśli chcesz skonfigurować niestandardowy poziom ochrony, kliknij przycisk **Ustawienia** i zdefiniuj własne ustawienia komponentu.

     Możesz przywrócić wartości predefiniowanych poziomów ochrony, klikając przycisk **Domyślny** w sekcji Domyślny.

6. W sekcji **Działanie po wykryciu zagrożenia** wybierz akcję, wykonywaną przez Kaspersky Endpoint Security po wykryciu szkodliwych obiektów w ruchu sieciowym:

   - **Zablokuj**. Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Ochrona WWW zablokuje dostęp do obiektu i wyświetli komunikat w przeglądarce.

   - **Poinformuj**. Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Kaspersky Endpoint Security pozwala na pobranie tego obiektu na komputer, ale dodaje informacje o zainfekowanym obiekcie do listy aktywnych zagrożeń.

7. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć komponent Ochrona WWW w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Komunikacja i Ochrona WWW** → **Ochrona WWW**.

5. Użyj przełącznika **Ochrona WWW WŁĄCZONA**, aby włączyć lub wyłączyć komponent.

6. W sekcji **Działanie po wykryciu zagrożenia** wybierz akcję, wykonywaną przez Kaspersky Endpoint Security po wykryciu szkodliwych obiektów w ruchu sieciowym:

   - **Zablokuj**. Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Ochrona WWW zablokuje dostęp do obiektu i wyświetli komunikat w przeglądarce.

   - **Zezwól, powiadom albo wezwij do działania (w zależności od systemu operacyjnego)**. Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Kaspersky Endpoint Security pozwala na pobranie tego obiektu na komputer, ale dodaje informacje o zainfekowanym obiekcie do listy aktywnych zagrożeń.

7. Jeśli to konieczne, utwórz listę zaufanych adresów internetowych.

8. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć komponent Ochrona WWW?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.

3. Użyj przełącznika **Ochrona WWW**, aby włączyć lub wyłączyć komponent.

4. Jeśli włączyłeś komponent, w sekcji **Poziom ochrony** wykonaj jedną z następujących czynności:

- Jeśli chcesz zastosować jeden z predefiniowanych poziomów ochrony, wybierz go, korzystając z suwaka:
  - **Wysoki**. Poziom ochrony, zgodnie z którym Ochrona WWW przeprowadza maksymalne skanowanie ruchu sieciowego, odbieranego przez komputer poprzez protokoły HTTP i FTP. Ochrona WWW szczegółowo skanuje wszystkie obiekty ruchu sieciowego, używając pełnego zestawu baz danych aplikacji, a także przeprowadza najbardziej szczegółową analizę heurystyczną.
  - **Zalecany**. Jest to poziom ochrony zapewniający optymalna równowagę pomiędzy wydajnością aplikacji a ochroną ruchu sieciowego. Ochrona WWW wykonuje analizę heurystyczną na średnim poziomie. Ten poziom ochrony ruchu sieciowego jest zalecany przez specjalistów z Kaspersky. Wartości ustawień dla zalecanego poziomu ochrony są dostępne w poniższej tabeli.
  - **Niski**. Ustawienia tego poziomu ochrony ruchu sieciowego zapewniają maksymalną prędkość skanowania ruchu sieciowego. Ochrona WWW wykonuje analizę heurystyczną na niskim poziomie.
- Jeśli chcesz skonfigurować niestandardowy poziom ochrony, kliknij przycisk **Ustawienia zaawansowane** i zdefiniuj własne ustawienia składnika.

  Możesz przywrócić wartości predefiniowanych poziomów ochrony, klikając przycisk **Domyślny** w sekcji Przywróć zalecany poziom ochrony.

5. W sekcji **Działanie po wykryciu zagrożenia** wybierz akcję, wykonywaną przez Kaspersky Endpoint Security po wykryciu szkodliwych obiektów w ruchu sieciowym:

- **Blokuj**. Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Ochrona WWW zablokuje dostęp do obiektu i wyświetli komunikat w przeglądarce.
- **Poinformuj**. Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Kaspersky Endpoint Security pozwala na pobranie tego obiektu na komputer, ale dodaje informacje o zainfekowanym obiekcie do listy aktywnych zagrożeń.

6. Zapisz swoje zmiany.

Ustawienia Ochrony WWW zalecane przez ekspertów z Kaspersky (zalecany poziom ochrony)

Parametr	Wartość	Opis
Sprawdź adres internetowy w bazie danych szkodliwych adresów internetowych	**Włączono**	Skanowanie odnośników do określenia, czy znajdują się w bazie danych szkodliwych odnośników pozwoli na śledzenie stron internetowych, które zostały dodane do listy zablokowanych. Baza danych szkodliwych adresów internetowych, która została stworzona przez Kaspersky, znajduje się w pakiecie instalacyjnym aplikacji i jest aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.
Sprawdź adres internetowy w bazie danych phishingowych adresów internetowych	**Włączono**	Baza danych phishingowych adresów internetowych zawiera adresy internetowe obecnie znanych stron wykorzystywanych przy atakach phishingowych. Kaspersky uzupełnia tę bazę odnośników phishingowych o adresy uzyskane z międzynarodowej organizacji znanej jako Anti-Phishing Working Group. Baza danych adresów phishingowych znajduje się w pakiecie instalacyjnym aplikacji, jest również aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.
Użyj analizy heurystycznej (Ochrona WWW)	**Poziom średni**	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa. Jeśli ruch sieciowy jest skanowany w poszukiwaniu wirusów i innych aplikacji, które stwarzają zagrożenie, analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.

Parametr	Wartość	Opis
Użyj analizy heurystycznej (Anti-Phishing)	**Włączono**	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa.
Działanie po wykryciu zagrożenia	**Blokuj**	Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Ochrona WWW zablokuje dostęp do obiektu i wyświetli komunikat w przeglądarce.

Konfigurowanie metod wykrywania szkodliwych adresów internetowych

Ochrona WWW wykrywa szkodliwe adresy internetowe przy użyciu antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej.

Możesz wybrać metody wykrywania szkodliwych adresów internetowych tylko w Konsoli administracyjnej (MMC) lub lokalnym interfejsie aplikacji. Nie możesz wybrać metod wykrywania szkodliwych adresów internetowych w konsoli Web Console lub Cloud Console. Domyślna opcja to sprawdzanie adresów internetowych w bazie danych szkodliwych adresów z użyciem analizy heurystycznej (średni poziom skanowania).

Skanowanie z użyciem baz danych szkodliwych adresów

Skanowanie odnośników do określenia, czy znajdują się w bazie danych szkodliwych odnośników pozwoli na śledzenie stron internetowych, które zostały dodane do listy zablokowanych. Baza danych szkodliwych adresów internetowych, która została stworzona przez Kaspersky, znajduje się w pakiecie instalacyjnym aplikacji i jest aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.

Kaspersky Endpoint Security skanuje wszystkie odnośniki, aby określić, czy znajdują się w bazie danych szkodliwych adresów internetowych. Ustawienia skanowania bezpiecznego połączenia aplikacji nie wpływają na funkcjonalność skanowania odnośników. Innymi słowy, jeśli skanowanie połączeń szyfrowanych jest wyłączone, Kaspersky Endpoint Security sprawdza odnośniki w bazach danych szkodliwych adresów internetowych nawet wtedy, gdy ruch sieciowy jest przesyłany poprzez połączenie szyfrowane.

Jak włączyć lub wyłączyć sprawdzanie adresów internetowych w bazie danych szkodliwych adresów internetowych przy użyciu Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.
4. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

5. W otwartym oknie, w sekcji **Metody skanowania** zaznacz lub odznacz pole **Sprawdź adres internetowy w bazie danych szkodliwych adresów internetowych**, aby włączyć lub wyłączyć sprawdzanie adresów w bazie danych szkodliwych adresów internetowych.

6. Zapisz swoje zmiany.

Jak w interfejsie aplikacji włączyć lub wyłączyć sprawdzanie adresów w bazie danych szkodliwych adresów?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.

3. Kliknij **Ustawienia zaawansowane**.

4. W sekcji **Metody skanowania** zaznacz lub odznacz pole **Sprawdź adres internetowy w bazie danych szkodliwych adresów internetowych**, aby włączyć lub wyłączyć sprawdzanie adresów w bazie danych szkodliwych adresów internetowych.

5. Zapisz swoje zmiany.

Analiza heurystyczna

Podczas analizy heurystycznej Kaspersky Endpoint Security analizuje aktywność aplikacji w systemie operacyjnym. Analiza heurystyczna może wykryć zagrożenia, dla których nie ma wpisów w bazach danych Kaspersky Endpoint Security.

Jeśli ruch sieciowy jest skanowany w poszukiwaniu wirusów i innych aplikacji, które stwarzają zagrożenie, analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.

Jak w Konsoli administracyjnej (MMC) włączyć lub wyłączyć analizę heurystyczną?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.

4. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

5. W oknie, które się otworzy, w sekcji **Metody skanowania** zaznacz pole **Użyj analizy heurystycznej**, jeśli chcesz, żeby aplikacja używała analizy heurystycznej podczas skanowania ruchu sieciowego pod kątem wirusów i innych szkodliwych programów.

6. Użyj suwaka, aby ustawić poziom analizy heurystycznej: **poziom niski**, **poziom średni** lub **poziom szczegółowy**.

   Jeśli ruch sieciowy jest skanowany w poszukiwaniu wirusów i innych aplikacji, które stwarzają zagrożenie, analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.

7. Zapisz swoje zmiany.

Jak w interfejsie aplikacji włączyć lub wyłączyć użycie analizy heurystycznej?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona WWW**.

3. Kliknij **Ustawienia zaawansowane**.

4. W sekcji **Metody skanowania** zaznacz pole **Użyj analizy heurystycznej**, jeśli chcesz, żeby aplikacja używała analizy heurystycznej podczas skanowania ruchu sieciowego pod kątem wirusów i innych szkodliwych programów.

   Jeśli ruch sieciowy jest skanowany w poszukiwaniu wirusów i innych aplikacji, które stwarzają zagrożenie, analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.

5. Zapisz swoje zmiany.

Anti-Phishing

Ochrona WWW sprawdza odnośniki, aby zobaczyć, czy należą do phishingowych adresów internetowych. To umożliwia zapobieganie *atakom phishingowym*. Atak phishingowy może być zamaskowany, na przykład, pod postacią wiadomości e-mail od banku z odsyłaczem do oficjalnej strony WWW banku. Po kliknięciu odnośnika zostaje otwarta strona internetowa przypominająca tę należącą do danej instytucji finansowej. W rzeczywistości jednak znajdziesz się na spreparowanej stronie. Od tego momentu wszystkie Twoje działania są śledzone i mogą zostać użyte do kradzieży pieniędzy.

Odnośniki do stron typu phishing mogą być otrzymywane zarówno za pomocą poczty elektronicznej, jak również z innych zasobów, takich jak komunikatory. Z tego powodu moduł Ochrona WWW monitoruje próby dostępu do stron phishingowych na poziomie ruchu sieciowego oraz blokuje dostęp do takich stron. Lista adresów phishingowych znajduje się w pakiecie dystrybucyjnym programu Kaspersky Endpoint Security.

Możesz skonfigurować moduł Anti-Phishing tylko w Konsoli administracyjnej (MMC) lub w lokalnym interfejsie aplikacji. Nie możesz skonfigurować modułu Anti-Phishing w konsoli Web Console lub Cloud Console. Domyślnie, moduł Anti-Phishing jest włączony z analizą heurystyczną.

Jak w Konsoli administracyjnej (MMC) włączyć lub wyłączyć moduł Anti-Phishing?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona WWW**.

4. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

5. W otwartym oknie, w sekcji **Ustawienia Anti-Phishing**, należy zaznaczyć lub odznaczyć pole wyboru **Sprawdź adres internetowy w bazie danych phishingowych adresów internetowych**, aby włączyć lub wyłączyć opcję Anti-Phishing.

   Baza danych phishingowych adresów internetowych zawiera adresy internetowe obecnie znanych stron wykorzystywanych przy atakach phishingowych. Kaspersky uzupełnia tę bazę odnośników phishingowych o adresy uzyskane z międzynarodowej organizacji znanej jako Anti-Phishing Working Group. Baza danych adresów phishingowych znajduje się w pakiecie instalacyjnym aplikacji, jest również aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.

6. Zaznacz pole **Użyj analizy heurystycznej**, jeśli chcesz, żeby aplikacja używała analizy heurystycznej podczas skanowania stron internetowych pod kątem odnośników phishingowych.

   Podczas analizy heurystycznej Kaspersky Endpoint Security analizuje aktywność aplikacji w systemie operacyjnym. Analiza heurystyczna może wykryć zagrożenia, dla których nie ma wpisów w bazach danych Kaspersky Endpoint Security.

   Aby skanować odnośniki, oprócz antywirusowej bazy danych i analizy heurystycznej możesz użyć bazy danych reputacji Kaspersky Security Network.

7. Zapisz swoje zmiany.

Jak w interfejsie aplikacji włączyć lub wyłączyć moduł Anti-Phishing?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona WWW**.

3. Kliknij **Ustawienia zaawansowane**.

4. Jeśli chcesz, żeby komponent Ochrona WWW sprawdzał odnośniki w bazach danych phishingowych adresów internetowych, w sekcji **Anti-Phishing** zaznacz pole **Sprawdź adres internetowy w bazie danych phishingowych adresów internetowych**. Baza danych phishingowych adresów internetowych zawiera adresy internetowe obecnie znanych stron wykorzystywanych przy atakach phishingowych. Kaspersky uzupełnia tę bazę odnośników phishingowych o adresy uzyskane z międzynarodowej organizacji znanej jako Anti-Phishing Working Group. Baza danych adresów phishingowych znajduje się w pakiecie instalacyjnym aplikacji, jest również aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.

5. Zaznacz pole **Użyj analizy heurystycznej**, jeśli chcesz, żeby aplikacja używała analizy heurystycznej podczas skanowania stron internetowych pod kątem odnośników phishingowych.

   Podczas analizy heurystycznej Kaspersky Endpoint Security analizuje aktywność aplikacji w systemie operacyjnym. Analiza heurystyczna może wykryć zagrożenia, dla których nie ma wpisów w bazach danych Kaspersky Endpoint Security.

   Aby skanować odnośniki, oprócz antywirusowej bazy danych i analizy heurystycznej możesz użyć bazy danych reputacji Kaspersky Security Network.

6. Zapisz swoje zmiany.

Tworzenie listy zaufanych adresów internetowych

Oprócz szkodliwych i phishingowych stron internetowych, Ochrona WWW może blokować inne strony internetowe. Na przykład, Ochrona WWW blokuje ruch http, który nie spełnia standardów RFC. Możesz utworzyć listę adresów internetowych, którym ufasz co do zawartości. Ochrona WWW nie sprawdza informacji pochodzących od zaufanych adresów internetowych w poszukiwaniu wirusów i innych zagrożeń. Ta opcja może być użyteczna, na przykład, gdy moduł nie pozwala na pobranie pliku ze znanej strony internetowej.

Adres internetowy może być adresem konkretnej strony internetowej lub witryny.

Zmiana listy zaufanych adresów sieciowych może zostać zablokowana przez właściwości zasady nadrzędnej. Aby zmienić listę, musisz zezwolić na zmianę ustawień strefy zaufanej w Web Console (kłódka musi być odblokowana).

Strefy zaufane są grupowane w różny sposób w Konsoli administracyjnej (MMC) i Web Console. Sposoby zapobiegania zmianom parametrów strefy zaufanej również mogą się różnić („kłódki" mogą być inne). Zalecamy korzystanie wyłącznie z Web Console do zarządzania aplikacją. Jeśli skonfigurujesz strefę zaufaną w różnych konsolach, wtyczka zarządzająca może przywrócić „kłódkę" do stanu domyślnego.

Jak dodawać zaufane adresy internetowe przy użyciu Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.
4. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
5. W otwartym oknie wybierz zakładkę **Zaufane adresy internetowe**.
6. Zaznacz pole **Nie skanuj ruchu sieciowego z zaufanych adresów internetowych**.

   Jeśli ta opcja jest zaznaczona, moduł Ochrona WWW nie skanuje zawartości stron internetowych lub stron, których adresy znajdują się na liście zaufanych adresów internetowych. Do listy zaufanych adresów internetowych możesz dodać określony adres i maskę adresu strony internetowej.
7. Utwórz listę adresów internetowych / stron internetowych, którym ufasz co do zawartości.

   Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski.

   Możesz także zaimportować listę zaufanych adresów internetowych z pliku XML.
8. Zapisz swoje zmiany.

Jak dodać zaufany adres internetowy w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Komunikacja i Ochrona WWW** → **Ochrona WWW**.
5. Kliknij **Zaufane adresy internetowe**.
6. Utwórz listę adresów internetowych / stron internetowych, którym ufasz co do zawartości.

   Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski.

   Możesz także zaimportować listę zaufanych adresów internetowych z pliku JSON.
7. Zapisz swoje zmiany.

Jak dodać zaufany adres internetowy w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.
3. Kliknij **Ustawienia zaawansowane**.
4. Zaznacz pole **Nie skanuj ruchu sieciowego z zaufanych adresów internetowych**.

   Jeśli ta opcja jest zaznaczona, moduł Ochrona WWW nie skanuje zawartości stron internetowych lub stron, których adresy znajdują się na liście zaufanych adresów internetowych. Do listy zaufanych adresów internetowych możesz dodać określony adres i maskę adresu strony internetowej.
5. Utwórz listę adresów internetowych / stron internetowych, którym ufasz co do zawartości.

   Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski.

   Możesz także zaimportować listę zaufanych adresów internetowych z pliku XML.
6. Zapisz swoje zmiany.

W wyniku tego działania Ochrona WWW nie skanuje ruchu internetowego zaufanych adresów internetowych. Użytkownik zawsze może otworzyć zaufaną stronę internetową i pobrać plik z tej strony internetowej. Jeśli nie możesz uzyskać dostępu do strony internetowej, sprawdź ustawienia komponentów Skanowanie połączeń szyfrowanych, Kontrola sieci i Monitorowanie portów sieciowych. Jeśli Kaspersky Endpoint Security wykryje plik pobrany z zaufanych stron internetowych jako szkodliwy, możesz dodać ten plik do wykluczeń.

Możesz także utworzyć ogólną listę wykluczeń dla połączeń szyfrowanych. W tym przypadku program Kaspersky Endpoint Security nie skanuje ruchu sieciowego HTTPS zaufanych adresów internetowych, gdy komponenty Ochrona WWW, Ochrona poczty, Kontrola sieci wykonują swoją pracę.

Eksportowanie i importowanie listy zaufanych adresów internetowych

Możesz wyeksportować listę zaufanych adresów internetowych do pliku XML. Następnie możesz zmodyfikować plik, na przykład, dodać dużą liczbę adresów internetowych tego samego typu. Możesz także użyć funkcji eksportowania/importowania w celu utworzenia kopii zapasowej listy zaufanych adresów internetowych lub w celu przeniesienia listy na inny serwer.

Eksportowanie i importowanie listy zaufanych adresów sieciowych w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.
4. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
5. W otwartym oknie wybierz zakładkę **Zaufane adresy internetowe**.
6. W celu utworzenia listy zaufanych adresów internetowych:
   a. Wybierz zaufane adresy internetowe, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.

      Jeśli nie wybrałeś żadnego zaufanego adresu internetowego, Kaspersky Endpoint Security wyeksportuje wszystkie adresy internetowe.

   b. Kliknij odnośnik **Eksportuj**.
   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę zaufanych adresów internetowych, wybierz folder, w którym chcesz zapisać ten plik.
   d. Zapisz plik.

      Kaspersky Endpoint Security wyeksportuje całą listę zaufanych adresów internetowych do pliku XML.
7. W celu zaimportowania listy zaufanych adresów:
   a. Kliknij odnośnik **Importuj**.

      W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę zaufanych adresów.

   b. Otwórz plik.

      Jeśli komputer ma już listę zaufanych adresów, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
8. Zapisz swoje zmiany.

Eksportowanie i importowanie listy zaufanych adresów internetowych w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Komunikacja i Ochrona WWW** → **Ochrona WWW**.
5. W celu wyeksportowania listy wykluczeń w sekcji **Lista reguł**:

   a. Wybierz zaufane adresy internetowe, które chcesz wyeksportować.

   b. Kliknij przycisk → **Eksportuj**.

   Kaspersky Endpoint Security eksportuje listę zaufanych adresów internetowych do pliku JSON w domyślnym folderze Pobrane.
6. W celu zaimportowania listy wykluczeń w sekcji **Lista reguł**:

   a. Kliknij przycisk → **Importuj**.

   W oknie, które zostanie otwarte, wybierz plik JSON, z którego chcesz zaimportować listę zaufanych adresów.

   b. Otwórz plik.

   Jeśli komputer ma już listę zaufanych adresów, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku JSON.
7. Zapisz swoje zmiany.

Ochrona poczty

Ochrona poczty skanuje załączniki odbieranych i wysyłanych wiadomości e-mail w poszukiwaniu wirusów i innych zagrożeń. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej.

Ochrona poczty może skanować zarówno wiadomości odbierane, jak i wysyłane. Aplikacja obsługuje protokoły POP3, SMTP, IMAP i NNTP w następujących klientach pocztowych:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail

- MyOffice Mail
- R7-Office Organizer

Aby skanować ruch w klientach pocztowych Mozilla Thunderbird, MyOffice Mail i R7-Office Organizer, musisz dodać certyfikat Kaspersky do magazynu certyfikatów oraz wybrać własny magazyn certyfikatów.

Ochrona poczty nie obsługuje innych protokołów i klientów pocztowych.

Ochrona poczty może nie zawsze być w stanie zyskać dostęp do wiadomości na *poziomie protokołu* (na przykład podczas korzystania z rozwiązania Microsoft Exchange). Z tego powodu Ochrona poczty obejmuje rozszerzenie dla programu Microsoft Office Outlook. Rozszerzenie umożliwia skanowanie wiadomości na *poziomie klienta pocztowego*. Rozszerzenie Ochrony poczty obsługuje 32- i 64-bitowe wersje programów Outlook 2010, 2013, 2016, 2019, 2021, 2024 i 365. Na komputerach opartych na architekturze Arm rozszerzenie Ochrony poczty obsługuje 32- i 64-bitowe wersje programów Outlook 2016, Outlook 2021, Outlook 2024 i Outlook 365 dla architektury Arm64.

Komponent Ochrona poczty nie skanuje wiadomości, jeśli klient poczty jest otwarty w przeglądarce.

Gdy w załączniku zostanie wykryty szkodliwy plik, Kaspersky Endpoint Security dodaje informację o wykonanej akcji do tematu wiadomości, na przykład: *[Wiadomość została przetworzona] <temat wiadomości>*.

Włączanie i wyłączanie modułu Ochrona poczty

Domyślnie moduł Ochrona poczty jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. Dla modułu Ochrona poczty aplikacja może zastosować różne grupy ustawień. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane *poziomami ochrony*: **Wysoki**, **Zalecany**, **Niski**. Ustawienia **Zalecany** poziomu ochrony poczty są uważane za optymalne ustawienia zalecane przez ekspertów z Kaspersky (patrz poniższa tabela). Możesz wybrać jeden z predefiniowanych poziomów ochrony poczty lub skonfigurować niestandardowy poziom ochrony poczty. Jeśli zmieniono ustawienia poziomu ochrony poczty, możesz zawsze powrócić do zalecanych ustawień poziomu ochrony poczty.

Podczas pracy z programem Mozilla Thunderbird moduł Ochrona poczty nie skanuje w poszukiwaniu wirusów i innych zagrożeń wiadomości przesyłanych poprzez protokół IMAP, jeśli filtry są wykorzystywane do przenoszenia wiadomości z folderu Skrzynka odbiorcza.

Jak włączyć lub wyłączyć Ochronę poczty w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
4. Użyj pola **Ochrona poczty**, aby włączyć lub wyłączyć komponent.

5. Jeśli włączyłeś komponent, w sekcji **Poziom ochrony** wykonaj jedną z następujących czynności:

   - Jeśli chcesz zastosować jeden z predefiniowanych poziomów ochrony, wybierz go, korzystając z suwaka:

     - **Wysoki**. Jeśli wybrany jest ten poziom ochrony, moduł Ochrona poczty szczegółowo skanuje wiadomości e-mail. Ochrona poczty skanuje przychodzące i wychodzące wiadomości e-mail, a także przeprowadza szczegółową analizę heurystyczną. Wysoki poziom ochrony poczty jest zalecany dla środowisk wysokiego ryzyka. Przykładem takiego środowiska jest korzystanie z darmowego serwera pocztowego, który nie jest chroniony żadnym systemem antywirusowym.

     - **Zalecany**. Jest to poziom ochrony zapewniający optymalną równowagę pomiędzy wydajnością aplikacji a ochroną poczty. Ochrona poczty skanuje wiadomości przychodzące i wychodzące, a także przeprowadza analizę heurystyczną na średnim poziomie intensywności. Ten poziom ochrony ruchu pocztowego jest zalecany przez specjalistów z Kaspersky. Wartości ustawień dla zalecanego poziomu ochrony są dostępne w poniższej tabeli.

     - **Niski**. Jeśli wybrany jest ten poziom ochrony, moduł Ochrona poczty skanuje tylko wiadomości przychodzące, wykonuje analizę heurystyczną na niskim poziomie, a także nie skanuje archiwów załączonych do wiadomości e-mail. Na tym poziomie moduł Ochrona poczty skanuje wiadomości z maksymalną prędkością i używa minimalnej ilości zasobów systemu operacyjnego. Niski poziom ochrony jest zalecany podczas pracy w dobrze chronionym środowisku. Przykładem takiego środowiska może być firmowa sieć LAN ze scentralizowaną ochroną poczty.

   - Jeśli chcesz skonfigurować niestandardowy poziom ochrony, kliknij przycisk **Ustawienia** i zdefiniuj własne ustawienia komponentu.

     Możesz przywrócić wartości predefiniowanych poziomów ochrony, klikając przycisk **Domyślny** w sekcji Domyślny.

6. W sekcji **Działanie po wykryciu zagrożenia** wybierz akcję, wykonywaną przez Kaspersky Endpoint Security po wykryciu szkodliwych obiektów:

   - **Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej lub wychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, aplikacja usunie zainfekowany obiekt. Aplikacja doda informacje o wykonanym działaniu do tematu wiadomości, na przykład: *[Przetworzono wiadomość] <temat wiadomości>*.

   - **Wylecz; blokuj, jeśli leczenie nie jest możliwe**. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, aplikacja doda ostrzeżenie do tematu wiadomości. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Jeśli obiektu nie można wyleczyć, aplikacja zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.

   - **Zablokuj**. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, aplikacja doda ostrzeżenie do tematu wiadomości. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, aplikacja zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.

7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć Ochronę poczty w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Komunikacja i Ochrona WWW** → **Ochrona poczty**.
5. Użyj przełącznika **Ochrona poczty WŁĄCZONA**, aby włączyć lub wyłączyć komponent.
6. W sekcji **Działanie po wykryciu zagrożenia** wybierz akcję, wykonywaną przez Kaspersky Endpoint Security po wykryciu szkodliwych obiektów:

   - **Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej lub wychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, aplikacja usunie zainfekowany obiekt. Aplikacja doda informacje o wykonanym działaniu do tematu wiadomości, na przykład: *[Przetworzono wiadomość] <temat wiadomości>*.

   - **Wylecz; blokuj, jeśli leczenie nie jest możliwe**. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, aplikacja doda ostrzeżenie do tematu wiadomości. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Jeśli obiektu nie można wyleczyć, aplikacja zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.

   - **Zablokuj**. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, aplikacja doda ostrzeżenie do tematu wiadomości. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, aplikacja zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.
7. W razie potrzeby edytuj zaawansowane ustawienia Ochrony poczty.
8. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć Ochronę poczty w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
3. Użyj przełącznika **Ochrona poczty**, aby włączyć lub wyłączyć komponent.

4. Jeśli włączyłeś komponent, w sekcji **Poziom ochrony** wykonaj jedną z następujących czynności:

   - Jeśli chcesz zastosować jeden z predefiniowanych poziomów ochrony, wybierz go, korzystając z suwaka:

     - **Wysoki**. Jeśli wybrany jest ten poziom ochrony, moduł Ochrona poczty szczegółowo skanuje wiadomości e-mail. Ochrona poczty skanuje przychodzące i wychodzące wiadomości e-mail, a także przeprowadza szczegółową analizę heurystyczną. Wysoki poziom ochrony poczty jest zalecany dla środowisk wysokiego ryzyka. Przykładem takiego środowiska jest korzystanie z darmowego serwera pocztowego, który nie jest chroniony żadnym systemem antywirusowym.

     - **Zalecany**. Jest to poziom ochrony zapewniający optymalną równowagę pomiędzy wydajnością aplikacji a ochroną poczty. Ochrona poczty skanuje wiadomości przychodzące i wychodzące, a także przeprowadza analizę heurystyczną na średnim poziomie intensywności. Ten poziom ochrony ruchu pocztowego jest zalecany przez specjalistów z Kaspersky. Wartości ustawień dla zalecanego poziomu ochrony są dostępne w poniższej tabeli.

     - **Niski**. Jeśli wybrany jest ten poziom ochrony, moduł Ochrona poczty skanuje tylko wiadomości przychodzące, wykonuje analizę heurystyczną na niskim poziomie, a także nie skanuje archiwów załączonych do wiadomości e-mail. Na tym poziomie moduł Ochrona poczty skanuje wiadomości z maksymalną prędkością i używa minimalnej ilości zasobów systemu operacyjnego. Niski poziom ochrony jest zalecany podczas pracy w dobrze chronionym środowisku. Przykładem takiego środowiska może być firmowa sieć LAN ze scentralizowaną ochroną poczty.

   - Jeśli chcesz skonfigurować niestandardowy poziom ochrony, kliknij przycisk **Ustawienia zaawansowane** i zdefiniuj własne ustawienia składnika.

     Możesz przywrócić wartości predefiniowanych poziomów ochrony, klikając przycisk **Domyślny** w sekcji Przywróć zalecany poziom ochrony.

5. W sekcji **Działanie po wykryciu zagrożenia** wybierz akcję, wykonywaną przez Kaspersky Endpoint Security po wykryciu szkodliwych obiektów:

   - **Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej lub wychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, aplikacja usunie zainfekowany obiekt. Aplikacja doda informacje o wykonanym działaniu do tematu wiadomości, na przykład: *[Przetworzono wiadomość] <temat wiadomości>*.

   - **Wylecz; blokuj, jeśli leczenie nie jest możliwe**. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, aplikacja doda ostrzeżenie do tematu wiadomości. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Jeśli obiektu nie można wyleczyć, aplikacja zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.

   - **Blokuj**. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, aplikacja doda ostrzeżenie do tematu wiadomości. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, aplikacja zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.

6. Zapisz swoje zmiany.

Ustawienia Ochrony poczty zalecane przez ekspertów z Kaspersky (zalecany poziom ochrony)

Parametr	Wartość	Opis
Obszar ochrony	**Wiadomości odbierane i wysyłane**	*Obszar ochrony* zawiera obiekty, które komponent sprawdza podczas działania: wiadomości odbierane i wysyłane lub tylko wiadomości przychodzące. Aby chronić komputery, należy skanować tylko wiadomości przychodzące. Możesz włączyć skanowanie wiadomości wychodzących, aby zapobiec wysłaniu zainfekowanych plików w archiwach. Możesz także włączyć skanowanie wiadomości wychodzących, jeśli chcesz zapobiec wysłaniu plików w określonych formatach, na przykład plików audio i wideo.
Włącz rozszerzenie Microsoft Outlook	**Włączono**	Jeśli pole jest zaznaczone, skanowanie wiadomości przesyłanych poprzez protokoły POP3, SMTP, NNTP, IMAP jest włączone po stronie rozszerzenia zintegrowanego w Microsoft Outlook. Jeśli poczta jest skanowana przy użyciu rozszerzenia dla programu Microsoft Outlook, zalecane jest korzystanie z Cached Exchange Mode. Więcej informacji dotyczących trybu buforowanego programu Exchange oraz zalecenia dotyczące korzystania z tego trybu można znaleźć w Bazie wiedzy Microsoft.
Skanuj załączone archiwa	**Włączono**	Skanowanie ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE i innych archiwów. Aplikacja skanuje archiwa nie tylko według rozszerzenia, ale także według formatu. Podczas sprawdzania archiwów aplikacja przeprowadzi cykliczne rozpakowywanie. Pozwala to na wykrywanie zagrożeń w archiwach wielopoziomowych (archiwach wewnątrz archiwów).
Skanuj załączone pliki w formatach Microsoft Office	**Włączono**	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty. Aplikacja skanuje pliki w formacie Office, które są mniejsze niż 1 MB, niezależnie od tego, czy pole wyboru jest zaznaczone, czy nie.
Filtr załączników	**Zmień nazwy załączników określonych typów**	Jeśli wybierzesz tę opcję, Ochrona poczty zastąpi ostatni znak rozszerzenia wykryty w załączonych plikach określonych typów znakiem podkreślenia (na przykład: attachment.doc_). Dlatego, aby otworzyć plik, użytkownik musi zmienić jego nazwę.
Analiza heurystyczna	**Poziom średni**	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa. Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.
Działanie po wykryciu zagrożenia	**Wylecz; usuń, jeśli leczenie nie jest możliwe**	Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej lub wychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, aplikacja usunie zainfekowany obiekt. Aplikacja doda informacje o wykonanym działaniu do tematu wiadomości, na przykład: *[Przetworzono wiadomość] <temat wiadomości>*.

Zmienianie akcji podejmowanej na zainfekowanych wiadomościach e-mail

Domyślnie, Ochrona poczty automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych wiadomości, które zostały wykryte. Jeśli leczenie nie powiedzie się, komponent Ochrona poczty usuwa zainfekowane wiadomości e-mail.

W celu zmiany akcji podejmowanej na zainfekowanych wiadomościach e-mail:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.

3. W sekcji **Działanie po wykryciu zagrożenia** wybierz akcję, jaką Kaspersky Endpoint Security wykona po wykryciu zainfekowanej wiadomości:

   - **Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej lub wychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, aplikacja usunie zainfekowany obiekt. Aplikacja doda informacje o wykonanym działaniu do tematu wiadomości, na przykład: *[Przetworzono wiadomość] <temat wiadomości>*.

   - **Wylecz; blokuj, jeśli leczenie nie jest możliwe**. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, aplikacja doda ostrzeżenie do tematu wiadomości. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Jeśli obiektu nie można wyleczyć, aplikacja zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.

   - **Blokuj**. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, aplikacja doda ostrzeżenie do tematu wiadomości. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, aplikacja zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.

4. Zapisz swoje zmiany.

Tworzenie obszaru ochrony modułu Ochrona poczty

Obszar ochrony odnosi się do obiektów, które są skanowane przez komponent, gdy jest on aktywny. Obszary ochrony różnych modułów mają odmienne właściwości. Właściwości obszaru ochrony modułu Ochrona poczty zawierają ustawienia integracji Ochrony poczty z klientami poczty oraz typy wiadomości pocztowych i protokołów pocztowych, których ruch jest skanowany przez Ochronę poczty. Domyślnie, Kaspersky Endpoint Security skanuje przychodzące i wychodzące wiadomości pocztowe oraz ruch przesyłany przez protokoły POP3, SMTP, NNTP i IMAP, integruje się również z klientem poczty Microsoft Office Outlook.

W celu utworzenia obszaru ochrony modułu Ochrona poczty:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona poczty**.

3. Kliknij **Ustawienia zaawansowane**.

4. W sekcji **Obszar ochrony** wybierz wiadomości, które będą skanowane:

   - **Wiadomości odbierane i wysyłane**.

   - **Tylko wiadomości przychodzące**.

   Aby chronić komputery, należy skanować tylko wiadomości przychodzące. Możesz włączyć skanowanie wiadomości wychodzących, aby zapobiec wysłaniu zainfekowanych plików w archiwach. Możesz także włączyć skanowanie wiadomości wychodzących, jeśli chcesz zapobiec wysłaniu plików w określonych formatach, na przykład plików audio i wideo.

Jeśli wybierzesz opcję skanowania tylko wiadomości odbieranych, zalecane jest przeprowadzenie jednorazowego skanowania wszystkich wiadomości wychodzących, aby sprawdzić, czy na Twoim komputerze nie ma robaków pocztowych, rozpowszechnianych za pośrednictwem wiadomości e-mail. Pozwoli to uniknąć problemów wynikających z niekontrolowanego wysyłania masowych, zainfekowanych wiadomości z Twojego komputera.

5. W sekcji **Łączność** wykonaj następujące czynności:

   - Jeśli chcesz, aby Ochrona poczty skanowała wiadomości pocztowe przesyłane poprzez protokoły POP3, SMTP, NNTP i IMAP zanim dotrą one na komputer użytkownika, zaznacz pole **Skanuj ruch POP3, SMTP, NNTP i IMAP**.

     Jeśli nie chcesz, aby Ochrona poczty skanowała wiadomości pocztowe przesyłane poprzez protokoły POP3, SMTP, NNTP i IMAP zanim dotrą one na komputer użytkownika, usuń zaznaczenie z pola **Skanuj ruch POP3, SMTP, NNTP i IMAP**. W tym przypadku wiadomości są skanowane przez rozszerzenie Ochrony poczty osadzone w programie pocztowym Microsoft Office Outlook po dotarciu na komputer użytkownika, jeśli zaznaczone jest pole **Włącz rozszerzenie Microsoft Outlook**.

     Jeśli korzystasz z klienta poczty innego niż Microsoft Office Outlook, komponent Ochrona poczty nie skanuje wiadomości przesyłanych poprzez protokoły POP3, SMTP, NNTP i IMAP, jeśli pole **Skanuj ruch POP3, SMTP, NNTP i IMAP** nie jest zaznaczone.

   - Jeśli chcesz umożliwić dostęp do ustawień Ochrony poczty z poziomu Microsoft Office Outlook i włączyć skanowanie wiadomości pocztowych przesyłanych poprzez protokoły POP3, SMTP, NNTP, IMAP i MAPI po ich odebraniu na komputerze przez wtyczkę wbudowaną w Microsoft Office Outlook, zaznacz pole **Włącz rozszerzenie Microsoft Outlook**.

     Jeśli chcesz zablokować dostęp do ustawień Ochrony poczty z poziomu Microsoft Office Outlook i wyłączyć skanowanie wiadomości pocztowych przesyłanych poprzez protokoły POP3, SMTP, NNTP, IMAP i MAPI po ich odebraniu na komputerze przez wtyczkę wbudowaną w Microsoft Office Outlook, usuń zaznaczenie z pola **Włącz rozszerzenie Microsoft Outlook**.

     Rozszerzenie Ochrony poczty jest integrowane z programem pocztowym Microsoft Office Outlook w trakcie instalacji Kaspersky Endpoint Security.

6. Zapisz swoje zmiany.

Skanowanie plików złożonych załączonych do wiadomości e-mail

Możesz włączyć lub wyłączyć skanowanie załączników w wiadomościach, ograniczyć maksymalny rozmiar skanowanych załączników, a także ograniczyć maksymalny czas skanowania załączników.

W celu skanowania plików złożonych załączonych do wiadomości e-mail:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona poczty**.
3. Kliknij **Ustawienia zaawansowane**.

4. W sekcji **Skanowanie plików złożonych** skonfiguruj ustawienia skanowania:

   - **Skanuj załączone pliki w formatach Microsoft Office**. Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty. Aplikacja skanuje pliki w formacie Office, które są mniejsze niż 1 MB, niezależnie od tego, czy pole wyboru jest zaznaczone, czy nie.

   - **Skanuj załączone archiwa**. Skanowanie ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE i innych archiwów. Aplikacja skanuje archiwa nie tylko według rozszerzenia, ale także według formatu. Podczas sprawdzania archiwów aplikacja przeprowadzi cykliczne rozpakowywanie. Pozwala to na wykrywanie zagrożeń w archiwach wielopoziomowych (archiwach wewnątrz archiwów).

     Jeżeli podczas skanowania aplikacja wykryje w tekście wiadomości hasło do archiwum, hasło to zostanie wykorzystane do przeskanowania zawartości archiwum w poszukiwaniu szkodliwych aplikacji. W tym przypadku hasło nie zostaje zapisane. Archiwum jest rozpakowywane podczas skanowania. Jeśli podczas rozpakowywania wystąpi błąd aplikacji, można ręcznie usunąć rozpakowane pliki, które są zapisywane w następującej ścieżce: %systemroot%\temp. Pliki mają prefiks PR.

   - **Nie skanuj archiwów większych niż N MB (od 1 do 9999)**. Jeżeli pole jest zaznaczone, moduł Ochrona poczty wyklucza ze skanowania archiwa, załączone do wiadomości, których rozmiar przekracza określoną wartość. Jeżeli pole nie jest zaznaczone, moduł Ochrona poczty skanuje załączone archiwa o dowolnym rozmiarze.

   - **Ogranicz czas sprawdzania archiwów do N sek (od 1 do 9999)**. Jeżeli pole jest zaznaczone, czas skanowania załączonych archiwów jest ograniczony.

5. Zapisz swoje zmiany.

Filtrowanie załączników wiadomości e-mail

Filtr załączników nie jest stosowany do wychodzących wiadomości e-mail.

Szkodliwe aplikacje mogą być rozpowszechniane w postaci załączników w wiadomościach e-mail. Możesz skonfigurować filtrowanie w oparciu o typ załączników wiadomości, aby automatycznie usuwano lub zmieniano nazwy plików określonych typów. Poprzez zmianę nazwy załącznika określonego typu, Kaspersky Endpoint Security może ochronić Twój komputer przed automatycznym wykonaniem szkodliwej aplikacji.

W celu skonfigurowania filtrowania załączników:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.

3. Kliknij **Ustawienia zaawansowane**.

4. W sekcji **Filtr załączników** wykonaj jedną z następujących czynności:

   - **Wyłącz filtrowanie**. Jeśli ta opcja jest wybrana, Ochrona poczty nie filtruje plików załączonych do wiadomości e-mail.

   - **Zmień nazwy załączników określonych typów**. Jeśli wybierzesz tę opcję, Ochrona poczty zastąpi ostatni znak rozszerzenia wykryty w załączonych plikach określonych typów znakiem podkreślenia (na przykład: attachment.doc_). Dlatego, aby otworzyć plik, użytkownik musi zmienić jego nazwę.

   - **Usuń załączniki wybranych typów**. Jeśli ta opcja jest zaznaczona, Ochrona poczty usuwa załączone pliki określonych typów z wiadomości e-mail.

5. Jeśli w poprzednim kroku wybrałeś opcję **Zmień nazwy załączników określonych typów** lub opcję **Usuń załączniki wybranych typów**, zaznacz pola obok odpowiednich typów plików.

6. Zapisz swoje zmiany.

Eksportowanie i importowanie rozszerzeń dla filtrowania załączników

Możesz wyeksportować listę rozszerzeń filtra załączników do pliku XML. Możesz użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy rozszerzeń lub przeniesienia listy na inny serwer.

Eksportowanie i importowanie listy rozszerzeń filtra załączników w Konsoli administracyjnej (MMC)

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Komunikacja i Ochrona WWW** → **Ochrona poczty**.

5. W celu wyeksportowania listy rozszerzeń w sekcji **Filtr załączników**:

   a. Wybierz rozszerzenia, które chcesz wyeksportować.

   b. Kliknij odnośnik **Eksportuj**.

   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę rozszerzeń, i wybierz folder, w którym chcesz zapisać ten plik.

   d. Zapisz plik.

      Kaspersky Endpoint Security wyeksportuje całą listę rozszerzeń do pliku XML.

6. W celu zaimportowania listy rozszerzeń w sekcji **Filtr załączników**:

   a. Kliknij odnośnik **Importuj**.

   b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę rozszerzeń.

c. Otwórz plik.

Jeśli komputer ma już listę rozszerzeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

7. Zapisz swoje zmiany.

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
4. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
5. Spowoduje to otwarcie okna. Wybierz w nim zakładkę **Filtr załączników**.
6. W celu wyeksportowania listy rozszerzeń:
   a. Wybierz rozszerzenia, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
   b. Kliknij odnośnik **Eksportuj**.
   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę rozszerzeń, i wybierz folder, w którym chcesz zapisać ten plik.
   d. Zapisz plik.

   Kaspersky Endpoint Security wyeksportuje całą listę rozszerzeń do pliku XML.
7. W celu zaimportowania listy rozszerzeń:
   a. Kliknij odnośnik **Importuj**.
   b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę rozszerzeń.
   c. Otwórz plik.

   Jeśli komputer ma już listę rozszerzeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
8. Zapisz swoje zmiany.

Skanowanie poczty elektronicznej w programie Microsoft Office Outlook

Podczas instalacji Kaspersky Endpoint Security rozszerzenie Ochrony poczty jest osadzane w kliencie poczty Microsoft Office Outlook (zwany dalej także Outlook). Rozszerzenie umożliwia skanowanie wiadomości na poziomie klienta pocztowego zamiast na poziomie protokołu. Oprócz wiadomości rozszerzenie umożliwia skanowanie obiektów otrzymanych przez interfejs MAPI z repozytoriów Microsoft Exchange (na przykład obiektów w Kalendarzu). To skanowanie odbywa się w kliencie pocztowym.

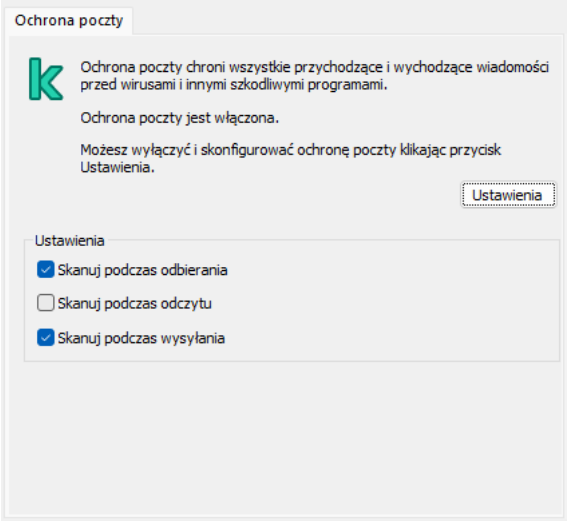
Możesz szybko otwierać ustawienia Ochrony poczty z poziomu programu Outlook, a także określać, kiedy wiadomość ma być skanowana w poszukiwaniu wirusów i innych zagrożeń.

Rozszerzenie Ochrony poczty obsługuje 32- i 64-bitowe wersje programów Outlook 2010, 2013, 2016, 2019, 2021, 2024 i 365.

Na komputerach opartych na architekturze Arm rozszerzenie Ochrony poczty obsługuje 32- i 64-bitowe wersje programów Outlook 2016, Outlook 2021, Outlook 2024 i Outlook 365 dla architektury Arm64.

W programie Outlook wiadomości przychodzące są najpierw skanowane przez Ochronę poczty (jeżeli w interfejsie Kaspersky Endpoint Security zaznaczone jest pole skanuj ruch POP3, SMTP, NNTP i IMAP), a dopiero później przez rozszerzenie Ochrony poczty osadzone w programie Outlook. Jeżeli Ochrona poczty wykryje w wiadomości szkodliwy obiekt, wyświetli odpowiedni komunikat.

Ustawienia Ochrony poczty mogą zostać skonfigurowane bezpośrednio w programie Outlook, jeśli w interfejsie Kaspersky Endpoint Security zaznaczono pole Rozszerzenie Microsoft Outlook zostało podłączone (patrz rysunek poniżej).



Ustawienia komponentu Ochrona poczty w programie Outlook

Wychodzące wiadomości są najpierw skanowane przez rozszerzenie Ochrony poczty osadzone w programie Outlook, a dopiero później przez Ochronę poczty.

Jeśli poczta jest skanowana przy użyciu rozszerzenia Ochrony poczty dla programu Outlook, zalecane jest korzystanie z trybu buforowanego programu Exchange. Więcej informacji dotyczących trybu buforowanego programu Exchange oraz zalecenia dotyczące korzystania z tego trybu można znaleźć w Bazie wiedzy Microsoft.

W celu skonfigurowano tryb działania rozszerzenia modułu Ochrona poczty Outlook:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
4. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.

5. W oknie, które się otworzy, w bloku **Łączność**, kliknij przycisk **Ustawienia**.

6. W oknie **Ochrona poczty** wykonaj następujące czynności:

   - Zaznacz pole **Skanuj podczas odbierania**, jeśli chcesz, żeby rozszerzenie Ochrony poczty dla programu Outlook skanowało wiadomości przychodzące w momencie pojawienia się w skrzynce odbiorczej.
   - Zaznacz pole **Skanuj podczas odczytu**, jeśli chcesz, żeby rozszerzenie Ochrony poczty dla programu Outlook skanowało wiadomości przychodzące w momencie otwarcia ich przez użytkownika.
   - Zaznacz pole **Skanuj podczas wysyłania**, jeśli chcesz, żeby rozszerzenie Ochrony poczty dla programu Outlook skanowało wiadomości wychodzące w momencie ich wysyłania.

7. Zapisz swoje zmiany.

Skanowanie wiadomości e-mail w Thunderbird, MyOffice, R7-Office

Ochrona poczty skanuje załączniki odbieranych i wysyłanych wiadomości e-mail w poszukiwaniu wirusów i innych zagrożeń. W przypadku klientów poczty Mozilla Thunderbird, MyOffice Mail i R7-Office Organizer aplikacja uzyskuje dostęp do wiadomości wyłącznie na *poziomie protokołu* (POP3, SMTP, IMAP, NNTP).

Aby skanować ruch w klientach pocztowych Mozilla Thunderbird, MyOffice Mail i R7-Office Organizer, musisz dodać certyfikat Kaspersky do magazynu certyfikatów oraz wybrać własny magazyn certyfikatów.

Komponent Ochrona poczty nie skanuje wiadomości, jeśli klient poczty jest otwarty w przeglądarce.

Ochrona poczty w czasie rzeczywistym

Ochrona poczty może skanować zarówno wiadomości odbierane, jak i wysyłane. Domyślnie, Ochrona poczty automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych wiadomości, które zostały wykryte. Jeśli leczenie nie powiedzie się, komponent Ochrona poczty usuwa zainfekowane wiadomości e-mail. Gdy w załączniku zostanie wykryty szkodliwy plik, Kaspersky Endpoint Security dodaje informację o wykonanej akcji do tematu wiadomości, na przykład: *[Wiadomość została przetworzona] <temat wiadomości>*.

Podczas pracy z programem Mozilla Thunderbird moduł Ochrona poczty nie skanuje w poszukiwaniu wirusów i innych zagrożeń wiadomości przesyłanych poprzez protokół IMAP, jeśli filtry są wykorzystywane do przenoszenia wiadomości z folderu Skrzynka odbiorcza.

Skanowanie baz danych poczty w poszukiwaniu złośliwego oprogramowania

To zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* zadanie pozwala na skanowanie plików w formacie poczty. Jeśli w plikach tych klientów poczty zostanie wykryty szkodliwy obiekt, Kaspersky Endpoint Security doda informacje o wykrytych obiektach wyłącznie do listy aktywnych zagrożeń. Aplikacja nie leczy ani nie usuwa zainfekowanych plików w bazach danych poczty, niezależnie od ustawień zadania.

Eliminowanie aktywnych zagrożeń

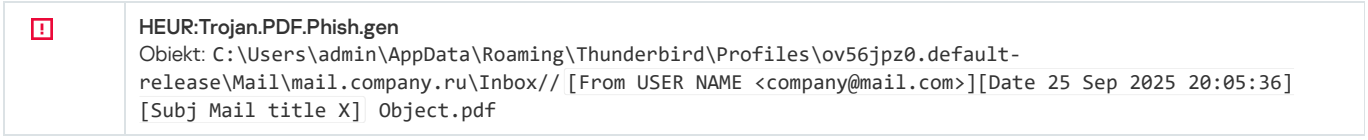
Ochrona poczty zapobiega infekcji komputera na poziomie protokołu, ale jeśli komputer został zainfekowany przed zainstalowaniem Kaspersky Endpoint Security, aplikacja może wykryć zagrożenie jedynie w bazach danych poczty. Ochrona poczty nie obejmuje komponentów, które umożliwiają w szczególności rozłożenie wiadomości na części (nagłówek, treść, załączniki), np. Microsoft Office Outlook. W związku z tym aplikacja nie może usunąć ani wyleczyć wykrytych obiektów. Kaspersky Endpoint Security dodaje do listy aktywnych zagrożeń tylko informacje o wykrytych obiektach.

Aby wyeliminować aktywne zagrożenia:

1. Ręcznie znajdź i usuń wiadomość zawierającą wykryty obiekt w interfejsie klienta poczty.

   Aplikacja dodaje do listy aktywnych zagrożeń informacje o wykrytym obiekcie.

   Przykład karty wykrytego obiektu:

2. Wykonaj operację kompresji bazy danych.

   Po usunięciu wiadomości w interfejsie użytkownika klient poczty dodaje jedynie znacznik usunięcia. Klient poczty faktycznie usuwa wiadomość dopiero po skompresowaniu bazy danych. Aby uzyskać szczegółowe informacje na temat kompresji bazy danych, zapoznaj się z pomocą swojego klienta poczty (na przykład: Mozilla Thunderbird).

3. Uruchom ponownie zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* i upewnij się, że zagrożenie już nie występuje.

Ochrona sieci

Składnik *Ochrona sieci* (zwany także Intrusion Detection System, IDS) monitoruje przychodzący ruch sieciowy pod kątem aktywności charakterystycznej dla ataków sieciowych. Gdy Kaspersky Endpoint Security wykryje próbę ataku sieciowego na komputerze użytkownika, zablokuje połączenie sieciowe z komputerem atakującym. Opisy znanych typów ataków sieciowych oraz sposoby ich zwalczania znajdują się w bazach danych aplikacji. Lista ataków sieciowych, wykrywanych przez komponent Ochrona sieci, jest uaktualniana podczas aktualizacji baz danych i modułów aplikacji.

Włączanie i wyłączanie modułu Ochrona sieci

Domyślnie moduł Ochrona sieci jest włączony i działa w trybie optymalnym. Kaspersky Endpoint Security monitoruje przychodzący ruch sieciowy pod kątem aktywności charakterystycznej dla ataków sieciowych i blokuje te ataki.

Jak włączyć lub wyłączyć Ochronę sieci w Konsoli administracyjnej (MMC)

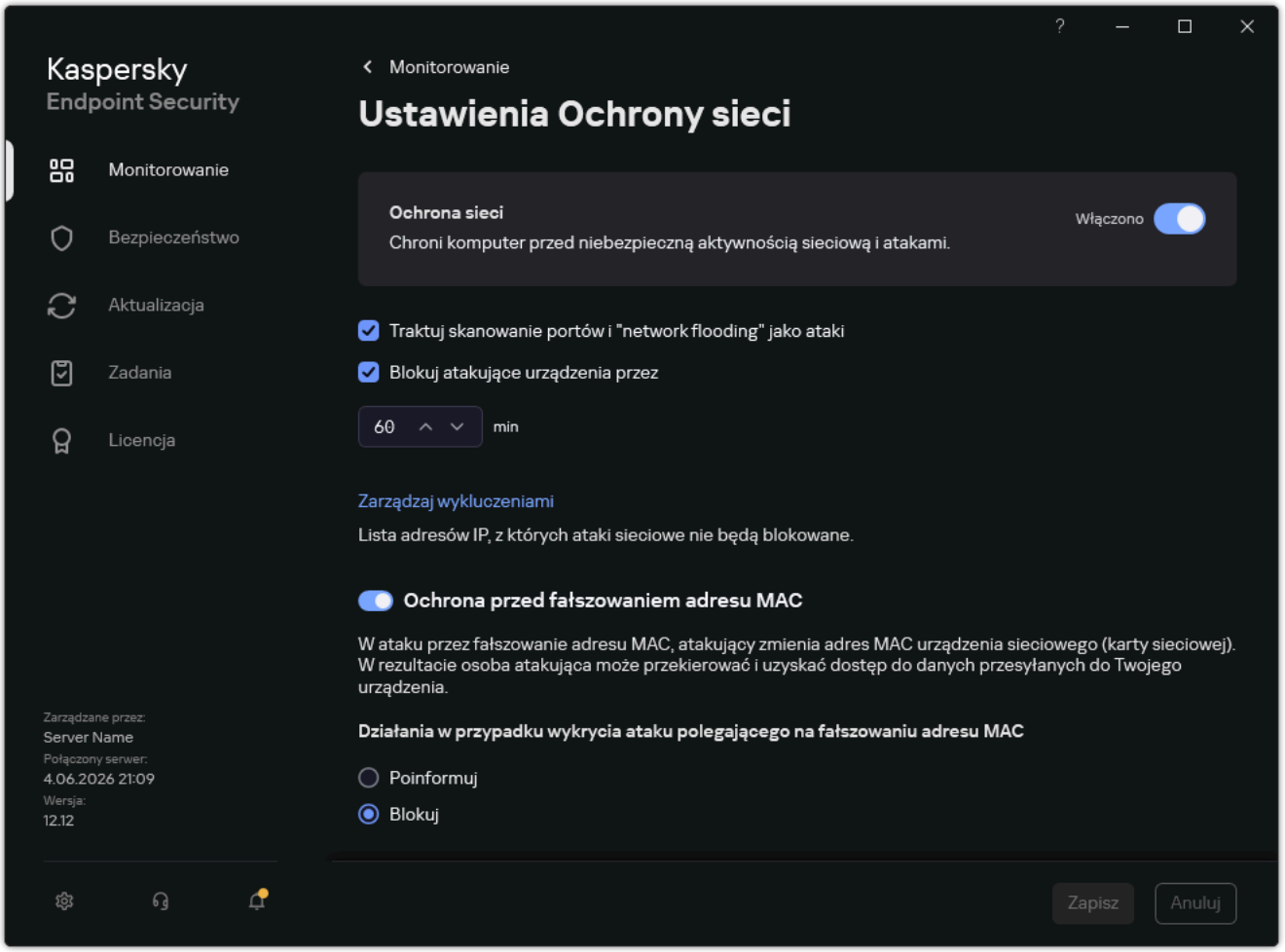
1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona sieci**.
4. Użyj pola **Ochrona sieci**, aby włączyć lub wyłączyć komponent.
5. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć Ochronę sieci w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Komunikacja i Ochrona WWW → Ochrona sieci**.
5. Użyj przełącznika **Ochrona sieci WŁĄCZONA**, aby włączyć lub wyłączyć komponent.
6. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć Ochronę sieci w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona sieci**.



Ustawienia Ochrony sieci

3. Użyj przełącznika **Ochrona sieci**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

Blokowanie atakującego komputera

Jeśli moduł Ochrona sieci jest włączony, Kaspersky Endpoint Security automatycznie blokuje zagrożenia sieciowe. Dodatkowo aplikacja może zablokować atakujący komputer i ograniczyć wysyłanie pakietów sieciowych na określony czas. Domyślnie Kaspersky Endpoint Security blokuje komputer na jedną godzinę.

Jak zablokować atakujący komputer w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona sieci**.

4. W sekcji **Ustawienia Ochrony sieci**, zaznacz pole wyboru **Blokuj atakujące urządzenia przez N min**.

   Jeśli pole jest zaznaczone, Ochrona sieci dodaje atakujący komputer do listy zablokowanych. Oznacza to, że komponent Ochrona sieci zablokuje na określony czas połączenie sieciowe z atakującym komputerem po pierwszej próbie ataku sieciowego. Ta blokada automatycznie chroni komputer użytkownika przed przyszłymi atakami sieciowymi pochodzącymi z tego samego adresu. Minimalny czas, przez jaki atakujący komputer będzie znajdować się na liście blokowanych, to jedna minuta. Maksymalny czas to 999 minut.

5. Ustaw inny czas trwania blokowana dla atakującego komputera w polu po prawej stronie opcji **Blokuj atakujące urządzenia przez N min**.

6. Zapisz swoje zmiany.

Jak zablokować atakujący komputer w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Komunikacja i Ochrona WWW** → **Ochrona sieci**.

5. W sekcji **Działanie po wykryciu zagrożenia** zaznacz pole **Zablokuj atak i atakujące urządzenie przez (min)**.

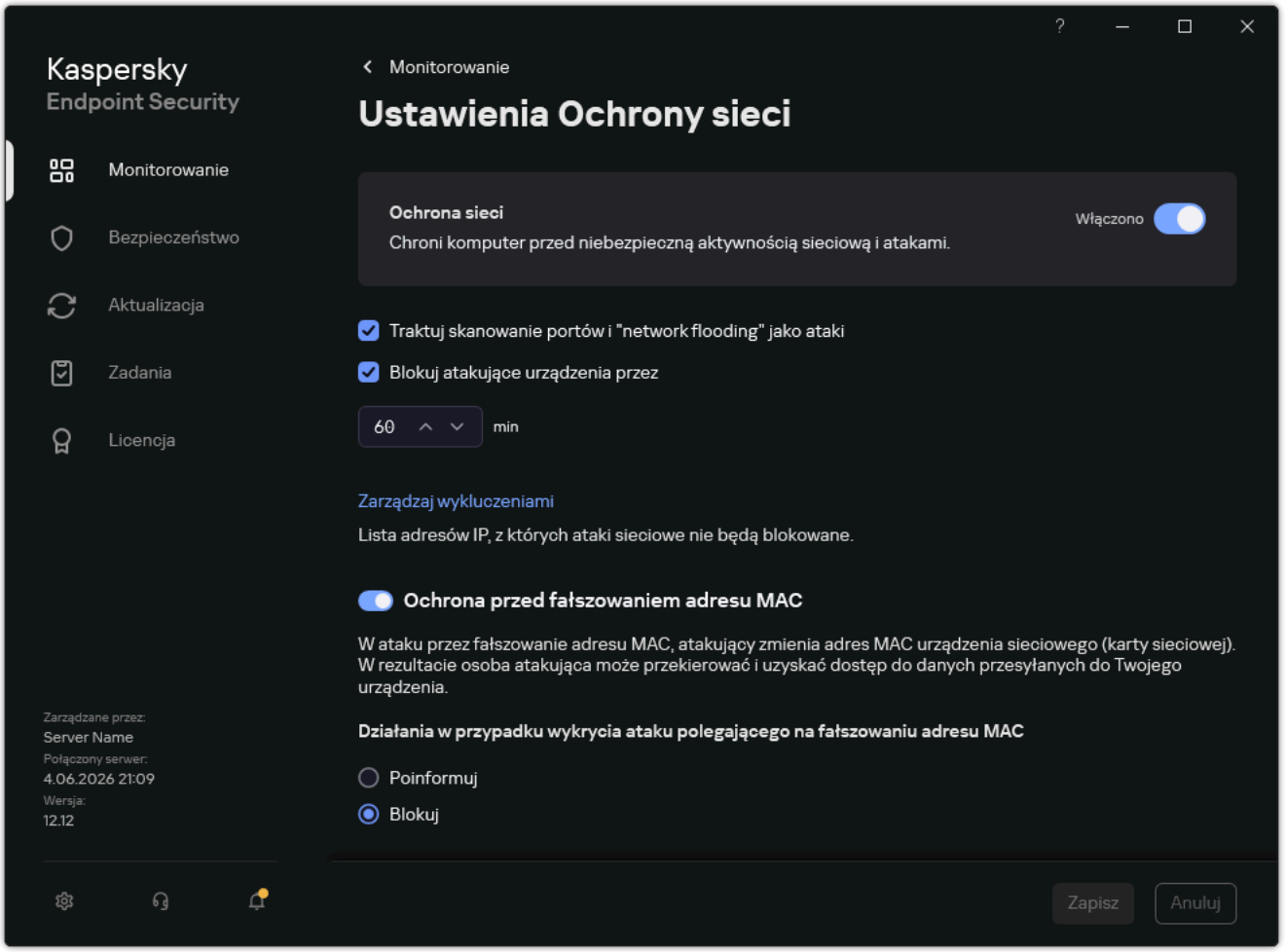
   Jeśli pole jest zaznaczone, Ochrona sieci dodaje atakujący komputer do listy zablokowanych. Oznacza to, że komponent Ochrona sieci zablokuje na określony czas połączenie sieciowe z atakującym komputerem po pierwszej próbie ataku sieciowego. Ta blokada automatycznie chroni komputer użytkownika przed przyszłymi atakami sieciowymi pochodzącymi z tego samego adresu. Minimalny czas, przez jaki atakujący komputer będzie znajdować się na liście blokowanych, to jedna minuta. Maksymalny czas to 999 minut.

6. Zmień czas blokowania atakującego komputera.

7. Zapisz swoje zmiany.

Jak zablokować atakujący komputer w interfejsie użytkownika aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona sieci**.



Ustawienia Ochrony sieci

3. Włącz przełącznik **Blokuj atakujące urządzenia przez N min**.

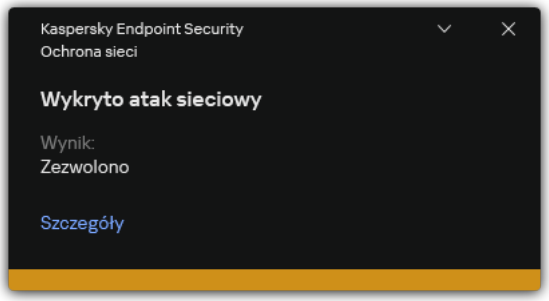
   Jeśli pole jest zaznaczone, Ochrona sieci dodaje atakujący komputer do listy zablokowanych. Oznacza to, że komponent Ochrona sieci zablokuje na określony czas połączenie sieciowe z atakującym komputerem po pierwszej próbie ataku sieciowego. Ta blokada automatycznie chroni komputer użytkownika przed przyszłymi atakami sieciowymi pochodzącymi z tego samego adresu. Minimalny czas, przez jaki atakujący komputer będzie znajdować się na liście blokowanych, to jedna minuta. Maksymalny czas to 999 minut.

4. Ustaw inny czas trwania blokowana dla atakującego komputera w polu poniżej przełącznika **Blokuj atakujące urządzenia przez N min**.

5. Zapisz swoje zmiany.

W wyniku tego działania, jeśli Kaspersky Endpoint Security wykryje próbę ataku sieciowego skierowanego na komputer użytkownika, zablokuje wszelkie połączenia z atakującym komputerem. Kaspersky Endpoint Security tworzy zdarzenie *Wykryto atak sieciowy*. Zdarzenie zawiera informacje o atakującym komputerze: adresy IP i MAC.

Adres MAC atakującego komputera można sprawdzić w interfejsie użytkownika aplikacji lub w konsoli Kaspersky Security Center Linux w wersji 15.1 lub nowszej.



Powiadomienie o wykryciu ataku sieciowego

Kaspersky Endpoint Security odblokuje komputer po upływie określonego czasu. Konsola Kaspersky Security Center nie udostępnia narzędzi do monitorowania zablokowanych komputerów innych niż zdarzenia *Wykryto atak sieciowy* w raporcie. Listę zablokowanych komputerów możesz przeglądać tylko w interfejsie aplikacji. Funkcjonalność tę zapewnia narzędzie *Monitor sieci*. Możesz także użyć narzędzia Monitor sieci, aby odblokować komputer.

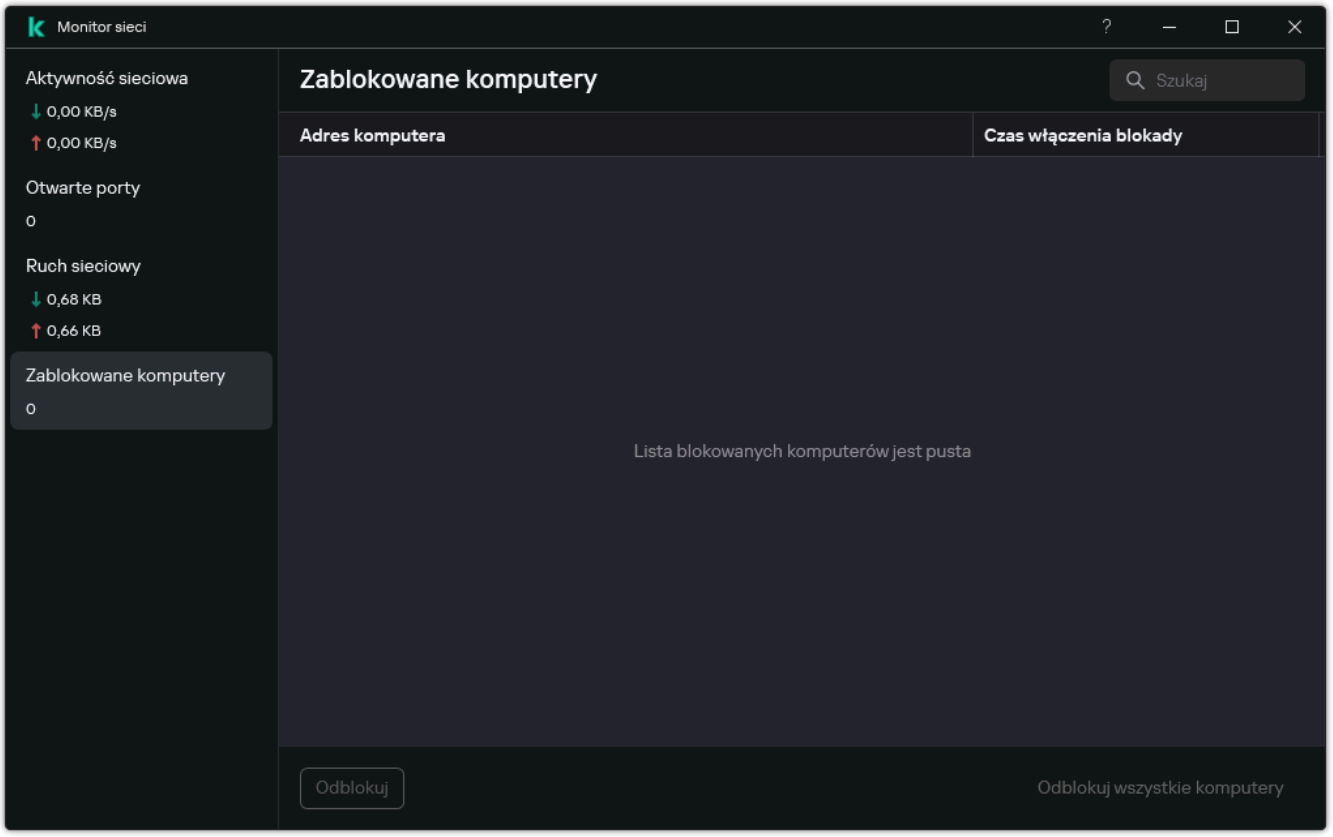
Aby odblokować komputer:

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Monitor sieci**.
2. Przejdź do zakładki **Zablokowane komputery**.

   Spowoduje to otwarcie listy zablokowanych komputerów (patrz rysunek poniżej).

   Kaspersky Endpoint Security czyści listę blokowania, gdy aplikacja zostanie ponownie uruchomiona, a ustawienia Ochrony sieci zostaną zmienione.

3. Wybierz komputer, który chcesz odblokować i kliknij **Odblokuj**.



Lista zablokowanych komputerów

Konfigurowanie wykluczania adresów z blokowania

Kaspersky Endpoint Security może rozpoznać atak sieciowy i zablokować niezabezpieczone połączenie sieciowe, za pośrednictwem którego przesyłana jest duża liczba pakietów (na przykład: z kamer nadzorujących). Aby móc pracować z zaufanymi urządzeniami, możesz dodać adresy IP tych urządzeń do listy wykluczeń. Możesz także wybrać protokół i port używane do komunikacji i zezwolić na określone działania sieciowe.

Możliwość wyboru protokołów i portów do wykluczeń została dodana w Kaspersky Endpoint Security 12.2. Upewnij się, że aplikacja i wtyczka do zarządzania są zaktualizowane do wersji 12.2 lub nowszej. Jeśli używasz wcześniejszej wersji aplikacji lub wtyczki do zarządzania, Kaspersky Endpoint Security może zezwolić na aktywność sieciową tylko na podstawie adresu IP.

Zmiana listy wykluczeń blokowania może zostać zablokowana przez właściwości zasady nadrzędnej. Aby zmienić listę, musisz zezwolić na zmianę ustawień strefy zaufanej w Web Console (kłódka musi być odblokowana).

Strefy zaufane są grupowane w różny sposób w Konsoli administracyjnej (MMC) i Web Console. Sposoby zapobiegania zmianom parametrów strefy zaufanej również mogą się różnić („kłódki" mogą być inne). Zalecamy korzystanie wyłącznie z Web Console do zarządzania aplikacją. Jeśli skonfigurujesz strefę zaufaną w różnych konsolach, wtyczka zarządzająca może przywrócić „kłódkę" do stanu domyślnego.

Jak skonfigurować adresy wykluczeń z blokowania w Konsoli administracyjnej (MMC)

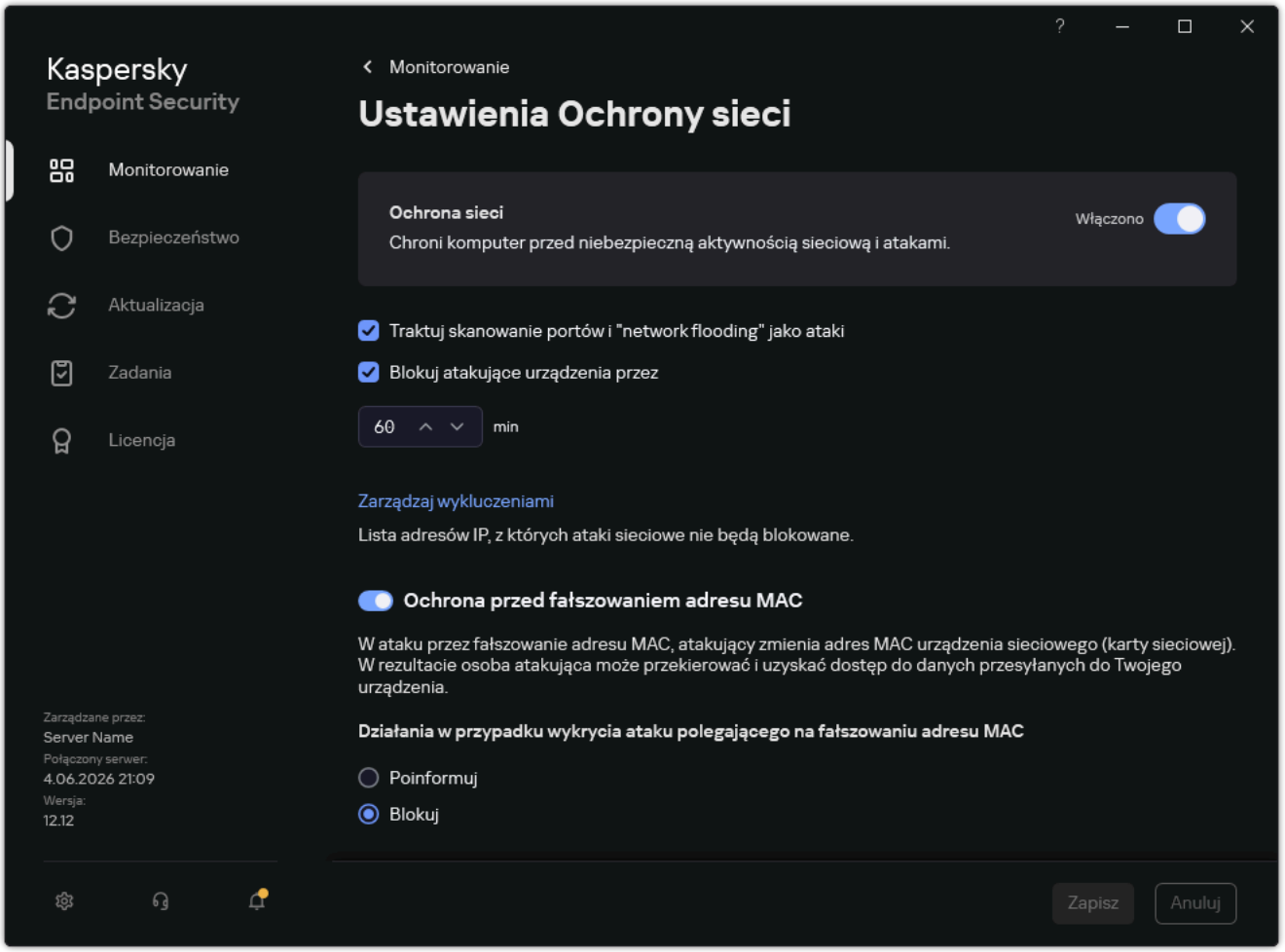
1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona sieci**.
4. W sekcji **Ustawienia Ochrony sieci** kliknij przycisk **Wykluczenia**.
5. W otwartym oknie kliknij przycisk **Dodaj**.
6. Wprowadź adres IP komputera, z którego ataki sieciowe nie będą blokowane.
   W razie potrzeby wybierz protokół i porty, przez które przesyłane są dane.
7. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console skonfigurować adresy wykluczeń z blokowania

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Komunikacja i Ochrona WWW → Ochrona sieci**.
5. W górnej części okna kliknij odnośnik **Zaufane adresy IP**.
6. W otwartym oknie kliknij przycisk **Dodaj**.
7. Wprowadź adres IP komputera, z którego ataki sieciowe nie będą blokowane.
   W razie potrzeby określ podsieć.
8. Zapisz swoje zmiany.

Jak skonfigurować adresy wykluczeń z blokowania w interfejsie użytkownika aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona sieci**.



Ustawienia Ochrony sieci

3. Kliknij odnośnik **Zarządzaj wykluczeniami**.
4. W otwartym oknie kliknij przycisk **Dodaj**.
5. Wprowadź adres IP komputera, z którego ataki sieciowe nie będą blokowane.

   W razie potrzeby wybierz protokół i porty, przez które przesyłane są dane.
6. Zapisz swoje zmiany.

Eksportowanie i importowanie listy wykluczeń z blokowania

Możesz wyeksportować listę wykluczeń do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę adresów tego samego typu. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy wykluczeń lub przeniesienia listy na inny serwer.

Eksportowanie i importowanie listy wykluczeń w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona sieci**.
4. W sekcji **Ustawienia Ochrony sieci** kliknij przycisk **Wykluczenia**.
5. W celu wyeksportowania listy reguł:
   a. Wybierz wykluczenia, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
      Jeśli nie wybrałeś żadnego wykluczenia, Kaspersky Endpoint Security wyeksportuje wszystkie wykluczenia.
   b. Kliknij przycisk → **Eksportuj**.
   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.
   d. Zapisz plik.
      Kaspersky Endpoint Security eksportuje całą listę wykluczeń do pliku XML.
6. W celu zaimportowania listy wykluczeń:
   a. Kliknij przycisk → **Importuj**.
   b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.
   c. Otwórz plik.
      Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
7. Zapisz swoje zmiany.

Eksportowanie i importowanie listy wykluczeń w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Komunikacja i Ochrona WWW → Ochrona sieci**.
5. W górnej części okna kliknij odnośnik **Zaufane adresy IP**.
   Zostanie otwarta lista wykluczeń.

6. W celu wyeksportowania listy reguł:

   a. Wybierz wykluczenia, które chcesz wyeksportować.

   b. Kliknij przycisk → **Eksportuj**.

      Kaspersky Endpoint Security eksportuje listę wykluczeń do pliku JSON w domyślnym folderze Pobrane.

7. W celu zaimportowania listy wykluczeń:

   a. Kliknij przycisk → **Importuj**.

      W oknie, które zostanie otwarte, wybierz plik JSON, z którego chcesz zaimportować listę wykluczeń.

   b. Otwórz plik.

      Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku JSON.

8. Zapisz swoje zmiany.

Konfigurowanie Ochrony sieci według typu

Kaspersky Endpoint Security umożliwia zarządzanie ochroną przed następującymi typami ataków sieciowych:

- *Zalewanie sieci* jest atakiem na zasoby sieciowe (takie jak serwery internetowe). Ten atak obejmuje wysyłanie dużej liczby żądań w celu przeciążenia przepustowości zasobów sieciowych. W takiej sytuacji użytkownicy nie mogą uzyskać dostępu do zasobów sieciowych organizacji.

- Atak *Skanowanie portów* obejmuje skanowanie portów UDP, portów TCP, a także usługi sieciowe komputera. Ten atak umożliwia atakującemu zidentyfikowanie stopnia podatności komputera przed przeprowadzeniem bardziej niebezpiecznych rodzajów ataków sieciowych. Skanowanie portów umożliwia atakującemu także zidentyfikowanie systemu operacyjnego na komputerze i wybranie odpowiednich ataków sieciowych dla tego systemu operacyjnego.

- *Atak przez fałszowanie adresu MAC* obejmuje zmianę adresu MAC urządzenia sieciowego (karty sieciowej). W rezultacie osoba atakująca może przekierować dane wysłane do urządzenia na inne urządzenie i uzyskać dostęp do tych danych. Kaspersky Endpoint Security umożliwia blokowanie ataków przez fałszowanie adresu MAC i otrzymywanie powiadomień o atakach.

Możesz wyłączyć wykrywanie tych rodzajów ataków w przypadku, gdy niektóre z Twoich dozwolonych aplikacji wykonują działania typowe dla tych rodzajów ataków. Pomoże to w uniknięciu fałszywych alarmów.

Domyślnie, Kaspersky Endpoint Security nie monitoruje ataków typu zalewanie sieci, skanowanie portów, a także ataku przez fałszowanie adresu MAC.

Nie zalecamy włączania ochrony przed fałszowaniem adresu MAC na maszynach wirtualnych w infrastrukturze Microsoft Hyper-V. Z uwagi na specyfikę platformy Microsoft Hyper-V rozwiązanie Kaspersky Industrial CyberSecurity for Nodes może blokować hipernadzorcę z powodu wyników fałszywie dodatnich.

Jak skonfigurować Ochronę sieci według typu w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona sieci**.
4. Użyj pola wyboru **Traktuj skanowanie portów i „network flooding" jako ataki**, aby włączyć lub wyłączyć wykrywanie tych ataków.

   Jeśli ta funkcja jest włączona, Kaspersky Endpoint Security monitoruje ruch sieciowy pod kątem skanowania portów i zalewania sieci. W przypadku wykrycia takiego zachowania aplikacja powiadamia użytkownika i wysyła odpowiednie zdarzenie do Kaspersky Security Center. Aplikacja dostarcza informacji o komputerze wysyłającym żądania. Informacje te są niezbędne do terminowej reakcji. Jednakże Kaspersky Endpoint Security nie blokuje komputera wysyłającego żądania, ponieważ taki ruch może być normalnym zjawiskiem w sieci firmowej.
5. W sekcji **Tryb ochrony przed fałszowaniem adresu MAC** wybierz jedną z następujących opcji:
   - **Nie śledź przypadków fałszowania adresu MAC**.
   - **Poinformuj**.
   - **Zablokuj**.
6. Zapisz swoje zmiany.

Jak skonfigurować Ochronę sieci według typu w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

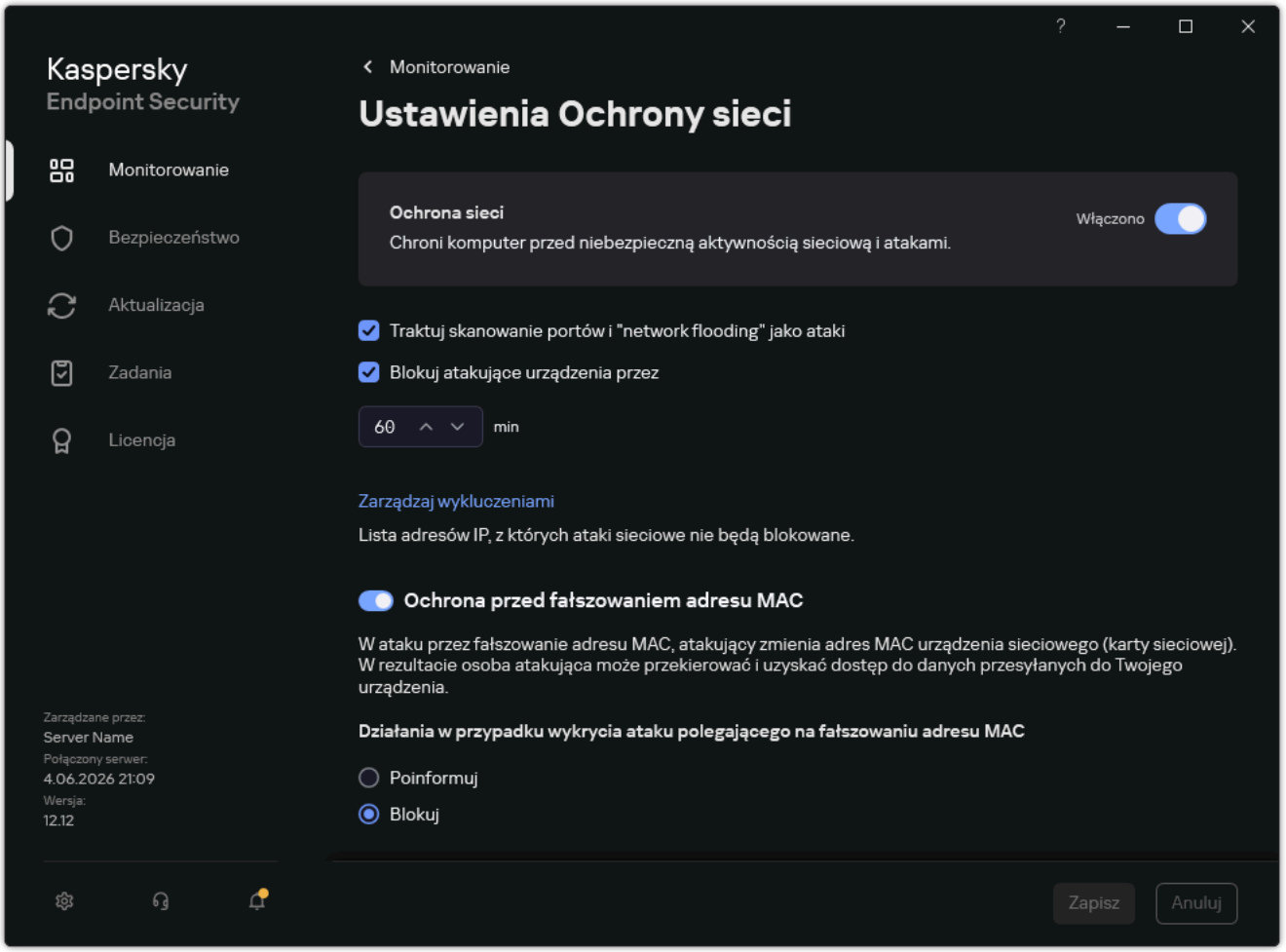
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Komunikacja i Ochrona WWW → Ochrona sieci**.
5. Użyj pola wyboru **Traktuj skanowanie portów i "network flooding" jako ataki**, aby włączyć lub wyłączyć wykrywanie tych ataków.

   Jeśli ta funkcja jest włączona, Kaspersky Endpoint Security monitoruje ruch sieciowy pod kątem skanowania portów i zalewania sieci. W przypadku wykrycia takiego zachowania aplikacja powiadamia użytkownika i wysyła odpowiednie zdarzenie do Kaspersky Security Center. Aplikacja dostarcza informacji o komputerze wysyłającym żądania. Informacje te są niezbędne do terminowej reakcji. Jednakże Kaspersky Endpoint Security nie blokuje komputera wysyłającego żądania, ponieważ taki ruch może być normalnym zjawiskiem w sieci firmowej.

6. W sekcji **Ochrona przed fałszowaniem adresu MAC** wybierz jedną z następujących opcji:
   - **Ochrona przed fałszowaniem adresu MAC włączona**.
   - **Powiadom**.
   - **Zablokuj**.
7. Zapisz swoje zmiany.

Jak skonfigurować Ochronę sieci według typu w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Ochrona sieci**.



Ustawienia Ochrony sieci

3. Użyj przełącznika **Traktuj skanowanie portów i "network flooding" jako ataki**, aby włączyć lub wyłączyć wykrywanie tych ataków.

   Jeśli ta funkcja jest włączona, Kaspersky Endpoint Security monitoruje ruch sieciowy pod kątem skanowania portów i zalewania sieci. W przypadku wykrycia takiego zachowania aplikacja powiadamia użytkownika i wysyła odpowiednie zdarzenie do Kaspersky Security Center. Aplikacja dostarcza informacji o komputerze wysyłającym żądania. Informacje te są niezbędne do terminowej reakcji. Jednakże Kaspersky Endpoint Security nie blokuje komputera wysyłającego żądania, ponieważ taki ruch może być normalnym zjawiskiem w sieci firmowej.

4. Użyj przełącznika **Ochrona przed fałszowaniem adresu MAC**, aby włączyć lub wyłączyć wykrywanie tych ataków.

5. W sekcji **Działania w przypadku wykrycia ataku polegającego na fałszowaniu adresu MAC** wybierz jedną z następujących opcji:

   - **Poinformuj**.
   - **Blokuj**.

6. Zapisz swoje zmiany.

Zapora sieciowa

Zapora sieciowa blokuje nieautoryzowane połączenia z komputerem podczas pracy w Internecie lub sieci lokalnej. Zapora sieciowa kontroluje również aktywność sieciową aplikacji na komputerze. Pozwala to chronić korporacyjną sieć LAN przed kradzieżą tożsamości i innymi atakami. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i predefiniowanych *reguł sieciowych*.

Agent sieciowy jest używany do interakcji z Kaspersky Security Center. Zapora sieciowa automatycznie tworzy reguły sieciowe wymagane do działania aplikacji i Agenta sieciowego. W wyniku działania Zapora sieciowa otwiera kilka portów na komputerze. Które porty są otwarte w zależności od roli komputera (na przykład, punkt dystrybucji). Więcej informacji o portach, które zostaną otwarte na komputerze, można znaleźć w pomocy dla Kaspersky Security Center.

Reguły sieciowe

Możesz skonfigurować reguły sieciowe na następujących poziomach:

- *Reguły pakietów sieciowych*. Reguły pakietów sieciowych nakładają ograniczenia na pakiety sieciowe, niezależnie od aplikacji. Takie reguły ograniczają ruch sieciowy wychodzący i przychodzący przez określone porty wybranego protokołu. Kaspersky Endpoint Security wstępnie zdefiniował reguły pakietów sieciowych z uprawnieniami zalecanymi przez ekspertów z Kaspersky.
- *Reguły sieciowe dla aplikacji*. Reguły sieciowe dla aplikacji nakładają ograniczenia na aktywność sieciową określonej aplikacji. W tym przypadku brane są pod uwagę cechy charakterystyczne pakietu sieciowego, a także aplikacja, dla której jest on przeznaczony lub która zainicjowała jego przesyłanie.

Kontrolowany dostęp aplikacji do zasobów systemu operacyjnego, procesów i danych osobowych jest zapewniany przez komponent Ochrona przed włamaniami przy użyciu *uprawnień aplikacji*.

Podczas pierwszego uruchomienia aplikacji Zapora sieciowa wykonuje następujące działania:

1. Sprawdza bezpieczeństwo aplikacji przy użyciu pobranych antywirusowych baz danych.
2. Sprawdza bezpieczeństwo aplikacji w Kaspersky Security Network.

   Zalecane jest uczestniczenie w Kaspersky Security Network, aby zapewnić bardziej efektywne działanie Zapory sieciowej.

3. Umieszcza aplikację w jednej z grup zaufania: *Zaufane*, *Niskie ograniczenia*, *Wysokie ograniczenia*, *Niezaufane*.

Grupa zaufania określa uprawnienia, do których program Kaspersky Endpoint Security odnosi się podczas kontrolowania aktywności aplikacji. Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera.

Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania dla składników Zapora sieciowa i Ochrona przed włamaniami. Nie można zmienić grupy zaufania tylko dla Zapory sieciowej lub Ochrony przed włamaniami.

Jeśli odmówiłeś uczestnictwa w KSN lub nie ma sieci, Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od ustawień modułu Ochrona przed włamaniami. Po otrzymaniu reputacji aplikacji od KSN, grupę zaufania można zmienić automatycznie.

4. Blokuje aktywność sieciową aplikacji w zależności od grupy zaufania. Na przykład, aplikacje z grupy *Wysokie ograniczenia* nie mogą korzystać z żadnych połączeń sieciowych.

Przy następnym uruchomieniu aplikacji, Kaspersky Endpoint Security sprawdzi integralność aplikacji. Jeżeli aplikacja nie została zmieniona, moduł użyje dla niej bieżących reguł sieciowych. Jeżeli aplikacja została zmodyfikowana, Kaspersky Endpoint Security analizuje aplikację tak, jakby była uruchamiana po raz pierwszy.

Priorytety reguł sieciowych

Każda reguła posiada priorytet. Im wyżej reguła znajduje się na liście reguł, tym wyższy priorytet posiada. Jeśli aktywność sieci zostanie dodana do kilku reguł, Zapora sieciowa reguluje aktywność sieciową zgodnie z regułą o najwyższym priorytecie.

Reguły pakietów sieciowych mają wyższy priorytet niż reguły sieciowe dla aplikacji. Jeżeli do tego samego typu aktywności sieciowej są zastosowane reguły pakietów sieciowych i reguły sieciowe dla aplikacji, będzie ona przetwarzana zgodnie z regułami pakietów sieciowych.

Reguły sieciowe dla aplikacji działają w określony sposób. Reguła sieciowa dla aplikacji zawiera reguły dostępu oparte na stanie sieci: *Sieć publiczna*, *Sieć lokalna*, *Sieć zaufana*. Na przykład, aplikacje z grupy zaufania *Wysokie ograniczenia* domyślnie nie zezwalają na żadną aktywność sieciową w sieciach o wszystkich stanach. Jeśli dla pojedynczej aplikacji (aplikacji nadrzędnej) zostanie określona reguła sieciowa, procesy potomne innych aplikacji będą działać zgodnie z regułą sieciową aplikacji nadrzędnej. Jeśli nie istnieje reguła sieciowa dla aplikacji, procesy potomne będą działały zgodnie z regułą dostępu do sieci grupy zaufania aplikacji.

Na przykład, zabroniona jest jakakolwiek aktywność sieciowa w sieciach o wszystkich stanach dla wszystkich aplikacji, za wyjątkiem przeglądarki X. Jeśli rozpoczniesz instalację przeglądarki Y (proces potomny) z przeglądarki X (aplikacja nadrzędna), wówczas instalator przeglądarki Y uzyska dostęp do sieci i pobierze niezbędne pliki. Po instalacji przeglądarka Y będzie odmawiała jakichkolwiek połączeń sieciowych zgodnie z ustawieniami Zapory sieciowej. Aby zabronić aktywności sieciowej instalatora przeglądarki Y jako procesu potomnego, należy dodać regułę sieciową dla instalatora przeglądarki Y.

Typy połączenia sieciowego

Zapora sieciowa pozwala kontrolować aktywność sieciową w zależności od typu połączenia sieciowego. Kaspersky Endpoint Security otrzymuje typ połączenia sieciowego z systemu operacyjnego komputera. Typ połączenia sieciowego w systemie operacyjnym jest ustawiany przez użytkownika podczas konfigurowania połączenia. Możesz zmienić typ połączenia sieciowego w ustawieniach Kaspersky Endpoint Security. Zapora sieciowa będzie monitorować aktywność sieci w zależności od typu sieci określonego w ustawieniach Kaspersky Endpoint Security, a nie w systemie operacyjnym.

Dostępne są następujące typy połączeń sieciowych:

- **Sieć publiczna**. Sieć nie jest chroniona przez aplikacje antywirusowe, zapory sieciowe ani filtry (takie jak Wi-Fi w kawiarni). Podczas korzystania z komputera podłączonego do tego typu sieci Zapora sieciowa blokuje dostęp do plików i drukarek tego komputera. Użytkownicy z zewnątrz nie będą mogli również uzyskać dostępu do danych poprzez folder współdzielony oraz zdalnego dostępu do pulpitu tego komputera. Zapora sieciowa filtruje aktywność sieciową każdej aplikacji zgodnie z utworzoną dla niej regułą sieciową.

  Domyślnie zapora sieciowa przypisuje do internetu typ *Sieć publiczna*. Nie możesz zmienić typu przypisanego do internetu.

- **Sieć lokalna**. Sieć dla użytkowników z ograniczonym dostępem do plików i drukarek na tym komputerze (na przykład dla firmowej sieci LAN lub sieci domowej).

- **Sieć zaufana**. Bezpieczna sieć, w której komputer nie jest wystawiony na ataki lub nieautoryzowane próby dostępu do danych. Zapora sieciowa zezwala na dowolną aktywność sieciową w obrębie sieci o tym stanie.

Włączanie i wyłączanie modułu Zapora sieciowa

Domyślnie moduł Zapora sieciowa jest włączony i działa w trybie optymalnym.

Jak włączyć lub wyłączyć Zaporę sieciową w Konsoli Administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa**.
4. Użyj pola **Zapora sieciowa**, aby włączyć lub wyłączyć komponent.
5. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć Zaporę sieciową w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Komunikacja i Ochrona WWW → Zapora sieciowa**.

5. Użyj przełącznika **Zapora sieciowa WŁĄCZONA**, aby włączyć lub wyłączyć komponent.

6. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć Zaporę sieciową w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa**.

3. Użyj przełącznika **Zapora sieciowa**, aby włączyć lub wyłączyć komponent.

4. Zapisz swoje zmiany.

W rezultacie, jeżeli Zapora sieciowa jest włączona, Kaspersky Endpoint Security kontroluje aktywność sieciową i blokuje nieautoryzowane połączenia sieciowe z komputerem, jak również blokuje nieautoryzowaną aktywność sieciową aplikacji na komputerze. Aktywność sieciowa jest również kontrolowana przez komponent Ochrona sieci. Składnik Ochrona przed zagrożeniami sieciowymi (zwany także systemem wykrywania włamań) monitoruje przychodzący ruch sieciowy pod kątem aktywności charakterystycznej dla ataków sieciowych.

> Kaspersky Endpoint Security rejestruje w swoich raportach zdarzenia ataków sieciowych niezależnie od ustawień Zapory sieciowej. Nawet jeśli Zapora sieciowa zablokuje połączenie sieciowe za pomocą reguł i w ten sposób zapobiegnie atakowi sieciowemu, komponent Ochrona sieci rejestruje zdarzenia związane z atakiem sieciowym. Jest to wymagane do generowania informacji statystycznych o atakach sieciowych na komputery w organizacji.

Zmiana typu połączenia sieciowego

Domyślnie zapora sieciowa przypisuje do internetu typ *Sieć publiczna*. Nie możesz zmienić typu przypisanego do internetu.

W celu zmiany typu połączenia sieciowego:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa**.

3. Kliknij **Dostępne sieci**.

4. Wybierz połączenie sieciowe, którego typ chcesz zmienić.

5. W kolumnie **Typ sieci** wybierz typ połączenia sieciowego:

   - **Sieć publiczna**. Sieć nie jest chroniona przez aplikacje antywirusowe, zapory sieciowe ani filtry (takie jak Wi-Fi w kawiarni). Podczas korzystania z komputera podłączonego do tego typu sieci Zapora sieciowa blokuje dostęp do plików i drukarek tego komputera. Użytkownicy z zewnątrz nie będą mogli również uzyskać dostępu do danych poprzez folder współdzielony oraz zdalnego dostępu do pulpitu tego komputera. Zapora sieciowa filtruje aktywność sieciową każdej aplikacji zgodnie z utworzoną dla niej regułą sieciową.

   - **Sieć lokalna**. Sieć dla użytkowników z ograniczonym dostępem do plików i drukarek na tym komputerze (na przykład dla firmowej sieci LAN lub sieci domowej).

   - **Sieć zaufana**. Bezpieczna sieć, w której komputer nie jest wystawiony na ataki lub nieautoryzowane próby dostępu do danych. Zapora sieciowa zezwala na dowolną aktywność sieciową w obrębie sieci o tym stanie.

6. Zapisz swoje zmiany.

Zarządzanie regułami dla pakietów sieciowych

Podczas zarządzania regułami dla pakietów sieciowych możesz wykonać następujące czynności:

- Utworzyć nową regułę dla pakietu sieciowego.

  Możesz utworzyć nową regułę dla pakietu sieciowego, tworząc zestaw warunków i akcji stosowany do pakietów sieciowych i strumieni danych.

- Włączyć lub wyłączyć regułę dla pakietu sieciowego.

  Wszystkie reguły pakietów sieciowych utworzone przez Zaporę sieciową domyślnie posiadają stan *Włączona*. Jeżeli reguła dla pakietu sieciowego jest włączona, Zapora sieciowa stosuje tę regułę.

  Możesz wyłączyć dowolną regułę dla pakietu sieciowego, która została wybrana z listy reguł dla pakietów sieciowych. Jeżeli reguła dla pakietu sieciowego jest wyłączona, Zapora sieciowa tymczasowo nie stosuje tej reguły.

  > Nowa niestandardowa reguła dla pakietu sieciowego jest dodawana do listy reguł dla pakietów sieciowych z domyślnym stanem *Włączona*.

- Zmodyfikować ustawienia już istniejącej reguły dla pakietu sieciowego.

  Po utworzeniu nowej reguły dla pakietu sieciowego, można zawsze powrócić do edycji jej ustawień i w razie potrzeby zmodyfikować je.

- Zmienić akcję Zapory sieciowej dla reguły dla pakietu sieciowego.

  Na liście reguł dla pakietów sieciowych możesz zmodyfikować akcję podejmowaną przez Zaporę sieciową po wykryciu aktywności sieciowej odpowiadającej określonej regule dla pakietu sieciowego.

- Zmienić priorytet reguły dla pakietu sieciowego.

  Możesz zwiększyć lub zmniejszyć priorytet wybranej reguły dla pakietu sieciowego.

- Usunąć regułę dla pakietu sieciowego.

  Możesz usunąć regułę dla pakietu sieciowego, aby Zapora sieciowa przestała stosować ją po wykryciu aktywności sieciowej, a także aby reguła ta nie była wyświetlana na liście reguł dla pakietów sieciowych ze stanem *Wyłączona*.

Tworzenie reguły dla pakietu sieciowego.

Zapora sieciowa filtruje całą aktywność sieciową na komputerze zgodnie z regułami pakietów sieciowych. Reguły pakietów sieciowych zawierają warunki (na przykład kierunek, protokół), które zapora stosuje, aby kontrolować połączenia sieciowe komputera. Reguły pakietów sieciowych określają również działanie, jakie zapora podejmie w przypadku połączenia zgodnego z regułą (zezwalanie na połączenie lub blokowanie go).

Zalecenia dotyczące tworzenia reguł pakietów sieciowych

Aby filtrować aktywność sieciową, możesz określić adres IP lub zakres adresów IP. Możesz również określić nazwę DNS, ale zalecamy używanie adresów IP i zakresów adresów IP. Używanie nazw DNS w nazwach pakietów sieciowych może być niebezpieczne, ponieważ właściciel serwera DNS może modyfikować parametry rekordu DNS. Złośliwcy mogą również podszywać się pod komunikaty DNS i obchodzić reguły zapory sieciowej.

Możesz kontrolować połączenia sieciowe za pomocą nazw DNS, używając zasad Kontroli sieci. Jeśli musisz określić nazwę DNS w regułach zapory:

- Zabezpiecz firmową sieć LAN.
- Zabezpiecz pamięć podręczną i autorytatywne serwery DNS.
- Włącz ochronę rekordu DNS przed modyfikacją.

Podczas tworzenia reguł dla pakietów sieciowych należy pamiętać, że posiadają one wyższy priorytet niż reguły sieciowe dla aplikacji.

Metody tworzenia reguł pakietów sieciowych

Regułę dla pakietu sieciowego można utworzyć na następujące sposoby:

- Użyj narzędzia Monitor sieci.

  Monitor sieci to narzędzie służące do wyświetlania informacji o aktywności sieciowej komputera użytkownika w czasie rzeczywistym. Jest to wygodne, ponieważ nie potrzebujesz konfigurować wszystkich ustawień reguły. Niektóre ustawienia Zapory sieciowej zostaną automatycznie uzupełnione z danych Monitora sieci. Monitor sieci jest dostępny tylko w interfejsie aplikacji.

- Skonfiguruj ustawienia Zapory sieciowej.

  To umożliwi dostosowanie ustawień Zapory sieciowej. Możesz utworzyć reguły dla dowolnej aktywności sieciowej nawet wtedy, gdy aktualnie nie ma aktywności sieciowej.

Jak używać narzędzia Monitor sieci do utworzenia reguły dla pakietu sieciowego w interfejsie aplikacji?

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Monitor sieci**.
2. Przejdź do zakładki **Aktywność sieciowa**.

   Zakładka **Aktywność sieciowa** wyświetla wszystkie aktualnie aktywne połączenia sieciowe komputera. Wyświetlane są połączenia przychodzące i wychodzące.
3. Z menu kontekstowego połączenia sieciowego wybierz **Utwórz regułę dla pakietu sieciowego**.

   Spowoduje to otwarcie właściwości reguły sieciowej.
4. Ustaw stan **Aktywny** dla reguły dla pakietów.
5. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
6. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).

   Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Szablon reguły sieciowej**. Szablony reguły opisują najczęściej używane połączenia sieciowe.

   Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.
7. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w raporcie, zaznacz pole **Zapisuj zdarzenia**.
8. Kliknij **Zapisz**.

   Nowa reguła sieciowa zostanie dodana do listy.
9. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.
10. Zapisz swoje zmiany.

Jak używać ustawień Zapory sieciowej do utworzenia reguły dla pakietu sieciowego w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
3. Kliknij **Reguły dla pakietów**.

   Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.
4. Używając listy rozwijanej **Dodaj** wybierz lokalizację reguły na liście: w górze listy, w dole listy lub obok wybranej reguły.

   Pozycja reguły na liście określa priorytet reguły. Reguła znajdująca się na szczycie listy ma najwyższy priorytet.
5. Ustaw stan **Aktywny** dla reguły dla pakietów.
6. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
7. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).

   Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Szablon reguły sieciowej**. Szablony reguły opisują najczęściej używane połączenia sieciowe.

   Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.
8. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w raporcie, zaznacz pole **Zapisuj zdarzenia**.

9. Kliknij **Zapisz**.

   Nowa reguła sieciowa zostanie dodana do listy.

10. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.

11. Zapisz swoje zmiany.

Jak utworzyć regułę dla pakietu sieciowego w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.

4. W sekcji **Ustawienia Zapory sieciowej** kliknij przycisk **Ustawienia**.

   To spowoduje otwarcie listy reguł dla pakietów sieciowych oraz listy reguł sieciowych dla aplikacji.

5. Przejdź do zakładki **Reguły pakietów sieciowych**.

   Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.

6. Używając listy rozwijanej **Dodaj** wybierz lokalizację reguły na liście: w górze listy, w dole listy lub obok wybranej reguły.

   Pozycja reguły na liście określa priorytet reguły. Reguła znajdująca się na szczycie listy ma najwyższy priorytet.

7. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.

8. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).

   Możesz wybrać predefiniowany szablon reguły, klikając przycisk . Szablony reguły opisują najczęściej używane połączenia sieciowe.

   Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.

9. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w raporcie, zaznacz pole **Zapisuj zdarzenia**.

10. Zapisz nową regułę sieciową.

11. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.

12. Zapisz swoje zmiany.

Zapora sieciowa będzie kontrolowała pakiety sieciowe zgodnie z regułą. Możesz wyłączyć regułę dla pakietów w Zaporze sieciowej bez usuwania jej z listy. W tym celu odznacz pole obok obiektu.

Jak utworzyć regułę pakietów sieciowych w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Komunikacja i Ochrona WWW** → **Zapora sieciowa**.

5. Wybierz zakładkę **Reguły pakietów sieciowych**.

   Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.

6. Kliknij **Dodaj**.

   To spowoduje otwarcie formularza nowej reguły sieciowej.

7. W polu **Nazwa reguły** wprowadź ręcznie nazwę usługi sieciowej.

8. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).

   Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Wybierz szablon reguły**. Szablony reguły opisują najczęściej używane połączenia sieciowe.

   Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.

9. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w raporcie, zaznacz pole **Zapisuj zdarzenia**.

10. Zapisz regułę sieciową.

    Nowa reguła sieciowa zostanie dodana do listy.

11. Użyj przycisku **Przenieś**, aby ustawić priorytet reguły sieciowej.

12. Zapisz swoje zmiany.

Zapora sieciowa będzie kontrolowała pakiety sieciowe zgodnie z regułą. Możesz wyłączyć regułę dla pakietów w Zaporze sieciowej bez usuwania jej z listy. Użyj przełącznika w kolumnie **Stan**, aby włączyć lub wyłączyć regułę dla pakietu.

Ustawienia reguły pakietów sieciowych

Parametr	Opis
Akcja	**Zezwól**. **Blokuj**. **Zgodnie z regułami aplikacji**. Jeśli ta opcja jest zaznaczona, Zapora sieciowa stosuje reguły sieciowe dla aplikacji do połączenia sieciowego.
Protokół	Kontroluje aktywność sieciową po wybranym protokole: TCP, UDP, ICMP, ICMPv6, IGMP i GRE. Jeśli wybrałeś protokół ICMP lub ICMPv6, możesz zdefiniować typ i kod pakietu ICMP. Jeżeli jako typ protokołu wybrano TCP lub UDP, możesz określić porty komputera lokalnego oraz komputera zdalnego, między którymi połączenie będzie monitorowane. Zakres możliwych wartości numerów portów: 0–65535. W każdym polu możesz wprowadzić wiele wartości oddzielonych `,` lub określ zakres wartości, używając `-`. Na przykład: • `100,101` • `100-130` • `100,110-130`
Kierunek	**Przychodzący (pakiet)**. Zapora sieciowa stosuje regułę sieciową do wszystkich przychodzących pakietów sieciowych. **Przychodzący**. Zapora sieciowa stosuje regułę sieciową do wszystkich pakietów sieciowych wysłanych za pośrednictwem połączenia zainicjowanego przez zdalny komputer. **Przychodzący / Wychodzący**. Zapora sieciowa stosuje regułę sieciową do wszystkich przychodzących i wychodzących pakietów sieciowych. **Wychodzący (pakiet)**. Zapora sieciowa stosuje regułę sieciową do wszystkich wychodzących pakietów sieciowych. **Wychodzący**. Zapora sieciowa stosuje regułę sieciową do wszystkich pakietów sieciowych wysłanych za pośrednictwem połączenia zainicjowanego przez komputer użytkownika.
Karty sieciowe	Karty sieciowe, które mogą wysyłać i/lub odbierać pakiety sieciowe. Podczas określania ustawień kart sieciowych możliwe jest rozróżnienie pomiędzy pakietami sieciowymi wysyłanymi lub odbieranymi przez karty sieciowe z takimi samymi adresami IP.
Czas wygaśnięcia (TTL)	Ograniczenie kontroli pakietów sieciowych przez ich czas życia (Time to Live, TTL).

Parametr	Opis
Adresy zdalne	Adresy sieciowe zdalnych komputerów, które mogą wysyłać i/lub odbierać pakiety sieciowe. Zapora sieciowa stosuje regułę sieciową do określonego zakresu zdalnych adresów sieciowych. Możesz włączyć wszystkie adresy IP do reguły sieciowej, utworzyć oddzielną listę adresów IP, określić zakres adresów IP lub wybrać podsieć (Sieci zaufane, Sieci lokalne, Sieci publiczne). Możesz także określić nazwę DNS komputera zamiast jego adresu IP. Powinieneś używać nazw DNS tylko dla komputerów LAN lub wewnętrznych usług. Interakcja z usługami chmury (takimi jak Microsoft Azure) i innymi zasobami internetowymi powinna być zarządzana przez komponent Kontrola sieci. Jeśli w regule pakietu sieciowego dodałeś nazwę DNS, dla której nie można określić adresu IP, Kaspersky Endpoint Security wyświetli ostrzeżenie. Na liście reguł pakietów sieciowych w konsoli internetowej dodawana jest kolumna z opisem błędu. W konsoli administracyjnej (MMC) opis błędu jest niedostępny. Takie reguły pakietów są podświetlone kolorem.
Adresy lokalne	Adresy sieciowe komputerów, które mogą wysyłać i odbierać pakiety sieciowe. Zapora sieciowa stosuje regułę sieciową do określonego zakresu lokalnych adresów sieciowych. Możesz włączyć wszystkie adresy IP do reguły sieciowej, utworzyć oddzielną listę adresów IP lub określić zakres adresów IP. Aplikacja przechowuje adresy lokalne tylko wtedy, gdy określono listę adresów zdalnych. To znaczy, gdy wybrano wartość **Adresy z listy** w polu **Adresy zdalne** i dodano co najmniej jeden adres. Zdarza się, że dla aplikacji nie można uzyskać adresu lokalnego. W takim przypadku ten parametr jest ignorowany.

Włączanie i wyłączanie reguły dla pakietu sieciowego

W celu włączenia lub wyłączenia reguły dla pakietu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa**.
3. Kliknij **Reguły dla pakietów**.

   Spowoduje to otwarcie listy domyślnych reguł dla pakietów sieciowych, ustawionych przez Zaporę sieciową.
4. Na liście wybierz żądaną regułę dla pakietu sieciowego.
5. Użyj przełącznika w kolumnie **Stan**, aby włączyć lub wyłączyć regułę.
6. Zapisz swoje zmiany.

Zmienianie akcji Zapory sieciowej dla reguły dla pakietu sieciowego

W celu zmiany akcji Zapory sieciowej stosowanej do reguły dla pakietu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa**.
3. Kliknij **Reguły dla pakietów**.

   Spowoduje to otwarcie listy domyślnych reguł dla pakietów sieciowych, ustawionych przez Zaporę sieciową.

4. Wybierz ją na liście reguł dla pakietów sieciowych i kliknij przycisk **Edytuj**.

5. Z listy rozwijalnej **Akcja** wybierz akcję, jaka zostanie wykonana przez Zaporę sieciową po wykryciu tego rodzaju aktywności sieciowej:

   - **Zezwól**.
   - **Blokuj**.
   - **Zgodnie z regułami aplikacji**. Jeśli ta opcja jest zaznaczona, Zapora sieciowa stosuje reguły sieciowe dla aplikacji do połączenia sieciowego.

6. Zapisz swoje zmiany.

Zmienianie priorytetu reguły dla pakietu sieciowego

Priorytet reguły dla pakietu sieciowego zależy od jej pozycji na liście reguł dla pakietów sieciowych. Reguła znajdująca się na najwyższej pozycji na liście reguł dla pakietów sieciowych ma najwyższy priorytet.

Każda ręcznie utworzona reguła dla pakietu sieciowego jest umieszczana na końcu listy i posiada najniższy priorytet.

Zapora sieciowa wykonuje reguły w kolejności, w jakiej występują na liście reguł dla pakietów sieciowych (od góry do dołu). Zgodnie z każdą przetworzoną regułą dla pakietu sieciowego, która odpowiada określonemu połączeniu sieciowemu, Zapora sieciowa zezwala na lub blokuje dostęp sieciowy do adresu i portu określonego w ustawieniach tego połączenia sieciowego.

W celu zmiany priorytetu reguły dla pakietu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.

3. Kliknij **Reguły dla pakietów**.

   Spowoduje to otwarcie listy domyślnych reguł dla pakietów sieciowych, ustawionych przez Zaporę sieciową.

4. Z listy wybierz regułę dla pakietu sieciowego, której priorytet chcesz zmienić.

5. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.

6. Zapisz swoje zmiany.

Eksportowanie i importowanie reguł dla pakietów sieciowych

Możesz wyeksportować listę reguł dla pakietów sieciowych do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę reguł tego samego typu. Możesz użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy reguł dla pakietów sieciowych lub przeniesienia listy na inny serwer.

Eksportowanie i importowanie listy reguł dla pakietów sieciowych w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa**.
4. W sekcji **Ustawienia Zapory sieciowej** kliknij przycisk **Ustawienia**.

   To spowoduje otwarcie listy reguł dla pakietów sieciowych oraz listy reguł sieciowych dla aplikacji.
5. Przejdź do zakładki **Reguły pakietów sieciowych**.
6. W celu wyeksportowania listy reguł dla pakietów sieciowych:

   a. Wybierz reguły, które chcesz zmienić. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.

   Jeśli nie wybrałeś żadnej reguły, Kaspersky Endpoint Security wyeksportuje wszystkie reguły.

   b. Kliknij odnośnik **Eksportuj**.

   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę reguł, i wybierz folder, w którym chcesz zapisać ten plik.

   d. Zapisz plik.

   Kaspersky Endpoint Security eksportuje listę reguł do pliku XML.
7. W celu zaimportowania listy reguł dla pakietów sieciowych:

   a. Kliknij odnośnik **Importuj**.

   W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.

   b. Otwórz plik.

   Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
8. Zapisz swoje zmiany.

Eksportowanie i importowanie listy reguł dla pakietów sieciowych w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Komunikacja i Ochrona WWW → Zapora sieciowa**.

5. W celu wyeksportowania listy reguł w sekcji **Reguły pakietów sieciowych**:

   a. Wybierz reguły, które chcesz zmienić.

   b. Kliknij przycisk → **Eksportuj**.

      Kaspersky Endpoint Security eksportuje listę reguł do pliku JSON w domyślnym folderze do pobrania.

6. W celu zaimportowania listy reguł w sekcji **Reguły pakietów sieciowych**:

   a. Kliknij przycisk → **Importuj**.

      W oknie, które zostanie otwarte, wybierz plik JSON, z którego chcesz zaimportować listę reguł.

   b. Otwórz plik.

      Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku JSON.

7. Zapisz swoje zmiany.

Definiowanie reguł pakietów sieciowych w pliku XML

Zapora pozwala eksportować reguły pakietów sieciowych w formacie XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę reguł tego samego typu.

Plik XML zawiera dwa główne węzły: `Rules` i `Resources`. Węzeł `Rules` zawiera listy reguł pakietów sieciowych. Ten węzeł zawiera reguły skonfigurowane domyślnie (*wstępnie zdefiniowane reguły*) oraz dodane przez użytkownika (*reguły niestandardowe*).

Adiustacja reguł pakietów sieciowych

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

Ustawienia reguł pakietów sieciowych w formacie XML

Parametr	Opis	Wartość
`<key name="0000">`	Priorytet reguły. Im niższa wartość, tym większy priorytet.	Liczba całkowita Wartość priorytetu musi składać się z 4 cyfr. Węzły w pliku XML muszą być uporządkowane według wartości priorytetu, zaczynając od `0000`.
`RuleId`	Identyfikator reguły.	**Wstępnie zdefiniowane reguły** `100` – **Żądania do serwera DNS poprzez TCP**. `101` – **Żądania do serwera DNS poprzez UDP**. `102` – **Wysyłanie wiadomości e-mail**. `110` – **Dowolna aktywność sieciowa** (Sieci zaufane). `125` – **Dowolna aktywność sieciowa** (Sieci lokalne). `130` – **Aktywność sieciowa usługi pulpitu zdalnego**. `131` – **Połączenia TCP poprzez porty lokalne**. `132` – **Połączenia UDP poprzez porty lokalne**. `133` – **Przychodzący strumień TCP**. `134` – **Przychodzący strumień UDP**. `137` – **Odpowiedzi przychodzące ICMP Destination Unreachable**. `138` – **Pakiety przychodzące ICMP Echo Reply**. `140` – **Odpowiedzi przychodzące ICMP Time Exceeded**. `142` – **Przychodzący strumień ICMP**. `266` – **Pakiety przychodzące ICMPv6 Echo Request**.
`RuleState`	Status reguły.	`0` – wstępnie zdefiniowana reguła jest wyłączona `1` – wstępnie zdefiniowana reguła jest włączona `2` – niestandardowa reguła jest wyłączona `3` – niestandardowa reguła jest włączona
`RuleTypeId`	Identyfikator typu reguły.	`4` – reguła pakietu sieciowego.
`AppIdEx`	Identyfikator aplikacji, do której należy reguła pakietu sieciowego.	Jeśli reguła nie należy do żadnej aplikacji, wartością jest `0`.
`ResIdEx`	Główny identyfikator zasobu z ustawieniami reguły. Możesz użyć tego identyfikatora, aby zlokalizować blok z ustawieniami reguł w węźle `Resources`.	Liczba całkowita
`ResIdEx2`	Identyfikator typu sieci.	`0` – **Dowolny adres**. `50` – **Sieci zaufane**. `51` – **Sieci lokalne**. `52` – **Sieci publiczne**. `<Network Identifier>` – **Adresy z listy** (adresy są definiowane ręcznie).
`AccessFlag`	Wartość ustawienia **Akcja**.	`0` – **Zezwól**. `2` – **Zgodnie z regułami aplikacji**. `3` – **Blokuj**. `4` – **Zezwól** i **Zapisuj zdarzenia**. `6` – **Zgodnie z regułami aplikacji** i **Zapisuj zdarzenia**. `7` – **Blokuj** i **Zapisuj zdarzenia**.
`</key>`		

Węzeł `Resources` zawiera ustawienia reguł pakietów sieciowych. Niestandardowe ustawienia reguły pakietów sieciowych są wymienione w bloku `<key name="0004">`.

Adiustacja niestandardowych reguł pakietów sieciowych

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

Ustawienia niestandardowej reguły pakietów sieciowych

Parametr	Opis	Wartość
`<key name="Data">`	Identyfikator bloku parametrów.	Liczba całkowita
`RemotePorts`	Wartość ustawienia **Porty zdalne**.	Lista zakresów portów zdalnych.
`LocalPorts`	Wartość ustawienia **Porty lokalne**.	Lista zakresów portów lokalnych.

Parametr	Opis	Wartość
`AdapterBindings`	Wartość ustawienia **Karty sieciowe**.	`IpAddresses` – wartość parametru **Adresy IP**. `MacAddresses` – wartość parametru **Adresy MAC**. `AdapterName` – nazwa karty sieciowej. `InterfaceType` – wartość parametru **Typ interfejsu**: • `0` – **Inne**. • `1` – **LoopBack**. • `2` – **Sieć szerokopasmowa (ethernet)**. • `3` – **Sieć bezprzewodowa (Wi-Fi)**. • `4` – **Tunel**. • `5` – **Połączenie PPP**. • `6` – **Połączenie PPPoE**. • `7` – **Połączenie VPN**. • `8` – **Połączenie modemowe**.
`unique`	Identyfikator wewnętrzny struktury.	Liczba całkowita Zaleca się pozostawienie tego parametru bez zmian.
`Proto`	Wartość ustawienia **Protokół**.	`0` – wyłączony. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.
`Direction`	Wartość ustawienia **Kierunek**.	`1` – **Przychodzący (pakiet)**. `2` – **Wychodzący (pakiet)**. `3` – **Przychodzący / Wychodzący**. `4` – **Przychodzący**. `5` – **Wychodzący**.

Parametr	Opis	Wartość
`IcmpType`	Wartość ustawienia **Typ ICMP**.	**Protokół ICMP** `0` – **Odpowiedź echa** (ICMP) lub wyłączone. `3` – **Miejsce docelowe nieosiągalne** (ICMP). `4` – **Wygaszenie źródła**. `5` – **Przekierowanie**. `6` – **Alternatywny adres hosta**. `8` – **Żądanie echa**. `9` – **Anons routera**. `10` – **Żądanie routera**. `11` – **Przekroczony limit czasu**. `12` – **Problem z parametrem**. `13` – **Sygnatura czasowa**. `14` – **Odpowiedź na sygnaturę czasową**. `15` – **Żądanie informacji**. `16` – **Odpowiedź informacji**. `17` – **Żądanie maski adresu**. `18` – **Odpowiedź maski adresu**. `30` – **Traceroute**. `31` – **Błąd konwersji datagramu**. `32` – **Przekierowanie mobilnego hosta**. `33` – **IPv6 Where-Are-You**. `34` – **IPv6 I-Am-Here**. `35` – **Żądanie mobilnej rejestracji**. `36` – **Odpowiedź mobilnej rejestracji**. `37` – **Żądanie nazwy domeny**. `38` – **Odpowiedź nazwy domeny**. `40` – **Photuris**. **Protokół ICMPv6** `1` – **Miejsce docelowe nieosiągalne**. `2` – **Pakiet jest zbyt duży**. `3` – **Przekroczony limit czasu**. `4` – **Problem z parametrem**. `128` – **Żądanie echa**. `129` – **Odpowiedź echa**. `130` – **Kwerenda odbiornika multiemisji**. `131` – **Raport odbiornika multiemisji**. `132` – **Zakończenie działania odbiornika multiemisji**. `133` – **Żądanie routera**. `134` – **Anons routera**. `135` – **Żądanie sąsiada**. `136` – **Anons sąsiada**. `137` – **Komunikat przekierowania**. `138` – **Przenumerowanie routera**. `139` – **Kwerenda informacji węzła ICMP**. `141` – **Komunikat zwrotny żądania poszukiwania sąsiada**. `142` – **Komunikat zwrotny anonsu poszukiwania sąsiada**. `143` – **Raport odbiornika multiemisji w wersji 2**.

Parametr	Opis	Wartość
		`144` – **Komunikat żądania poszukiwania adresu agenta macierzystego**. `145` – **Komunikat odpowiedzi na poszukiwanie adresu agenta macierzystego**. `146` – **Żądanie prefiksu mobilnego**. `147` – **Anons prefiksu mobilnego**. `148` – **Komunikat żądania ścieżki certyfikacji**. `149` – **Komunikat anonsu ścieżki certyfikacji**. `151` – **Anons routera multiemisji**. `152` – **Żądanie routera multiemisji**. `153` – **Zakończenie routera multiemisji**.
`IcmpCode`	Wartość ustawienia **Kod ICMP**.	`0` – **Kod 0** lub wyłączone. `1` – **Kod 1**. `2` – **Kod 2**.
`Flags`	Wskaźnik atrybutu struktury.	Liczba całkowita Zaleca się pozostawienie tego parametru bez zmian.
`TTL`	Wartość ustawienia **Czas wygaśnięcia (TTL)**.	Wartość w sekundach. Jeśli wyłączone, wartość to `0`.
`</key>`		
`Id`	Główny identyfikator zasobu (patrz węzeł `Rules`).	Liczba całkowita
`ParentID`	Identyfikator grupy nadrzędnej.	Liczba całkowita Zaleca się pozostawienie tego parametru bez zmian.
`Flags`	Status reguły.	`6` – reguła jest wyłączona. `38` – reguła jest włączona.
`Name`	Nazwa reguły pakietów sieciowych.	Ciąg

Zarządzanie regułami sieciowymi dla aplikacji

Domyślnie Kaspersky Endpoint Security grupuje wszystkie aplikacje zainstalowane na komputerze według nazwy producenta oprogramowania, którego aktywność sieciową lub plikową monitoruje. Grupy aplikacji są dzielone na grupy zaufania. Wszystkie aplikacje i grupy aplikacji dziedziczą właściwości od grupy nadrzędnej: reguły kontroli aplikacji, reguły sieciowe dla aplikacji i ich priorytet wykonania.

Podobnie, jak w przypadku komponentu Ochrona przed włamaniami, domyślnie moduł Zapora sieciowa stosuje reguły sieciowe do grupy aplikacji podczas filtrowania aktywności sieciowej wszystkich aplikacji w tej grupie. Reguły sieciowe dla grup aplikacji definiują dla aplikacji w obrębie grupy uprawnienia dostępu do różnych połączeń sieciowych.

Domyślnie Zapora sieciowa tworzy zestaw reguł sieciowych dla każdej grupy aplikacji wykrytej na komputerze przez Kaspersky Endpoint Security. Możesz zmienić akcję Zapory sieciowej stosowaną do domyślnie utworzonych reguł sieciowych dla grupy aplikacji. Nie można modyfikować, usuwać, wyłączać oraz zmieniać priorytetu domyślnie utworzonych reguł sieciowych dla grupy aplikacji.

Możesz także utworzyć regułę sieciową dla pojedynczej aplikacji. Taka reguła będzie miała wyższy priorytet niż reguła sieciowa grupy, do której należy aplikacja.

Tworzenie reguły sieciowej dla aplikacji

Domyślnie aktywność aplikacji jest kontrolowana przez reguły sieciowe, które są definiowane dla grupy zaufania, do której Kaspersky Endpoint Security przypisał aplikację przy jej pierwszym uruchomieniu. Jeżeli jest to konieczne, możesz utworzyć reguły sieciowe dla całej grupy zaufania, dla pojedynczej aplikacji lub dla grupy aplikacji znajdujących się w grupie zaufania.

Ręcznie zdefiniowane reguły sieciowe posiadają wyższy priorytet niż reguły sieciowe, które zostały określone dla grupy zaufania. Innymi słowy, jeśli ręcznie zdefiniowane reguły dla aplikacji różnią się od reguł dla aplikacji określonych dla grupy zaufania, Zapora sieciowa kontroluje aktywność aplikacji zgodnie z ręcznie zdefiniowanymi regułami dla aplikacji.

Domyślnie, Zapora sieciowa tworzy następujące reguły sieciowe dla każdej aplikacji:

- Dowolna aktywność sieciowa w sieciach Zaufanych.
- Dowolna aktywność sieciowa w sieciach Lokalnych.
- Dowolna aktywność sieciowa w sieciach Publicznych.

Kaspersky Endpoint Security kontroluje aktywność sieciową aplikacji zgodnie z predefiniowanymi regułami sieciowymi w następujący sposób:

- Zaufane i Niski poziom ograniczeń: wszelka aktywność sieciowa jest dozwolona.
- Wysoki poziom ograniczeń i Niezaufane: wszelka aktywność sieciowa jest zablokowana.

Predefiniowane reguły aplikacji nie mogą być edytowane lub usuwane.

Możesz utworzyć regułę sieciową dla aplikacji w następujące sposoby:

- Użyj narzędzia Monitor sieci.

  Monitor sieci to narzędzie służące do wyświetlania informacji o aktywności sieciowej komputera użytkownika w czasie rzeczywistym. Jest to wygodne, ponieważ nie potrzebujesz konfigurować wszystkich ustawień reguły. Niektóre ustawienia Zapory sieciowej zostaną automatycznie uzupełnione z danych Monitora sieci. Monitor sieci jest dostępny tylko w interfejsie aplikacji.

- Skonfiguruj ustawienia Zapory sieciowej.

  To umożliwi dostosowanie ustawień Zapory sieciowej. Możesz utworzyć reguły dla dowolnej aktywności sieciowej nawet wtedy, gdy aktualnie nie ma aktywności sieciowej.

Podczas tworzenia reguł sieciowych dla aplikacji pamiętaj, że reguły pakietów sieciowych posiadają priorytet wyższy niż reguły sieciowe dla aplikacji.

Jak używać narzędzia Monitor sieci do utworzenia reguły sieciowej dla aplikacji w interfejsie aplikacji?

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Monitor sieci**.
2. Przejdź do zakładki **Aktywność sieciowa** lub **Otwarte porty**.

   Zakładka **Aktywność sieciowa** wyświetla wszystkie aktualnie aktywne połączenia sieciowe komputera. Wyświetlane są połączenia przychodzące i wychodzące.

   Na zakładce **Otwarte porty** wyświetlane są wszystkie otwarte porty sieciowe komputera.
3. Z menu kontekstowego połączenia sieciowego wybierz **Utwórz regułę sieciową dla aplikacji**.

   Zostanie otwarte okno właściwości i reguł aplikacji.
4. Wybierz zakładkę **Reguły sieciowe**.

   Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.
5. Kliknij **Dodaj**.

   Spowoduje to otwarcie właściwości reguły sieciowej.
6. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
7. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).

   Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Szablon reguły sieciowej**. Szablony reguły opisują najczęściej używane połączenia sieciowe.

   Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.
8. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w raporcie, zaznacz pole **Zapisuj zdarzenia**.
9. Kliknij **Zapisz**.

   Nowa reguła sieciowa zostanie dodana do listy.
10. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.
11. Zapisz swoje zmiany.

Jak używać ustawień Zapory sieciowej do utworzenia reguły sieciowej dla aplikacji w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
3. Kliknij **Reguły dla aplikacji**.

   Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.
4. Na liście aplikacji wybierz aplikację lub grupę aplikacji, dla której chcesz utworzyć regułę sieciową.

5. Kliknij plik prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Szczegóły i reguły**.

   Zostanie otwarte okno właściwości i reguł aplikacji.

6. Wybierz zakładkę **Reguły sieciowe**.

7. Kliknij **Dodaj**.

   Spowoduje to otwarcie właściwości reguły sieciowej.

8. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.

9. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).

   Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Szablon reguły sieciowej**. Szablony reguły opisują najczęściej używane połączenia sieciowe.

   Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.

10. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w raporcie, zaznacz pole **Zapisuj zdarzenia**.

11. Kliknij **Zapisz**.

    Nowa reguła sieciowa zostanie dodana do listy.

12. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.

13. Zapisz swoje zmiany.

Jak utworzyć regułę sieciową dla aplikacji w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.

4. W sekcji **Ustawienia Zapory sieciowej** kliknij przycisk **Ustawienia**.

   To spowoduje otwarcie listy reguł dla pakietów sieciowych oraz listy reguł sieciowych dla aplikacji.

5. Przejdź do zakładki **Reguły sieciowe dla aplikacji**.

6. Kliknij **Dodaj**.

7. W otwartym oknie wprowadź kryteria wyszukiwania aplikacji, dla których chcesz utworzyć regułę sieciową.

   Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

8. Kliknij **Odśwież**.

   Kaspersky Endpoint Security wyszuka aplikację na skonsolidowanej liście aplikacji zainstalowanych na zarządzanych komputerach. Kaspersky Endpoint Security wyświetli listę aplikacji spełniających Twoje kryteria wyszukiwania.

9. Wybierz żądaną aplikację.

10. Z listy rozwijalnej **Dodaj wybraną aplikację do grupy zaufania** wybierz **Grupy domyślne** i kliknij **OK**.

    Aplikacja zostanie dodana do domyślnej grupy.

11. Wybierz odpowiednią aplikację, a następnie wybierz **Uprawnienia aplikacji** z menu kontekstowego aplikacji.

    Zostanie otwarte okno właściwości i reguł aplikacji.

12. Wybierz zakładkę **Reguły sieciowe**.

    Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.

13. Kliknij **Dodaj**.

    Spowoduje to otwarcie właściwości reguły sieciowej.

14. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.

15. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).

    Możesz wybrać predefiniowany szablon reguły, klikając przycisk . Szablony reguły opisują najczęściej używane połączenia sieciowe.

    Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.

16. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w raporcie, zaznacz pole **Zapisuj zdarzenia**.

17. Zapisz nową regułę sieciową.

18. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.

19. Zapisz swoje zmiany.

Jak utworzyć regułę sieciową dla aplikacji w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Komunikacja i Ochrona WWW** → **Zapora sieciowa**.

5. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij odnośnik **Uprawnienia aplikacji**.

   To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.

6. Przejdź do zakładki **Uprawnienia aplikacji**.

   W lewej części okna zobaczysz listę grup zaufania, a w prawej części okna zobaczysz i ich właściwości.

7. W sekcji **Aplikacje** kliknij przycisk **Dodaj**.

   To spowoduje uruchomienie Kreatora dodawania aplikacji do grupy zaufania.

8. Wybierz odpowiednią grupę zaufania dla aplikacji.

9. Wybierz typ **Aplikacja**. Przejdź do następnego kroku.

   Jeśli chcesz utworzyć regułę sieciową dla kilku aplikacji, wybierz typ **Grupa** i określ nazwę grupy aplikacji.

10. Na otwartej liście aplikacji wybierz aplikacje, dla których chcesz utworzyć regułę sieciową.

    Użyj filtra. Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

11. Zakończ działanie Kreatora.

    Aplikacja zostanie dodana do grupy zaufania.

12. W lewej części okna wybierz odpowiednią aplikację.

13. W prawej części okna, z listy rozwijalnej wybierz **Reguły sieciowe**.

    Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.

14. Kliknij **Dodaj**.

    Spowoduje to otwarcie właściwości reguły aplikacji.

15. W polu **Nazwa reguły** wprowadź ręcznie nazwę usługi sieciowej.

16. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).

    Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Wybierz szablon reguły**. Szablony reguły opisują najczęściej używane połączenia sieciowe.

    Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.

17. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w raporcie, zaznacz pole **Zapisuj zdarzenia**.

18. Zapisz regułę sieciową.

    Nowa reguła sieciowa zostanie dodana do listy.

19. Użyj przycisku **Przenieś**, aby ustawić priorytet reguły sieciowej.

20. Zapisz swoje zmiany.

Ustawienia reguły sieciowej dla aplikacji

Parametr	Opis
Akcja	**Zezwól**. **Blokuj**.
Protokół	Kontroluje aktywność sieciową po wybranym protokole: TCP, UDP, ICMP, ICMPv6, IGMP i GRE. Jeśli wybrałeś protokół ICMP lub ICMPv6, możesz zdefiniować typ i kod pakietu ICMP. Jeżeli jako typ protokołu wybrano TCP lub UDP, możesz określić porty komputera lokalnego oraz komputera zdalnego, między którymi połączenie będzie monitorowane. Zakres możliwych wartości numerów portów: 0–65535. W każdym polu możesz wprowadzić wiele wartości oddzielonych `,` lub określ zakres wartości, używając `-`. Na przykład: • `100,101` • `100-130` • `100,110-130`
Kierunek	**Przychodzący**. **Przychodzący / Wychodzący**. **Wychodzący**.
Adresy zdalne	Adresy sieciowe zdalnych komputerów, które mogą wysyłać i/lub odbierać pakiety sieciowe. Zapora sieciowa stosuje regułę sieciową do określonego zakresu zdalnych adresów sieciowych. Możesz włączyć wszystkie adresy IP do reguły sieciowej, utworzyć oddzielną listę adresów IP, określić zakres adresów IP lub wybrać podsieć (Sieci zaufane, Sieci lokalne, Sieci publiczne). Możesz także określić nazwę DNS komputera zamiast jego adresu IP. Powinieneś używać nazw DNS tylko dla komputerów LAN lub wewnętrznych usług. Interakcja z usługami chmury (takimi jak Microsoft Azure) i innymi zasobami internetowymi powinna być zarządzana przez komponent Kontrola sieci. Jeśli w regule pakietu sieciowego dodałeś nazwę DNS, dla której nie można określić adresu IP, Kaspersky Endpoint Security wyświetli ostrzeżenie. Na liście reguł pakietów sieciowych w konsoli internetowej dodawana jest kolumna z opisem błędu. W konsoli administracyjnej (MMC) opis błędu jest niedostępny. Takie reguły pakietów są podświetlone kolorem.

Parametr	Opis
Adresy lokalne	Adresy sieciowe komputerów, które mogą wysyłać i odbierać pakiety sieciowe. Zapora sieciowa stosuje regułę sieciową do określonego zakresu lokalnych adresów sieciowych. Możesz włączyć wszystkie adresy IP do reguły sieciowej, utworzyć oddzielną listę adresów IP lub określić zakres adresów IP. Aplikacja przechowuje adresy lokalne tylko wtedy, gdy określono listę adresów zdalnych. To znaczy, gdy wybrano wartość **Adresy z listy** w polu **Adresy zdalne** i dodano co najmniej jeden adres. Zdarza się, że dla aplikacji nie można uzyskać adresu lokalnego. W takim przypadku ten parametr jest ignorowany.

Włączanie i wyłączanie reguły sieciowej dla aplikacji

W celu włączenia lub wyłączenia reguły sieciowej dla aplikacji:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa**.
3. Kliknij **Reguły dla aplikacji**.

   Spowoduje to otwarcie listy reguł aplikacji.
4. Na liście aplikacji wybierz aplikację lub grupę aplikacji, dla której chcesz utworzyć lub zmodyfikować regułę sieciową.
5. Kliknij plik prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Szczegóły i reguły**.

   Zostanie otwarte okno właściwości i reguł aplikacji.
6. Wybierz zakładkę **Reguły sieciowe**.
7. Na liście reguł sieciowych dla grupy aplikacji wybierz wymaganą regułę sieciową.

   Zostanie otwarte okno właściwości reguły sieciowej.
8. Ustaw stan **Aktywny** lub **Nieaktywny** dla reguły sieciowej.

   Nie możesz wyłączyć reguły sieciowej dla grupy aplikacji utworzonej domyślnie przez Zaporę sieciową.
9. Zapisz swoje zmiany.

Zmienianie akcji Zapory sieciowej dla reguły sieciowej dla aplikacji

Możesz zmienić akcję Zapory sieciowej stosowaną do wszystkich domyślnie utworzonych reguł sieciowych dla aplikacji lub grupy aplikacji, a także możesz zmienić akcję Zapory sieciowej stosowaną do pojedynczej niestandardowej reguły sieciowej dla aplikacji lub grupy aplikacji.

W celu zmiany akcji Zapory sieciowej stosowanej do wszystkich reguł sieciowych dla aplikacji lub grupy aplikacji:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa**.
3. Kliknij **Reguły dla aplikacji**.

   Spowoduje to otwarcie listy reguł aplikacji.
4. Jeśli chcesz zmienić akcję Zapory sieciowej, która jest stosowana do wszystkich domyślnie utworzonych reguł sieciowych, na liście wybierz aplikację lub grupę aplikacji. Ręcznie utworzone reguły sieciowe pozostają niezmienione.
5. Kliknij prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Reguły sieciowe**, a następnie wybierz działanie, które chcesz przypisać:
   - **Dziedzicz**.
   - **Zezwól**.
   - **Blokuj**.
6. Zapisz swoje zmiany.

W celu zmiany odpowiedzi Zapory sieciowej dla reguły sieciowej dla aplikacji lub grupy aplikacji:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa**.
3. Kliknij **Reguły dla aplikacji**.

   Spowoduje to otwarcie listy reguł aplikacji.
4. Na liście wybierz aplikację lub grupę aplikacji, dla której chcesz zmienić regułę sieciową.
5. Kliknij plik prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Szczegóły i reguły**.

   Zostanie otwarte okno właściwości i reguł aplikacji.
6. Wybierz zakładkę **Reguły sieciowe**.
7. Wybierz regułę sieciową, dla której chcesz zmienić działanie Zapory sieciowej.
8. Kliknij prawym przyciskiem myszy kolumnę **Uprawnienia** i z otwartego menu kontekstowego wybierz akcję, którą chcesz przypisać:
   - **Dziedzicz**.
   - **Zezwól**.
   - **Blokuj**.
   - **Zapisuj zdarzenia**.
9. Zapisz swoje zmiany.

Zmienianie priorytetu reguły sieciowej dla aplikacji

Priorytet reguły sieciowej zależy od jej pozycji na liście reguł sieciowych. Zapora sieciowa wykonuje reguły w kolejności, w jakiej występują na liście reguł sieciowych (od góry do dołu). Zgodnie z każdą przetworzoną regułą sieciową, która odpowiada określonemu połączeniu sieciowemu, Zapora sieciowa zezwala na lub blokuje dostęp sieciowy do adresu i portu określonego w ustawieniach tego połączenia sieciowego.

Ręcznie utworzone reguły sieciowe mają wyższy priorytet niż domyślne reguły sieciowe.

Nie można zmieniać priorytetu domyślnie utworzonych reguł sieciowych dla grupy aplikacji.

W celu zmiany priorytetu reguły sieciowej:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
3. Kliknij **Reguły dla aplikacji**.
   Spowoduje to otwarcie listy reguł aplikacji.
4. Na liście aplikacji wybierz aplikację lub grupę aplikację, dla której chcesz zmienić priorytet reguły sieciowej.
5. Kliknij plik prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Szczegóły i reguły**.
   Zostanie otwarte okno właściwości i reguł aplikacji.
6. Wybierz zakładkę **Reguły sieciowe**.
7. Wybierz regułę sieciową, której priorytet chcesz zmienić.
8. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.
9. Zapisz swoje zmiany.

Monitor sieci

Monitor sieci to narzędzie służące do wyświetlania informacji o aktywności sieciowej komputera użytkownika w czasie rzeczywistym.

W celu uruchomienia Monitora sieci:

W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Monitor sieci**.

Zostanie otwarte okno Monitor sieci. W tym oknie informacje o aktywności sieciowej komputera są wyświetlane na czterech zakładkach:

- Zakładka **Aktywność sieciowa** wyświetla wszystkie aktualnie aktywne połączenia sieciowe komputera. Wyświetlane są połączenia przychodzące i wychodzące. Na tej zakładce możesz także utworzyć reguły pakietów sieciowych do działania Zapory sieciowej.
- Na zakładce **Otwarte porty** wyświetlane są wszystkie otwarte porty sieciowe komputera. Na tej zakładce możesz także utworzyć reguły pakietów sieciowych i reguły aplikacji do działania Zapory sieciowej.
- Zakładka **Ruch sieciowy** zawiera informacje dotyczące ilości wychodzącego i przychodzącego ruchu sieciowego między komputerem użytkownika a innymi komputerami w sieci, do której aktualnie podłączony jest użytkownik.
- Na zakładce **Zablokowane komputery** wyświetlane są adresy IP zdalnych komputerów, których aktywność sieciowa została zablokowana przez moduł Ochrona sieci po wykryciu prób ataków sieciowych pochodzących z tych adresów IP.

Ochrona przed exploitami

Komponent Ochrona przed exploitami wykrywa kod programu, który wykorzystuje luki na komputerze, aby użyć uprawnień administratora lub wykonać szkodliwe aktywności. Na przykład, exploity mogą używać ataku typ buffer overflow (przepełnienie bufora). Aby to zrobić, exploit wysyła dużą ilość danych do aplikacji zawierającej lukę. Podczas przetwarzania tych danych aplikacja zawierająca lukę wykona szkodliwy kod. W wyniku tego ataku exploit może uruchomić nieautoryzowaną instalację szkodliwego programu. Po wykryciu, że próba uruchomienia pliku wykonywalnego z aplikacji zawierającej luki nie została zainicjowana przez użytkownika, Kaspersky Endpoint Security zablokuje uruchomienie tego pliku lub poinformuje użytkownika.

Komponent Ochrona przed exploitami dodatkowo monitoruje porty sieciowe w poszukiwaniu procesów aplikacji, które mogą zagrozić bezpieczeństwu komputera. Aplikacja pobiera informacje o takich procesach z baz danych programów antywirusowych.

Włączanie i wyłączanie modułu Ochrona przed exploitami

Domyślnie moduł Ochrona przed exploitami jest włączony i działa w trybie optymalnym. Kaspersky Endpoint Security monitoruje pliki wykonywalne uruchamiane przez aplikacje podatne na ataki. Jeśli Kaspersky Endpoint Security wykryje, że plik wykonywalny z aplikacji zawierającej luki nie został uruchomiony przez użytkownika, Kaspersky Endpoint Security wykona wybraną akcję (na przykład, zablokuje działanie).

Jak włączyć lub wyłączyć Ochronę przed exploitami w Konsoli Administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed exploitami**.
4. Użyj pola **Ochrona przed exploitami**, aby włączyć lub wyłączyć komponent.

5. W sekcji **Po wykryciu exploita** wybierz żądaną akcję:

   - **Blokuj**. Jeśli ten element jest wybrany, po wykryciu exploita, Kaspersky Endpoint Security zablokuje działania tego exploita i zarejestruje w raporcie informacje o tym exploicie.

   - **Poinformuj**. Jeśli ten element jest wybrany, gdy Kaspersky Endpoint Security wykryje exploita, zarejestruje w raporcie informacje o exploicie i doda informacje o tym exploicie do listy aktywnych zagrożeń.

6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć Ochronę przed exploitami w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ochrona hosta** → **Analiza zachowań** → **Ochrona przed exploitami**.

5. Użyj przełącznika **Ochrona przed exploitami**, aby włączyć lub wyłączyć komponent.

6. W sekcji **Działanie po wykryciu zagrożenia** wybierz żądaną akcję:

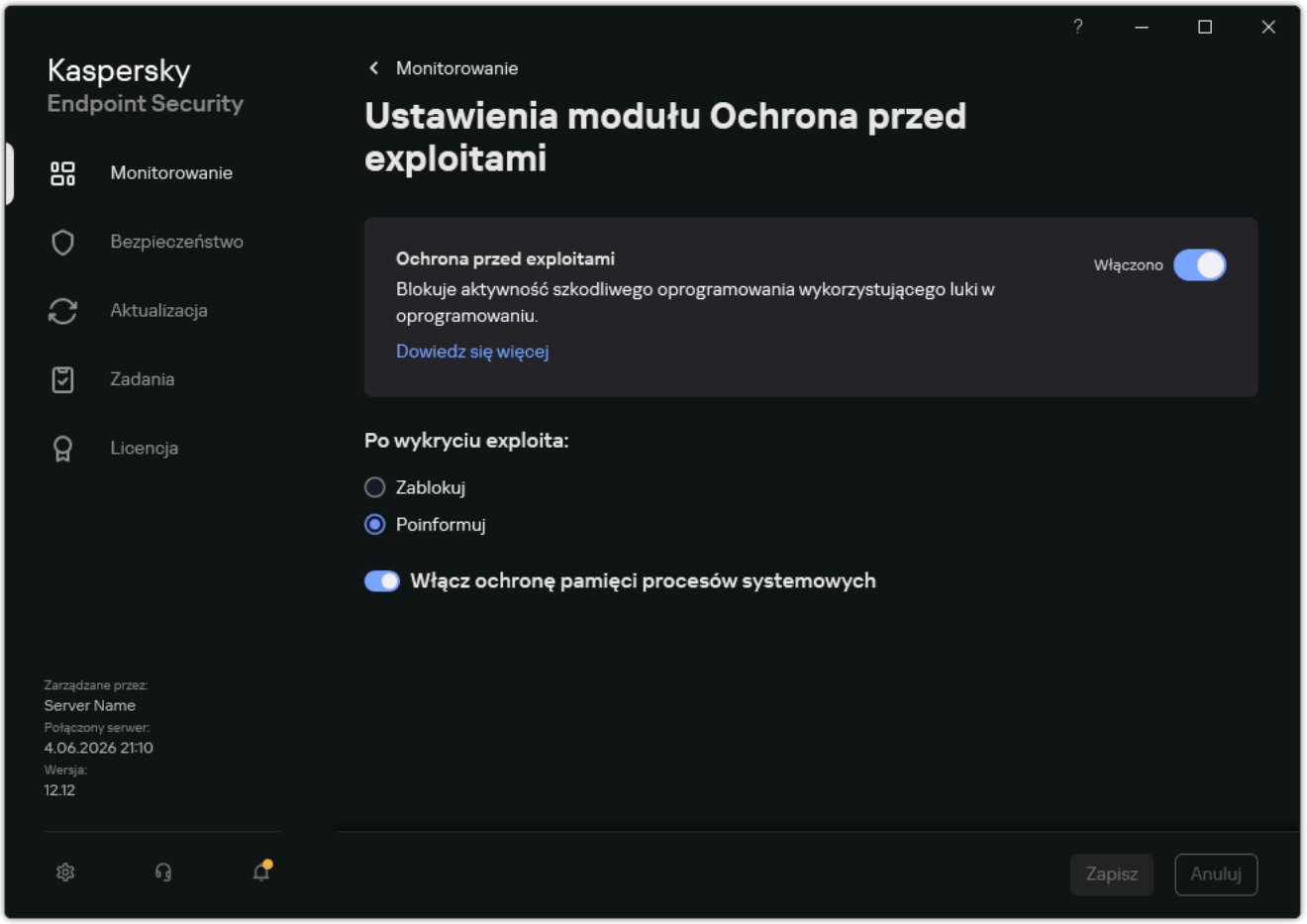
   - **Zablokuj**. Jeśli ten element jest wybrany, po wykryciu exploita, Kaspersky Endpoint Security zablokuje działania tego exploita i zarejestruje w raporcie informacje o tym exploicie.

   - **Powiadom**. Jeśli ten element jest wybrany, gdy Kaspersky Endpoint Security wykryje exploita, zarejestruje w raporcie informacje o exploicie i doda informacje o tym exploicie do listy aktywnych zagrożeń.

7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć Ochronę przed exploitami w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed exploitami**.



Ustawienia Ochrony przed exploitami

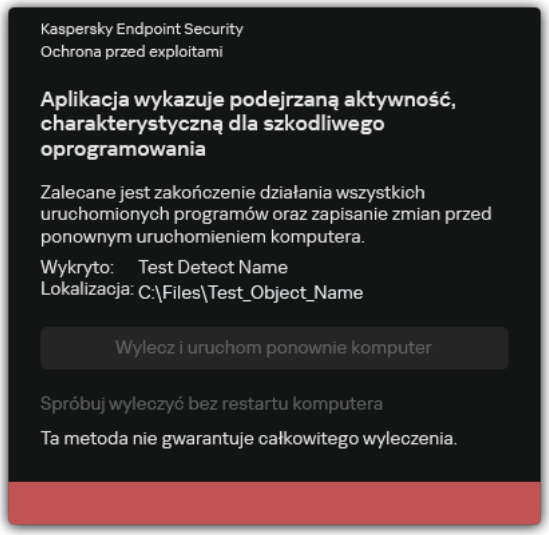
3. Użyj przełącznika **Ochrona przed exploitami**, aby włączyć lub wyłączyć komponent.

4. W sekcji **Po wykryciu exploita** wybierz żądaną akcję:

   - **Zablokuj**. Jeśli ten element jest wybrany, po wykryciu exploita, Kaspersky Endpoint Security zablokuje działania tego exploita i zarejestruje w raporcie informacje o tym exploicie.

   - **Poinformuj**. Jeśli ten element jest wybrany, gdy Kaspersky Endpoint Security wykryje exploita, zarejestruje w raporcie informacje o exploicie i doda informacje o tym exploicie do listy aktywnych zagrożeń.

5. Zapisz swoje zmiany.



Powiadomienie dotyczące aktywnego zagrożenia

Ochrona pamięci procesów systemowych

Domyślnie ochrona pamięci procesów systemowych jest włączona. Kaspersky Endpoint Security blokuje procesy zewnętrzne, które próbują uzyskać dostęp do procesów systemowych.

Jak włączyć lub wyłączyć ochronę pamięci procesów systemowych w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Ochrona przed exploitami**.

4. Użyj pola **Włącz ochronę pamięci procesów systemowych**, aby włączyć lub wyłączyć opcję.

5. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć ochronę pamięci procesów systemowych w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ochrona hosta** → **Analiza zachowań** → **Ochrona przed exploitami**.

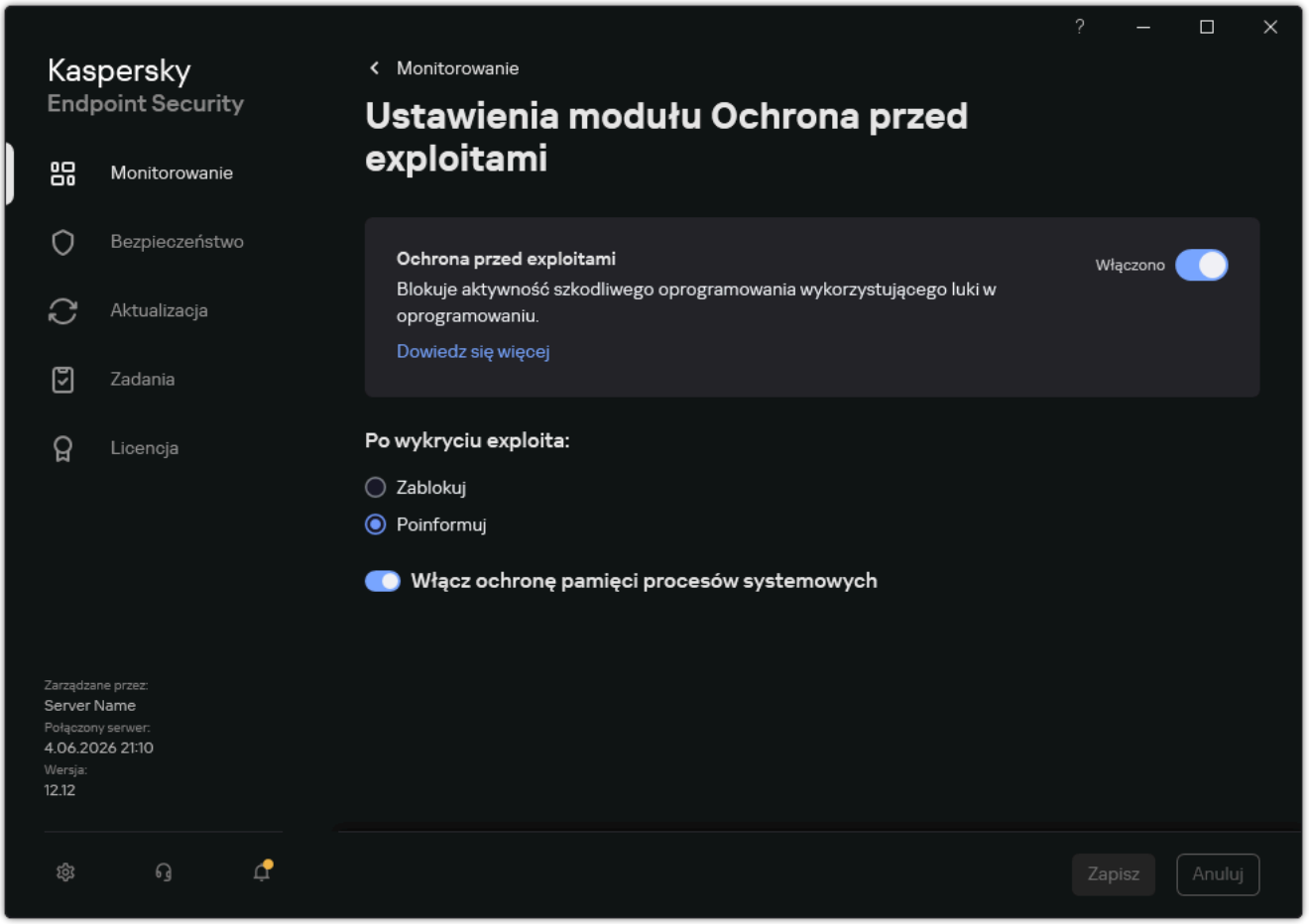
5. Użyj przełącznika **Ochrona pamięci procesów systemowych WŁĄCZONA**, aby włączyć lub wyłączyć tę funkcję.

6. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć ochronę pamięci procesów systemowych w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed exploitami**.



Ustawienia Ochrony przed exploitami

3. Użyj przełącznika **Włącz ochronę pamięci procesów systemowych**, aby włączyć lub wyłączyć tę funkcję.

4. Zapisz swoje zmiany.

Wykrywanie zachowań

Komponent Wykrywanie zachowań gromadzi dane na temat działań aplikacji na komputerze i dostarcza te informacje innym składnikom ochrony w celu udoskonalenia ich działania. Komponent Wykrywanie zachowań używa sygnatur strumieni zachowań (BSS) dla aplikacji. Jeśli aktywność aplikacji odpowiada sygnaturze strumienia zachowań, Kaspersky Endpoint Security wykona wybrane działanie. Funkcjonalność Kaspersky Endpoint Security oparta na sygnaturach strumieni zachowań zapewnia proaktywną ochronę komputera.

Komponent Wykrywanie zachowań dodatkowo monitoruje porty sieciowe w poszukiwaniu procesów aplikacji, które mogą zagrozić bezpieczeństwu komputera. Aplikacja pobiera informacje o takich procesach z baz danych programów antywirusowych.

Domyślnie moduł Wykrywanie zachowań jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. Po wykryciu szkodliwej działalności Kaspersky Endpoint Security usuwa plik wykonywalny szkodliwej aplikacji.

Nie jest zalecane wyłączanie modułu Wykrywanie zachowań, chyba że jest to faktycznie konieczne, gdyż może to zmniejszyć efektywność składników ochrony. Składniki ochrony mogą żądać danych zebranych przez komponent Wykrywanie zachowań do wykrywania zagrożeń.

Jak włączyć lub wyłączyć Wykrywanie zachowań w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Wykrywanie zachowań**.
5. Użyj pola **Wykrywanie zachowań**, aby włączyć lub wyłączyć komponent.
6. W sekcji **Akcja wykonywana po wykryciu aktywności szkodliwego oprogramowania** wybierz żądaną akcję:
   - **Usuń**. Jeśli ten element jest wybrany, po wykryciu szkodliwej aktywności program Kaspersky Endpoint Security usunie plik wykonywalny szkodliwej aplikacji i utworzy kopię zapasową pliku w Kopii zapasowej.
   - **Zablokuj**. Jeśli wybrano ten element, po wykryciu szkodliwej aktywności Kaspersky Endpoint Security zakończy działanie tej aplikacji.
   - **Poinformuj**. Jeśli ten element jest wybrany i zostanie wykryta szkodliwa aktywność aplikacji, Kaspersky Endpoint Security doda informację o szkodliwej aktywności aplikacji do listy aktywnych zagrożeń.
7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć Wykrywanie zachowań w konsoli Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta → Analiza zachowań → Wykrywanie zachowań**
5. Użyj przełącznika **Wykrywanie zachowań WŁĄCZONE**, aby włączyć lub wyłączyć komponent.

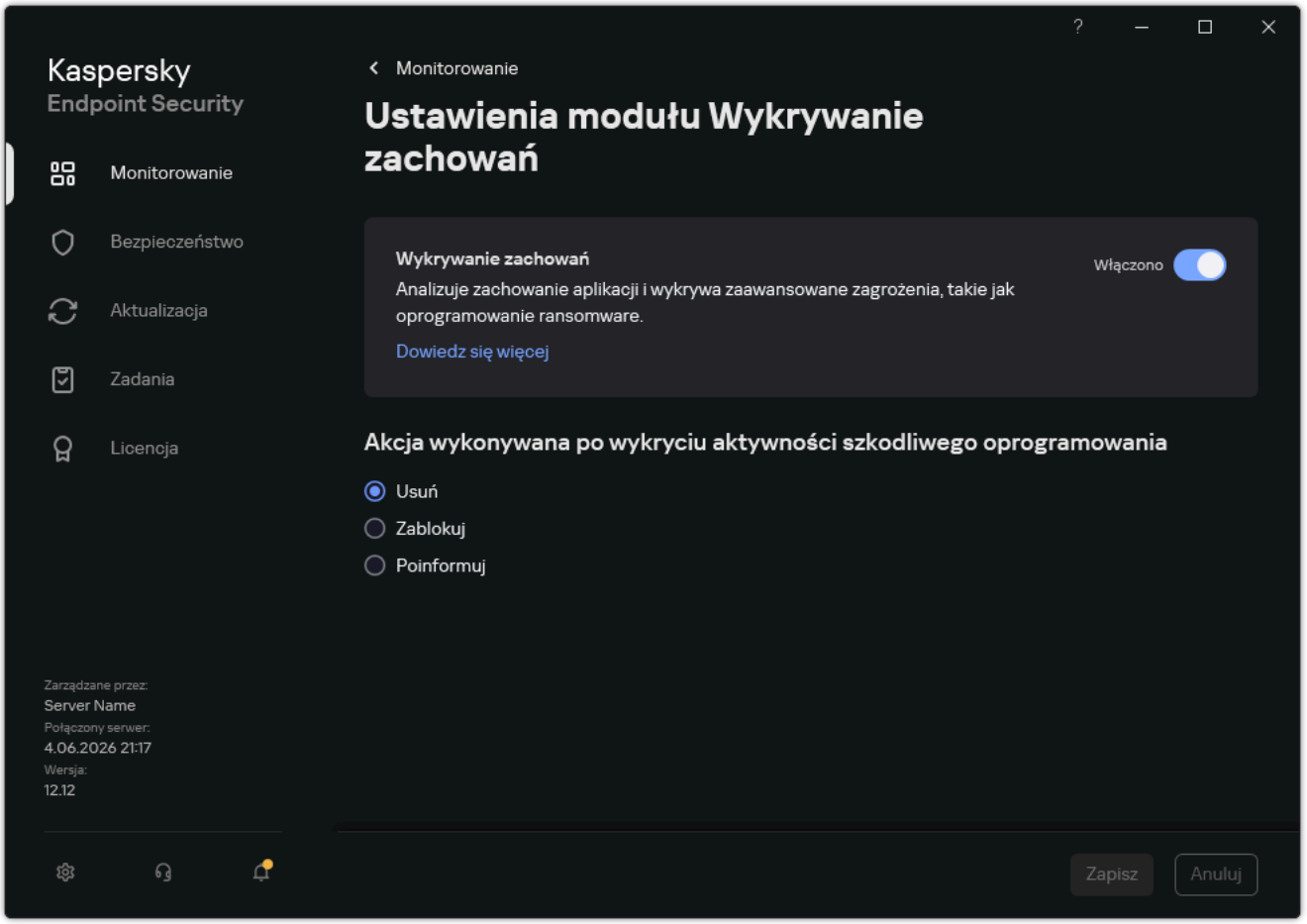
6. W sekcji **Działanie po wykryciu zagrożenia** wybierz żądaną akcję:

   - **Usuń**. Jeśli ten element jest wybrany, po wykryciu szkodliwej aktywności program Kaspersky Endpoint Security usunie plik wykonywalny szkodliwej aplikacji i utworzy kopię zapasową pliku w Kopii zapasowej.
   - **Zablokuj**. Jeśli wybrano ten element, po wykryciu szkodliwej aktywności Kaspersky Endpoint Security zakończy działanie tej aplikacji.
   - **Powiadom**. Jeśli ten element jest wybrany i zostanie wykryta szkodliwa aktywność aplikacji, Kaspersky Endpoint Security doda informację o szkodliwej aktywności aplikacji do listy aktywnych zagrożeń.

7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć Wykrywanie zachowań w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami → Wykrywanie zachowań**.



Ustawienia modułu Wykrywanie zachowań

3. Użyj przełącznika **Wykrywanie zachowań**, aby włączyć lub wyłączyć komponent.

4. W sekcji **Akcja wykonywana po wykryciu aktywności szkodliwego oprogramowania** wybierz żądaną akcję:

   - **Usuń**. Jeśli ten element jest wybrany, po wykryciu szkodliwej aktywności program Kaspersky Endpoint Security usunie plik wykonywalny szkodliwej aplikacji i utworzy kopię zapasową pliku w Kopii zapasowej.
   - **Zablokuj**. Jeśli wybrano ten element, po wykryciu szkodliwej aktywności Kaspersky Endpoint Security zakończy działanie tej aplikacji.
   - **Poinformuj**. Jeśli ten element jest wybrany i zostanie wykryta szkodliwa aktywność aplikacji, Kaspersky Endpoint Security doda informację o szkodliwej aktywności aplikacji do listy aktywnych zagrożeń.

5. Zapisz swoje zmiany.

W wyniku tego działania, jeśli Wykrywanie zachowań jest włączone, Kaspersky Endpoint Security będzie używał sygnatury strumieni zachowań do analizy aktywności aplikacji w systemie operacyjnym.

Anti-Cryptor

Od wersji Kaspersky Endpoint Security 12.12 for Windows ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym, które wcześniej było częścią komponentu Wykrywanie zachowań, jest teraz osobnym komponentem, Anti-Cryptor.

Komponent monitoruje operacje wykonywane tylko na tych plikach, które są przechowywane na urządzeniach pamięci masowej z systemem plików NTFS i które nie są zaszyfrowane za pomocą systemu szyfrowania EFS.

Komponent Anti-Cryptor analizuje aktywność w folderach współdzielonych. Jeśli to działanie jest zgodne z sygnaturą strumieni zachowań, która jest typowa dla zewnętrznego szyfrowania, Kaspersky Endpoint Security wykonuje wybraną akcję.

Aby komponent Anti-Cryptor działał, musisz włączyć komponent Wykrywanie zachowań.

Jeśli Kaspersky Endpoint Security wykryje próbę zmodyfikowania plików w folderach współdzielonych, wykona następujące działania:

- Zablokuje dostęp do modyfikacji pliku dla sesji, która zainicjowała złośliwe działanie (plik będzie tylko do odczytu).
- Utworzy kopie zapasowe plików, które są modyfikowane.
- Doda wpis do raportów dotyczących interfejsu aplikacji lokalnej i wyśle informacje o wykrytej szkodliwej aktywności do Kaspersky Security Center.
- Dodatkowo, jeśli komponent Silnik korygujący jest włączony, zmodyfikowane pliki zostają przywrócone z kopii zapasowych.

Włączanie i wyłączanie ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym

Domyślnie ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym jest włączona i działa zgodnie z zaleceniami ekspertów firmy Kaspersky. Aby skonfigurować tę funkcję, można w razie potrzeby utworzyć zakres ochrony i skonfigurować wykluczenia. Domyślnie aplikacja automatycznie identyfikuje foldery współdzielone i monitoruje aktywność plików we wszystkich folderach. W przypadku wykrycia próby zewnętrznego zaszyfrowania plików w folderach współdzielonych Kaspersky Endpoint Security zablokuje sesję zdalnego użytkownika na godzinę (domyślnie).

Po zainstalowaniu Kaspersky Endpoint Security, ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym zostanie ograniczona do momentu ponownego uruchomienia komputera.

Instrukcje włączania lub wyłączania ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Anti-Cryptor**.
4. Użyj pola wyboru **Anti-Cryptor**, aby włączyć lub wyłączyć wykrywanie aktywności typowej dla szyfrowania zewnętrznego.
5. Wybierz odpowiednią akcję, którą aplikacja będzie podejmować w przypadku wykrycia próby modyfikacji plików w folderach współdzielonych:
   - **Blokuj połączenie na N min**. Jeśli ta opcja jest zaznaczona, gdy Kaspersky Endpoint Security wykryje próbę zmodyfikowania plików w folderach współdzielonych, zablokuje dostęp do modyfikacji pliku w sesji, która zainicjowała podejrzane działanie i utworzy kopie zapasowe zmodyfikowanych plików.

     Jeśli komponent Silnik korygujący jest włączony, a opcja **Blokuj połączenie na N min** jest zaznaczona, zmodyfikowane pliki zostaną przywrócone z kopii zapasowych.

   - **Poinformuj**. Jeśli ta opcja jest zaznaczona, po wykryciu próby modyfikacji plików w folderach współdzielonych Kaspersky Endpoint Security doda informacje o tym zdarzeniu do listy aktywnych zagrożeń oraz wpis do raportów dotyczących interfejsu aplikacji lokalnej i wyśle informacje o wykrytej szkodliwej aktywności do Kaspersky Security Center.
6. W razie potrzeby edytuj zakres ochrony i zdefiniuj wykluczenia.
7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Instrukcje włączania lub wyłączania ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Analiza zachowań** → **Anti-Cryptor**.
5. Użyj przełącznika **Anti-Cryptor WŁĄCZONY**, aby włączyć lub wyłączyć wykrywanie aktywności typowej dla szyfrowania zewnętrznego.
6. Wybierz odpowiednią akcję, którą aplikacja będzie podejmować w przypadku wykrycia próby modyfikacji plików w folderach współdzielonych:

   - **Blokuj połączenie przez (min) N min**. Jeśli ta opcja jest zaznaczona, gdy Kaspersky Endpoint Security wykryje próbę zmodyfikowania plików w folderach współdzielonych, zablokuje dostęp do modyfikacji pliku w sesji, która zainicjowała podejrzane działanie i utworzy kopie zapasowe zmodyfikowanych plików.

     Jeśli komponent Silnik korygujący jest włączony, a opcja **Blokuj połączenie przez (min) N min** jest zaznaczona, zmodyfikowane pliki zostaną przywrócone z kopii zapasowych.

   - **Powiadom**. Jeśli ta opcja jest zaznaczona, po wykryciu próby modyfikacji plików w folderach współdzielonych Kaspersky Endpoint Security doda informacje o tym zdarzeniu do listy aktywnych zagrożeń oraz wpis do raportów dotyczących interfejsu aplikacji lokalnej i wyśle informacje o wykrytej szkodliwej aktywności do Kaspersky Security Center.
7. W razie potrzeby edytuj zakres ochrony i zdefiniuj wykluczenia.
8. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Instrukcje włączania lub wyłączania ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Anti-Cryptor**.
3. Użyj pola wyboru **Ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym**, aby włączyć lub wyłączyć wykrywanie aktywności typowej dla szyfrowania zewnętrznego.
4. Użyj pola wyboru **Ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym**, aby włączyć lub wyłączyć wykrywanie aktywności typowej dla szyfrowania zewnętrznego.

5. Wybierz odpowiednią akcję, którą aplikacja będzie podejmować w przypadku wykrycia próby modyfikacji plików w folderach współdzielonych:

   - **Blokuj połączenie przez (min) N min**. Jeśli ta opcja jest zaznaczona, gdy Kaspersky Endpoint Security wykryje próbę zmodyfikowania plików w folderach współdzielonych, zablokuje dostęp do modyfikacji pliku w sesji, która zainicjowała podejrzane działanie i utworzy kopie zapasowe zmodyfikowanych plików.

     Jeśli komponent Silnik korygujący jest włączony, a opcja **Blokuj połączenie przez (min) N min** jest zaznaczona, zmodyfikowane pliki zostaną przywrócone z kopii zapasowych.

   - **Poinformuj**. Jeśli ta opcja jest zaznaczona, po wykryciu próby modyfikacji plików w folderach współdzielonych Kaspersky Endpoint Security doda informacje o tym zdarzeniu do listy aktywnych zagrożeń oraz wpis do raportów dotyczących interfejsu aplikacji lokalnej i wyśle informacje o wykrytej szkodliwej aktywności do Kaspersky Security Center.

6. W razie potrzeby edytuj zakres ochrony i zdefiniuj wykluczenia.

7. Zapisz swoje zmiany.

Konfigurowanie okresu blokowania niezaufanego komputera

Niezaufany komputer to zdalny komputer, który jest używany do złośliwych działań lub szyfrowania danych. Domyślnie Kaspersky Endpoint Security blokuje sesję użytkownika zdalnego na godzinę. Po upływie okresu blokady Kaspersky Endpoint Security usuwa komputer z listy zablokowanych i przywraca mu dostęp do folderu współdzielonego.

Instrukcje konfigurowania okresu blokady niezaufanego komputera w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Anti-Cryptor**.

4. W sekcji **Działanie po wykryciu zagrożenia** wybierz **Blokuj połączenie na N min**.

5. Skonfiguruj okres blokowania niezaufanego komputera, który jest używany do złośliwych działań lub szyfrowania danych.

6. Zapisz swoje zmiany.

Instrukcje konfigurowania okresu blokady niezaufanego komputera w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ochrona hosta** → **Analiza zachowań** → **Anti-Cryptor**.

5. W obszarze **Działanie po wykryciu zagrożenia** skonfiguruj okres blokowania niezaufanego komputera, który jest używany do złośliwych działań lub szyfrowania danych.

6. Zapisz swoje zmiany.

Instrukcje konfigurowania okresu blokady niezaufanego komputera w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Anti-Cryptor**.

3. W bloku **Działanie po wykryciu zagrożenia** wybierz **Blokuj połączenie przez (min)**.

4. Skonfiguruj okres blokowania niezaufanego komputera, który jest używany do złośliwych działań lub szyfrowania danych.

5. Zapisz swoje zmiany.

W rezultacie komputer zdalny zostanie zablokowany. Aby odblokować komputer zdalny, możesz ponownie uruchomić Kaspersky Endpoint Security.

Modyfikowanie zakresu ochrony

Ten *zakres ochrony* jest listą ścieżek do folderów współdzielonych, w których Kaspersky Endpoint Security monitoruje aktywność plików. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. Domyślnie aplikacja automatycznie identyfikuje foldery współdzielone i monitoruje aktywność plików we wszystkich folderach.

Wykluczenie folderu z zakresu ochrony może zmniejszyć liczbę fałszywych alarmów, jeśli Twoja organizacja używa szyfrowania danych podczas wymiany plików za pomocą folderów współdzielonych. Na przykład Wykrywanie zachowania może dawać fałszywe alarmy, gdy użytkownik pracuje z plikami z rozszerzeniem ENC w folderze współdzielonym. Takie działanie odpowiada wzorcowi zachowania, który jest typowy dla szyfrowania zewnętrznego. Jeśli w celu ochrony danych zaszyfrowałeś pliki w folderze współdzielonym, dodaj ten folder do wykluczeń.

Możesz także wyklucz komputery, z których próby zewnętrznego szyfrowania nie muszą być zatrzymywane.

Jak edytować zakres ochrony w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Anti-Cryptor**.

4. W bloku **Obszar ochrony** wybierz **Tylko określone foldery współdzielone**.

5. Na liście folderów kliknij **Dodaj**.

6. Spowoduje to otwarcie okna, w którym należy wprowadzić ścieżkę do folderu współdzielonego, który ma zostać objęty ochroną (na przykład: `C:\Share`).

   Aby dodać folder współdzielony do zakresu ochrony, użyj ścieżki lokalnej.

7. Kliknij **OK**.

8. W razie potrzeby zdefiniuj wyłączenia z zakresu ochrony:

   a. W sekcji **Wykluczenia ze skanowania** kliknij przycisk **Wg maski**.

   b. W otwartym oknie kliknij przycisk **Dodaj**.

   c. W wyświetlonym oknie należy określić rozszerzenie pliku w formacie `*.<file extension>` lub ścieżkę folderu. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski.

      Aplikacja nie obsługuje niektórych wykluczonych rozszerzeń plików. W ten sposób można określić wykluczenie jako `*.docx` lub `**\Folder\**`.

   Można wykluczyć obiekt ze skanowania bez usuwania go z listy obiektów w zakresie ochrony. W tym celu odznacz pole obok obiektu.

9. Zapisz swoje zmiany.

Jak edytować zakres ochrony w konsoli Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ochrona hosta** → **Analiza zachowań** → **Anti-Cryptor**.

5. W bloku **Obszar ochrony** wybierz **Tylko określone foldery współdzielone**.

6. Na liście folderów kliknij **Dodaj**.

7. Spowoduje to otwarcie okna, w którym należy wprowadzić ścieżkę do folderu współdzielonego, który ma zostać objęty ochroną (na przykład: `C:\Share`).

   Aby dodać folder współdzielony do zakresu ochrony, użyj ścieżki lokalnej.

8. Kliknij **OK**.

9. W razie potrzeby zdefiniuj wyłączenia z zakresu ochrony:

   a. W górnej części okna kliknij odnośnik **Wykluczenia ze skanowania**.

   b. W otwartym oknie kliknij przycisk **Dodaj**.

c. W wyświetlonym oknie należy określić rozszerzenie pliku w formacie `*.<file extension>` lub ścieżkę folderu. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski.

Aplikacja nie obsługuje niektórych wykluczonych rozszerzeń plików. W ten sposób można określić wykluczenie jako `*.docx` lub `**\Folder\**`.

Można wykluczyć obiekt ze skanowania bez usuwania go z listy obiektów w zakresie ochrony. W tym celu odznacz pole obok obiektu.

10. Zapisz swoje zmiany.

Jak edytować zakres ochrony w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Anti-Cryptor**.
3. W bloku **Obszar ochrony** wybierz **Tylko określone foldery współdzielone**.
4. Na liście folderów kliknij **Dodaj**.
5. Spowoduje to otwarcie okna, w którym należy wprowadzić ścieżkę do folderu współdzielonego, który ma zostać objęty ochroną (na przykład: `C:\Share`).

> Aby dodać folder współdzielony do zakresu ochrony, użyj ścieżki lokalnej.

6. Kliknij **OK**.
7. W razie potrzeby zdefiniuj wyłączenia z zakresu ochrony:

a. W górnej części okna kliknij odnośnik **Wykluczenia wg maski**.

b. W otwartym oknie kliknij przycisk **Dodaj**.

c. W wyświetlonym oknie należy określić rozszerzenie pliku w formacie `*.<file extension>` lub ścieżkę folderu. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski.

Aplikacja nie obsługuje niektórych wykluczonych rozszerzeń plików. W ten sposób można określić wykluczenie jako `*.docx` lub `**\Folder\**`.

Można wykluczyć obiekt ze skanowania bez usuwania go z listy obiektów w zakresie ochrony. W tym celu odznacz pole obok obiektu.

8. Zapisz swoje zmiany.

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Wykluczenia i typy wykrytych obiektów**.
3. W sekcji **Wykluczenia** kliknij odnośnik **Zarządzaj wykluczeniami**.
4. Kliknij **Dodaj**.
5. Kliknij **Przeglądaj** i wybierz folder współdzielony.

Możesz także wprowadzić ścieżkę ręczne. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski.

- Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.

- Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.

- Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

Możesz użyć masek na początku, w środku lub na końcu ścieżki pliku. Na przykład, jeśli chcesz dodać do wykluczeń folder dla wszystkich użytkowników, należy wprowadzić maskę `?:\Users\*\Folder\`.

6. W sekcji **Składniki ochrony** wybierz moduł **Wykrywanie zachowań**.

7. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

8. Dla wykluczenia wybierz stan **Aktywny**.

   W dowolnym momencie możesz użyć przełącznika do zatrzymania wykluczenia.

9. Zapisz swoje zmiany.

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Przejdź do sekcji **Strefa zaufana**.

5. W otwartym oknie kliknij odnośnik **Wykluczenia ze skanowania w poszukiwaniu złośliwego oprogramowania**.

6. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę wykluczeń dla wszystkich komputerów w firmie. Listy wykluczeń w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Wykluczenia z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie wykluczeń zasady nadrzędnej nie jest możliwe.

7. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy wykluczeń, zaznacz pole **Zezwól na korzystanie z lokalnych wykluczeń**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę wykluczeń jako dodatek do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

   Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Ponadto jeśli to pole wyboru jest odznaczone, Kaspersky Endpoint Security ukryje skonsolidowaną listę wykluczeń ze skanowania w interfejsie użytkownika aplikacji.

8. Kliknij **Dodaj** i wybierz działanie:

   - **Kategoria**. Możesz grupować wykluczenia ze skanowania w ramach osobnych kategorii. Aby utworzyć nową kategorię, wprowadź nazwę kategorii i dodaj do niej co najmniej jedno wykluczenie ze skanowania.
   - **Nowe wykluczenie**. Kaspersky Endpoint Security dodaje nowe wykluczenie ze skanowania do katalogu głównego listy.
   - **Wybierz wykluczenie z listy**. Aby szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w System Center Configuration Manager, aplikacja zawiera *predefiniowane wykluczenia skanowania*. Dodano także predefiniowane wykluczenia ze skanowania, aby ułatwić konfigurowanie aplikacji w środowiskach wirtualnych Citrix i Vmware. Musisz wybrać predefiniowane wykluczenia ze skanowania w zależności od przeznaczenia chronionego serwera.

9. Wybierz sposób dodania wykluczenia: **Ścieżka do pliku lub folderu**.

10. Wprowadź ścieżkę do udostępnionego folderu.

    Możesz także wprowadzić ścieżkę ręczne. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski.

    - Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
    - Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.
    - Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

    Możesz użyć masek na początku, w środku lub na końcu ścieżki pliku. Na przykład, jeśli chcesz dodać do wykluczeń folder dla wszystkich użytkowników, należy wprowadzić maskę `C:\Users\*\Folder\`.

11. W sekcji **Zastosuj wykluczenie do** wybierz moduł **Wykrywanie zachowań**.

12. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

13. Dla wykluczenia wybierz stan **Dodaj do wykluczeń**.

    W dowolnym momencie możesz użyć przełącznika do zatrzymania wykluczenia.

14. Zapisz swoje zmiany.

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Wykluczenia i typy obiektów**.
4. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** → **Wykluczenia ze skanowania** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno zawierające listę wykluczeń.

5. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę wykluczeń dla wszystkich komputerów w firmie. Listy wykluczeń w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Wykluczenia z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie wykluczeń zasady nadrzędnej nie jest możliwe.
6. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy wykluczeń, zaznacz pole **Zezwól na korzystanie z lokalnych wykluczeń**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę wykluczeń jako dodatek do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

   Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Ponadto jeśli to pole wyboru jest odznaczone, Kaspersky Endpoint Security ukryje skonsolidowaną listę wykluczeń ze skanowania w interfejsie użytkownika aplikacji.

7. Kliknij **Dodaj** i wybierz działanie:

   - **Kategoria**. Możesz grupować wykluczenia ze skanowania w ramach osobnych kategorii. Aby utworzyć nową kategorię, wprowadź nazwę kategorii i dodaj do niej co najmniej jedno wykluczenie ze skanowania.
   - **Nowe wykluczenie**. Kaspersky Endpoint Security dodaje nowe wykluczenie ze skanowania do katalogu głównego listy.
   - **Wybierz wykluczenie z listy**. Aby szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w System Center Configuration Manager, aplikacja zawiera *predefiniowane wykluczenia skanowania*. Dodano także predefiniowane wykluczenia ze skanowania, aby ułatwić konfigurowanie aplikacji w środowiskach wirtualnych Citrix i Vmware. Musisz wybrać predefiniowane wykluczenia ze skanowania w zależności od przeznaczenia chronionego serwera.

8. Kliknij **Dodaj**.
9. W sekcji **Właściwości** zaznacz pole **Plik lub folder**.
10. Kliknij odnośnik **Wybierz plik lub folder** w sekcji **Opis wykluczenia ze skanowania (kliknij podkreślone elementy, aby je zmodyfikować)**, aby otworzyć okno **Nazwa pliku lub folderu**.
11. Kliknij **Przeglądaj** i wybierz folder współdzielony.

Możesz także wprowadzić ścieżkę ręczne. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski.

- Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.

- Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.

- Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

Możesz użyć masek na początku, w środku lub na końcu ścieżki pliku. Na przykład, jeśli chcesz dodać do wykluczeń folder dla wszystkich użytkowników, należy wprowadzić maskę `?:\Users\*\Folder\`.

12. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

13. W bloku **Opis wykluczenia ze skanowania (kliknij podkreślone elementy, aby je zmodyfikować)** kliknij odnośnik, aby otworzyć okno **Składniki ochrony**.

14. Zaznacz pole wyboru obok składnika **Wykrywanie zachowań**.

15. Zapisz swoje zmiany.

Dodawanie zaufanych komputerów na potrzeby zewnętrznego szyfrowania danych

Jeśli w procesie wymiany plików w Twojej organizacji stosowane jest zewnętrzne szyfrowanie danych, musisz utworzyć listę zaufanych komputerów. Kaspersky Endpoint Security nie monitoruje szyfrowania danych przez zaufane komputery.

Aby możliwe było włączenie wykluczeń adresów z ochrony folderów współdzielonych przed zewnętrznym szyfrowaniem, musi być włączona usługa Przeprowadź inspekcję logowania. Domyślnie, usługa Przeprowadź inspekcję logowania jest wyłączona (szczegółowe informacje dotyczące włączania usługi Przeprowadź inspekcję logowania można znaleźć na stronie internetowej firmy Microsoft).

Funkcjonalność wykluczania adresów z ochrony folderów sieciowych nie działa na zdalnym komputerze, jeśli zdalny komputer został włączony przed uruchomieniem Kaspersky Endpoint Security. Możesz ponownie uruchomić ten zdalny komputer po uruchomieniu Kaspersky Endpoint Security, aby upewnić się, że funkcjonalność wykluczania adresów z ochrony folderów współdzielonych działa na tym zdalnym komputerze.

Zmiana listy zaufanych komputerów może zostać zablokowana przez właściwości zasady nadrzędnej. Aby zmienić listę, musisz zezwolić na zmianę ustawień strefy zaufanej w Web Console (kłódka musi być odblokowana).

Strefy zaufane są grupowane w różny sposób w Konsoli administracyjnej (MMC) i Web Console. Sposoby zapobiegania zmianom parametrów strefy zaufanej również mogą się różnić („kłódki" mogą być inne). Zalecamy korzystanie wyłącznie z Web Console do zarządzania aplikacją. Jeśli skonfigurujesz strefę zaufaną w różnych konsolach, wtyczka zarządzająca może przywrócić „kłódkę" do stanu domyślnego.

Instrukcje dodawania zaufanego komputera na potrzeby zewnętrznego szyfrowania danych w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Anti-Cryptor**.
4. W sekcji **Wykluczenia ze skanowania** kliknij przycisk **Według nazwy lub adresu IP**.
5. W otwartym oknie kliknij przycisk **Według nazwy lub adresu IP**.
6. Wprowadź adresy IP, zakres adresów IP lub nazwy komputerów, z których próby zewnętrznego szyfrowania nie muszą być zatrzymywane.

   Na przykład:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`

- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

7. Zapisz swoje zmiany.

Instrukcje dodawania zaufanego komputera na potrzeby zewnętrznego szyfrowania danych w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Analiza zachowań** → **Anti-Cryptor**.
5. W górnej części okna kliknij odnośnik **Wykluczenia według nazwy lub adresu IP**.
6. W otwartym oknie kliknij przycisk **Dodaj**.
7. Wprowadź adresy IP, zakres adresów IP lub nazwy komputerów, z których próby zewnętrznego szyfrowania nie muszą być zatrzymywane.

   Na przykład:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. Zapisz swoje zmiany.

Instrukcje dodawania zaufanego komputera na potrzeby zewnętrznego szyfrowania danych w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Anti-Cryptor**.
3. W górnej części okna kliknij odnośnik **Wykluczenia według nazwy lub adresu IP**.
4. W otwartym oknie kliknij przycisk **Dodaj**.
5. Wprowadź adresy IP, zakres adresów IP lub nazwy komputerów, z których próby zewnętrznego szyfrowania nie muszą być zatrzymywane.

Na przykład:

- `192.168.0.0 - 192.168.255.255`
- `192.168.0.0/24`
- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

6. Zapisz swoje zmiany.

Eksportowanie i importowanie listy wykluczeń z ochrony folderów współdzielonych przed zewnętrznym szyfrowaniem

Możesz wyeksportować listę wykluczeń do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę adresów tego samego typu. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy wykluczeń lub przeniesienia listy na inny serwer.

Eksportowanie i importowanie listy wykluczeń w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Anti-Cryptor**.
4. W sekcji **Wykluczenia ze skanowania** kliknij przycisk **Według nazwy lub adresu IP**.
5. W celu wyeksportowania listy reguł:
   a. Wybierz wykluczenia, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
      Jeśli nie wybrałeś żadnego wykluczenia, Kaspersky Endpoint Security wyeksportuje wszystkie wykluczenia.
   b. Kliknij przycisk → **Eksportuj**.
   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.
   d. Zapisz plik.
      Kaspersky Endpoint Security eksportuje całą listę wykluczeń do pliku XML.
6. W celu zaimportowania listy wykluczeń:
   a. Kliknij przycisk → **Importuj**.
   b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.

c. Otwórz plik.

Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

7. Zapisz swoje zmiany.

Eksportowanie i importowanie listy wykluczeń w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Analiza zachowań** → **Anti-Cryptor**.
5. Kliknij odnośnik **Wykluczenia według nazwy lub adresu IP**.
6. W celu wyeksportowania listy reguł:

   a. Wybierz wykluczenia, które chcesz wyeksportować.

   b. Kliknij przycisk → **Eksportuj**.

   Kaspersky Endpoint Security eksportuje listę wykluczeń do pliku JSON w domyślnym folderze Pobrane.
7. W celu zaimportowania listy wykluczeń:

   a. Kliknij przycisk → **Importuj**.

   W oknie, które zostanie otwarte, wybierz plik JSON, z którego chcesz zaimportować listę wykluczeń.

   b. Otwórz plik.

   Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku JSON.
8. Zapisz swoje zmiany.

Silnik korygujący

Silnik korygujący umożliwia Kaspersky Endpoint Security wycofanie działań, które zostały wykonane przez szkodliwe oprogramowanie w systemie operacyjnym.

Podczas cofania szkodliwej aktywności w systemie operacyjnym Kaspersky Endpoint Security podejmuje działanie na następujących typach szkodliwej aktywności:

- **Aktywność plikowa**

Kaspersky Endpoint Security wykonuje następujące działania:

- Usuwa pliki wykonywalne, które zostały utworzone przez szkodliwe oprogramowanie (na wszystkich mediach za wyjątkiem dysków sieciowych).
- Usuwa pliki wykonywalne, które zostały utworzone przez programy, do których przeniknęło szkodliwe oprogramowanie.
- Przywraca pliki, które zostały zmodyfikowane lub usunięte przez szkodliwe oprogramowanie.

Funkcja odzyskiwania plików posiada kilka ograniczeń.

- **Aktywność w rejestrze**

  Kaspersky Endpoint Security wykonuje następujące działania:

  - Usuwa klucze rejestru, które zostały utworzone przez szkodliwe oprogramowanie.
  - Nie przywraca kluczy rejestru, które zostały zmodyfikowane lub usunięte przez szkodliwe oprogramowanie.

- **Aktywność w systemie**

  Kaspersky Endpoint Security wykonuje następujące działania:

  - Kończy procesy, które zostały zainicjowane przez szkodliwe oprogramowanie.
  - Kończy procesy, do których przeniknęła szkodliwa aplikacja.
  - Nie wznawia procesów zatrzymanych przez szkodliwy program.

- **Aktywność sieciowa**

  Kaspersky Endpoint Security wykonuje następujące działania:

  - Blokuje aktywność sieciową szkodliwego oprogramowania.
  - Blokuje aktywność sieciową procesów, do których przeniknęło szkodliwe oprogramowanie.

Wycofanie działań szkodliwych programów może być zainicjowane przez komponent Ochrona plików lub Wykrywanie zachowań lub podczas skanowania antywirusowego.

Wycofywanie działań szkodliwego oprogramowania oddziałuje na ściśle określony zestaw danych. Nie ma negatywnego wpływu na system operacyjny i integralność danych komputera.

Jak włączyć lub wyłączyć komponent Silnik korygujący w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Silnik korygujący**.
4. Użyj pola **Silnik korygujący**, aby włączyć lub wyłączyć komponent.
5. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć komponent Silnik korygujący w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ochrona hosta** → **Analiza zachowań** → **Silnik korygujący**.
5. Użyj przełącznika **Silnik korygujący WŁĄCZONY**, aby włączyć lub wyłączyć komponent.
6. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć komponent Silnik korygujący w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Silnik korygujący**.
3. Użyj przełącznika **Silnik korygujący**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

W wyniku tego działania, jeśli Silnik korygujący jest włączony, Kaspersky Endpoint Security wycofa działania wykonane przez szkodliwe aplikacje w systemie operacyjnym.

Kaspersky Security Network



Aby lepiej chronić Twój komputer, Kaspersky Endpoint Security wykorzystuje dane otrzymane od użytkowników z całego świata. Usługa Kaspersky Security Network została zaprojektowana do gromadzenia tych danych.

Funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Kaspersky Security Network (KSN) jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobów sieciowych oraz oprogramowania. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi programu Kaspersky Endpoint Security na nowe zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów. Jeśli uczestniczysz w Kaspersky Security Network, usługi KSN zapewniają Kaspersky Endpoint Security informacje o reputacji przeskanowanych adresów internetowych, a także informacje o kategorii i reputacji przeskanowanych plików. Więcej szczegółowych informacji o konfigurowaniu dostępu do KSN można znaleźć w pomocy do Kaspersky Security Center.

Korzystanie z Kaspersky Security Network jest dobrowolne. Aplikacja oferuje użytkownikowi możliwość korzystania z KSN podczas wstępnej konfiguracji aplikacji. Użytkownik może rozpocząć lub zakończyć uczestniczenie w KSN w dowolnym momencie.

Więcej informacji na temat wysyłania do Kaspersky informacji statystycznych, wygenerowanych w trakcie uczestnictwa w KSN, a także informacji o przechowywaniu i niszczeniu takich informacji można znaleźć w Umowie Kaspersky Security Network oraz na stronie Kaspersky. Plik ksn_<ID języka>.txt zawierający treść Oświadczenia Kaspersky Security Network znajduje się w pakiecie dystrybucyjnym aplikacji.

Infrastruktura baz danych reputacji firmy Kaspersky

Kaspersky Endpoint Security obsługuje następujące rozwiązania infrastrukturalne do pracy z bazami danych reputacji Kaspersky:

- *Kaspersky Security Network (KSN)* to rozwiązanie używane przez większość aplikacji Kaspersky. Uczestnicy KSN otrzymują informacje od firmy Kaspersky i wysyłają do Kaspersky informacje o obiektach wykrytych na komputerze użytkownika w celu dodatkowego przeanalizowania przez analityków Kaspersky i dołączenia ich do baz danych reputacji oraz statystycznych.
- *Kaspersky Private Security Network (KPSN)* to rozwiązanie, które umożliwia użytkownikom komputerów z zainstalowanym programem Kaspersky Endpoint Security lub innymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów. Sieć KPSN została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z dowolnego z następujących powodów:
  - Lokalne stacje robocze nie są połączone z internetem.
  - Przesyłanie wszelkich danych poza kraj lub poza korporacyjną sieć LAN są zabronione przez prawo lub ograniczone przez politykę bezpieczeństwa firmy.

Włączanie i wyłączanie korzystania z Kaspersky Security Network

Domyślnie, Kaspersky Endpoint Security używa Rozszerzonego trybu KSN. *Rozszerzony tryb KSN* to tryb, w którym Kaspersky Endpoint Security wysyła dodatkowe dane do Kaspersky.

Jak włączyć lub wyłączyć Użycie KSN w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Kaspersky Security Network**.
4. Użyj przełącznika **Kaspersky Security Network**, aby włączyć lub wyłączyć komponent.

   Jeśli włączyć korzystanie z KSN, Kaspersky Endpoint Security wyświetli Oświadczenie Kaspersky Security Network. Przeczytaj i zaakceptuj (jeśli wyrażasz na nie zgodę) warunki korzystania Oświadczenia Kaspersky Security Network (KSN).
5. Jeśli to konieczne, odznacz pole wyboru **Włącz rozszerzony tryb KSN**. Rozszerzony tryb KSN jest domyślnie włączony.
6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć Użycie KSN w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Kaspersky Security Network**.
5. Użyj przełącznika **Korzystanie z Kaspersky Security Network (KSN) WŁĄCZONE**, aby włączyć lub wyłączyć komponent.

   Jeśli włączyć korzystanie z KSN, Kaspersky Endpoint Security wyświetli Oświadczenie Kaspersky Security Network. Przeczytaj i zaakceptuj (jeśli wyrażasz na nie zgodę) warunki korzystania Oświadczenia Kaspersky Security Network (KSN).
6. Jeśli to konieczne, przesuń przełącznik **Użyj rozszerzonego trybu KSN** na pozycję wyłączenia. Rozszerzony tryb KSN jest domyślnie włączony.
7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć Użycie KSN w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Kaspersky Security Network**.
3. Użyj przełącznika **Kaspersky Security Network**, aby włączyć lub wyłączyć komponent.

   Jeśli włączyć korzystanie z KSN, Kaspersky Endpoint Security wyświetli Oświadczenie Kaspersky Security Network. Przeczytaj i zaakceptuj (jeśli wyrażasz na nie zgodę) warunki korzystania Oświadczenia Kaspersky Security Network (KSN).
4. Jeśli to konieczne, przesuń przełącznik **Włącz rozszerzony tryb KSN** na pozycję wyłączenia. Rozszerzony tryb KSN jest domyślnie włączony.
5. Zapisz swoje zmiany.

W wyniku tego działania, jeśli korzystanie z KSN jest włączone, Kaspersky Endpoint Security używa informacji o reputacji plików, zasobów sieciowych i aplikacji, otrzymanych z Kaspersky Security Network.

Ograniczenia Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) to rozwiązanie, które umożliwia użytkownikom komputerów z zainstalowanym programem Kaspersky Endpoint Security lub innymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów. Sieć Kaspersky Private Security Network umożliwia korzystanie z własnych lokalnych baz danych reputacji do sprawdzania reputacji obiektów (pliki lub adresy internetowe). Reputacja obiektu dodanego do lokalnej bazy danych reputacji posiada wyższy priorytet niż obiektu dodanego do KSN/KPSN. Na przykład, Kaspersky Endpoint Security skanuje komputer i żąda reputacji pliku z KSN/KPSN. Jeśli plik posiada *Niezaufane* reputację w lokalnej bazie danych reputacji, ale posiada *Zaufane* reputację w KSN/KPSN, Kaspersky Endpoint Security wykryje plik jako *Niezaufane* i podejmie działanie zdefiniowane dla wykrytych zagrożeń.

Jednakże w niektórych przypadkach Kaspersky Endpoint Security może nie zażądać reputacji obiektu z KSN/KPSN. W takiej sytuacji Kaspersky Endpoint Security nie otrzyma danych z lokalnej bazy danych reputacji KPSN. Kaspersky Endpoint Security może nie zażądać reputacji obiektu z KSN/KPSN z następujących względów:

- Aplikacje firmy Kaspersky wykorzystują bazy danych reputacji offline. Bazy danych reputacji offline zostały zaprojektowane do optymalizacji zasobów podczas działania firmy Kaspersky i do ochrony krytycznie ważnych obiektów na komputerze. Bazy danych reputacji offline są tworzone przez ekspertów z Kaspersky w oparciu o dane z Kaspersky Security Network. Aplikacje firmy Kaspersky aktualizują bazy danych reputacji offline wraz z antywirusowymi bazami danych określonej aplikacji. Jeśli bazy danych reputacji offline zawierają informacje o skanowanym obiekcie, aplikacja nie żąda reputacji tego obiektu z KSN/KPSN.

- Wykluczenia ze skanowania (strefa zaufana) są konfigurowane w ustawieniach aplikacji. W takim przypadku aplikacja nie weźmie pod uwagę reputacji obiektu w lokalnej bazie danych reputacji.

- Aplikacja wykorzystuje technologie optymalizacji skanowania, takie jak iSwift lub iChecker, lub buforuje żądania reputacji do KSN / KPSN. Jeśli taka sytuacja ma miejsce, aplikacja może nie zażądać reputacji wcześniej skanowanych obiektów.

- Aby zoptymalizować jego obciążenie, aplikacja skanuje pliki pewnego formatu i rozmiaru. Lista odpowiednich formatów i ograniczeń rozmiaru została określona przez ekspertów z Kaspersky. Ta lista jest aktualizowana o antywirusowe bazy danych aplikacji. Ustawienia optymalizacji skanowania możesz skonfigurować także w interfejsie aplikacji, na przykład, dla komponentu Ochrona plików.

- Kaspersky Endpoint Security w trybie Light Agent komunikuje się z serwerami KSN poprzez serwer proxy KSN. Bezpośrednia komunikacja z KSN nie jest obsługiwana.

Włączanie i wyłączanie dla składników ochrony trybu chmury

Tryb chmury odnosi się do trybu działania aplikacji, w którym Kaspersky Endpoint Security używa lekkiej wersji antywirusowych baz danych. Kaspersky Security Network obsługuje działanie aplikacji, gdy używana jest lekka wersja antywirusowych baz danych. Lekka wersja antywirusowych baz danych umożliwia korzystanie z około połowy pamięci RAM komputera, która inaczej zostałaby użyta ze zwykłymi bazami danych. Jeśli nie uczestniczysz w Kaspersky Security Network lub jeśli tryb chmury jest wyłączony, Kaspersky Endpoint Security pobierze pełną wersję antywirusowych baz danych z serwerów Kaspersky.

Podczas korzystania z Kaspersky Private Security Network, funkcjonalność trybu chmury jest dostępna począwszy od Kaspersky Private Security Network w wersji 3.0.

Jeśli aplikacja działa w trybie Light Agent, tryb chmury jest niedostępny.

Jak włączyć lub wyłączyć tryb chmury dla składników ochrony w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Kaspersky Security Network**.
4. Użyj pola **Włącz tryb chmury**, aby włączyć lub wyłączyć komponent.
5. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć tryb chmury dla składników ochrony w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Kaspersky Security Network**.
5. Użyj przełącznika **Użyj trybu chmury**, aby włączyć lub wyłączyć komponent.
6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć lub wyłączyć tryb chmury dla składników ochrony w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Kaspersky Security Network**.
3. Użyj przełącznika **Włącz tryb chmury**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

W wyniku tego działania, Kaspersky Endpoint Security pobiera lżejszą wersję lub pełną wersję antywirusowych baz danych podczas kolejnej aktualizacji.

Jeśli podstawowa wersja antywirusowych baz danych nie jest dostępna do użycia, Kaspersky Endpoint Security automatycznie przełączy do wersji premium antywirusowych baz danych.

Ustawienia proxy KSN

Komputery użytkowników zarządzane przez Kaspersky Security Center Administration Server mogą komunikować się z KSN bezpośrednio lub poprzez usługę KSN Proxy.

Jeśli aplikacja działa w trybie Light Agent, bezpośrednia komunikacja z KSN nie jest obsługiwana. Kaspersky Endpoint Security komunikuje się z serwerami KSN poprzez serwer proxy KSN.

Usługa KSN Proxy posiada następujące możliwości:

- Komputer użytkownika może łatwo odpytywać KSN i przesyłać informacje do KSN, nawet bez bezpośredniego dostępu do internetu.
- Usługa KSN Proxy buforuje przetwarzane dane, ograniczając obciążenie zewnętrznego kanału komunikacji sieciowej i przyśpieszając odbieranie informacji żądanych przez komputer użytkownika.

Domyślnie, po włączeniu KSN i zaakceptowaniu Oświadczenia KSN, aplikacja używa serwera proxy do połączenia z Kaspersky Security Network. Serwerem proxy używanym przez aplikację jest Serwer administracyjny Kaspersky Security Center na porcie TCP 13111. Dlatego, jeśli KSN Proxy nie jest dostępne, musisz sprawdzić następujące elementy:

- Usługa `ksnproxy` działa na serwerze administracyjnym.
- Zapora sieciowa na komputerze nie blokuje portu 13111.

Możesz skonfigurować użycie KSN Proxy w następujący sposób: włączyć lub wyłączyć KSN Proxy oraz skonfigurować port dla połączenia. Aby to zrobić, musisz otworzyć właściwości Serwera administracyjnego. Więcej szczegółowych informacji na konfiguracji KSN Proxy można znaleźć w pomocy Kaspersky Security Center. Można również włączyć lub wyłączyć KSN Proxy dla poszczególnych komputerów w zasadach Kaspersky Endpoint Security.

Jak włączyć lub wyłączyć KSN Proxy w Konsoli Administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami → Kaspersky Security Network**.
4. W sekcji **Ustawienia KSN Proxy** użyj pola **Użyj serwera administracyjnego jako serwera proxy KSN**, aby włączyć lub wyłączyć KSN Proxy.
5. Jeśli to konieczne, zaznacz pole wyboru **Użyj serwerów Kaspersky Security Network, jeżeli KSN Proxy jest niedostępny**.

   Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security używa serwerów KSN, jeśli usługa KSN Proxy jest niedostępna. Serwery KSN mogą znajdować się zarówno po stronie firmy Kaspersky, jak i stron trzecich (w przypadku korzystania z Kaspersky Private Security Network).
6. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć KSN Proxy w Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne → Kaspersky Security Network**.
5. Użyj pola **Użyj serwera administracyjnego jako serwera proxy KSN**, aby włączyć lub wyłączyć KSN Proxy.
6. Jeśli to konieczne, zaznacz pole wyboru **Użyj serwerów Kaspersky Security Network, jeśli serwer proxy KSN jest niedostępny**.

   Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security używa serwerów KSN, jeśli usługa KSN Proxy jest niedostępna. Serwery KSN mogą znajdować się zarówno po stronie firmy Kaspersky, jak i stron trzecich (w przypadku korzystania z Kaspersky Private Security Network). Domyślnie to pole wyboru nie jest zaznaczone.
7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Adres KSN Proxy jest zgodny z adresem Serwera Administracyjnego. Kiedy nazwa domeny Serwera Administracyjnego zostanie zmieniona, musisz ręcznie zaktualizować adres KSN Proxy.

Aby skonfigurować adres KSN Proxy:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz folder **Zaawansowane** → **Zdalna instalacja** → **Pakiety instalacyjne**.
3. Z menu kontekstowego folderu **Pakiety instalacyjne** wybierz **Właściwości**.
4. W zakładce **Ogólne**, w otwartym oknie, określ nowy adres serwera KSN Proxy.
5. Zapisz swoje zmiany.

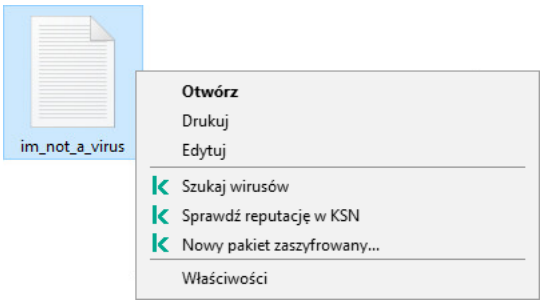
Sprawdzanie reputacji pliku w Kaspersky Security Network

Jeśli masz wątpliwości co do bezpieczeństwa pliku, możesz sprawdzić jego reputację w Kaspersky Security Network.

Możesz sprawdzić reputację pliku, jeśli zaakceptowałeś warunki Oświadczenia Kaspersky Security Network.

W celu sprawdzenia reputacji pliku w Kaspersky Security Network:

Otwórz menu kontekstowe pliku i wybierz opcję **Sprawdź reputację w KSN** (patrz rysunek poniżej).



Menu kontekstowe pliku

Kaspersky Endpoint Security wyświetla reputację pliku:

Zaufana (Kaspersky Security Network). Aplikacja uznaje plik za zaufany, jeżeli spełnia przynajmniej jeden z następujących warunków:

- plik jest podpisany cyfrowo przez zaufanego dostawcę;
- plik ma zaufaną reputację w Kaspersky Security Network;
- użytkownik umieścił aplikacje w grupie Zaufane.

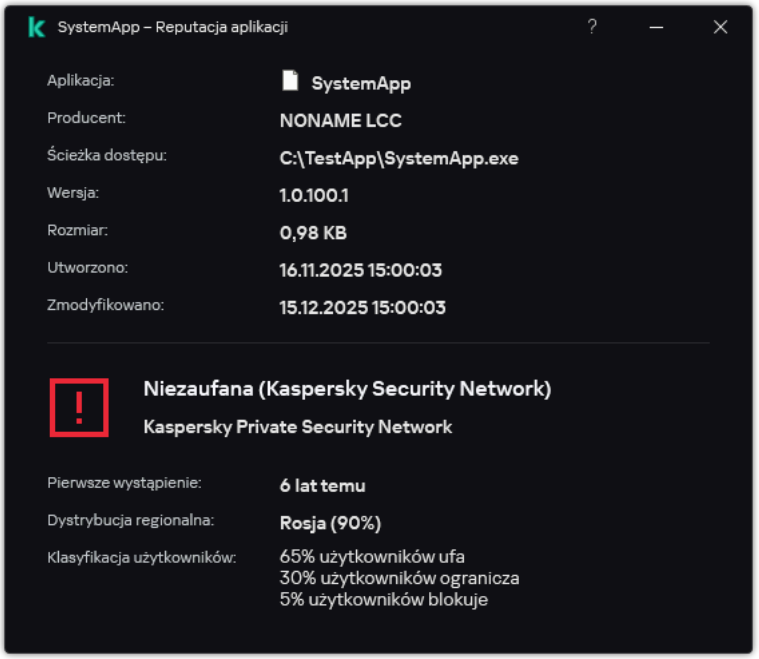
Legalne oprogramowanie, które może zostać wykorzystane przez intruzów do uszkodzenia komputera lub prywatnych danych. Nie posiadają one żadnych szkodliwych funkcji, ale mogą zostać wykorzystane przez cyberprzestępców. Szczegółowe informacje o legalnym oprogramowaniu, które może zostać użyte przez cyberprzestępców do uszkodzenia komputera lub danych osobistych użytkownika, znajdują się na stronie internetowej Encyklopedii IT Kaspersky. Możesz dodać te aplikacje do listy zaufanych.

Niezaufana (Kaspersky Security Network). Wirus lub inna aplikacja, które stwarzają zagrożenie.

Nieznana (Kaspersky Security Network). Kaspersky Security Network nie ma żadnych informacji o pliku. Możesz przeskanować plik przy użyciu antywirusowych baz danych (opcja **Szukaj wirusów** w menu kontekstowym).

Kaspersky Endpoint Security wyświetla rozwiązanie KSN, które zostało użyte do ustalenia reputacji pliku: *Kaspersky Security Network* lub *Kaspersky Private Security Network*.

Kaspersky Endpoint Security wyświetla również dodatkowe informacje o pliku (patrz rysunek poniżej).



Reputacja pliku w Kaspersky Security Network

Skanowanie połączeń szyfrowanych

Po instalacji Kaspersky Endpoint Security dodaje certyfikat Kaspersky do magazynu systemowego zaufanych certyfikatów (magazyn certyfikatów systemu Windows). Kaspersky Endpoint Security używa tego certyfikatu do skanowania połączeń szyfrowanych. Kaspersky Endpoint Security obejmuje również używanie magazynu systemowego zaufanych certyfikatów w Firefox i Thunderbird do skanowania ruchu sieciowego tych aplikacji.

Komponenty Kontrola sieci, Ochrona poczty, Ochrona WWW, Wykrywanie zachowań i Ochrona przed exploitami mogą deszyfrować i skanować ruch sieciowy przesyłany za pośrednictwem połączeń szyfrowanych przy użyciu następujących protokołów:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Włączanie skanowania połączeń szyfrowanych

Domyślnie Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych zawsze, lecz tylko wtedy, gdy zażądają tego składniki ochrony.

Jak włączyć skanowanie połączeń szyfrowanych w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
5. W sekcji **Skanowanie połączeń szyfrowanych** wybierz tryb skanowania połączeń szyfrowanych:
   - **Skanuj połączenia szyfrowane**. Kaspersky Endpoint Security nie będzie miał dostępu do zawartości stron internetowych, których adresy zaczynają się od `https://`.
   - **Skanuj połączenia szyfrowane po zgłoszeniach od składników ochrony**. Kaspersky Endpoint Security będzie skanować zaszyfrowany ruch sieciowy tylko na żądanie składników: Ochrona WWW, Ochrona poczty i Kontrola sieci.
   - **Zawsze skanuj połączenia szyfrowane**. Kaspersky Endpoint Security będzie skanował zaszyfrowany ruch sieciowy nawet wtedy, gdy składniki ochrony są wyłączone.

   Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych, które zostały nawiązane przez zaufane aplikacje, dla których skanowanie ruchu sieciowego jest wyłączone. Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych z predefiniowanej listy zaufanych stron internetowych. Predefiniowana lista zaufanych stron internetowych jest tworzona przez ekspertów Kaspersky. Ta lista jest aktualizowana o antywirusowe bazy danych aplikacji. Predefiniowaną listę zaufanych stron internetowych możesz przejrzeć tylko w interfejsie Kaspersky Endpoint Security. Listy nie można przejrzeć w Kaspersky Security Center Console.
6. W razie potrzeby dodaj wyjątki skanowania: zaufane adresy i aplikacje.
7. Skonfiguruj ustawienia skanowania połączeń szyfrowanych (patrz tabela poniżej).
8. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć skanowanie połączeń szyfrowanych w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.

5. W menu **Skanowanie połączeń szyfrowanych** włącz przełącznik **Skanowanie połączeń szyfrowanych WŁĄCZONE**.

   Gdy ten przełącznik jest wyłączony, Kaspersky Endpoint Security nie ma dostępu do zawartości stron internetowych, których adresy zaczynają się od `https://`.

6. Kliknij **Ustawienia** i wybierz tryb skanowania połączeń szyfrowanych:

   - **Skanuj połączenia szyfrowane po zgłoszeniach od składników ochrony**. Kaspersky Endpoint Security będzie skanować zaszyfrowany ruch sieciowy tylko na żądanie składników: Ochrona WWW, Ochrona poczty i Kontrola sieci.

   - **Zawsze skanuj połączenia szyfrowane**. Kaspersky Endpoint Security będzie skanował zaszyfrowany ruch sieciowy nawet wtedy, gdy składniki ochrony są wyłączone.

   > Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych, które zostały nawiązane przez zaufane aplikacje, dla których skanowanie ruchu sieciowego jest wyłączone. Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych z predefiniowanej listy zaufanych stron internetowych. Predefiniowana lista zaufanych stron internetowych jest tworzona przez ekspertów Kaspersky. Ta lista jest aktualizowana o antywirusowe bazy danych aplikacji. Predefiniowaną listę zaufanych stron internetowych możesz przejrzeć tylko w interfejsie Kaspersky Endpoint Security. Listy nie można przejrzeć w Kaspersky Security Center Console.

7. W razie potrzeby dodaj wyjątki skanowania: zaufane adresy i aplikacje.

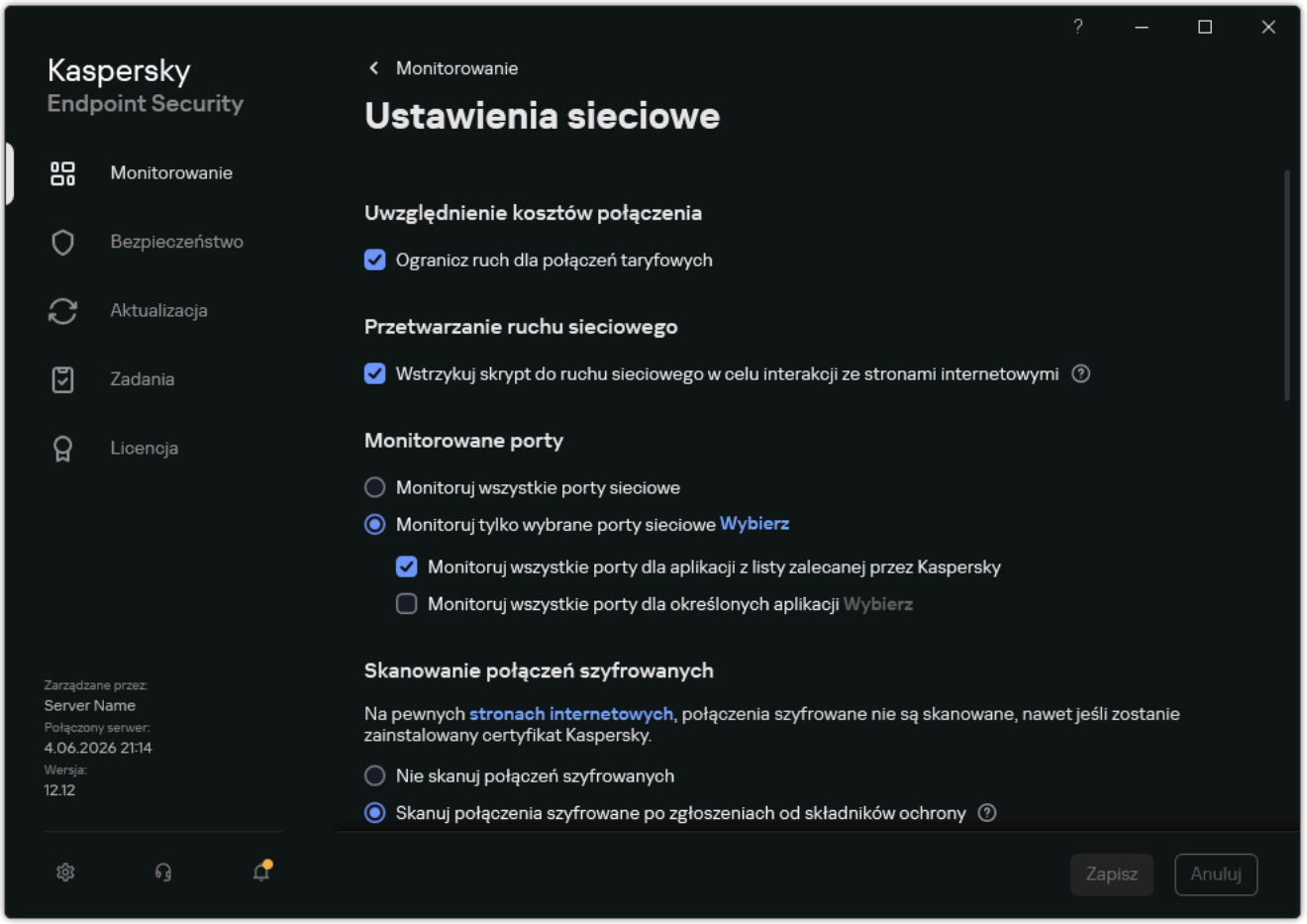
8. Skonfiguruj ustawienia skanowania połączeń szyfrowanych (patrz tabela poniżej).

9. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć skanowanie połączeń szyfrowanych w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.



Ustawienia skanowania połączeń szyfrowanych

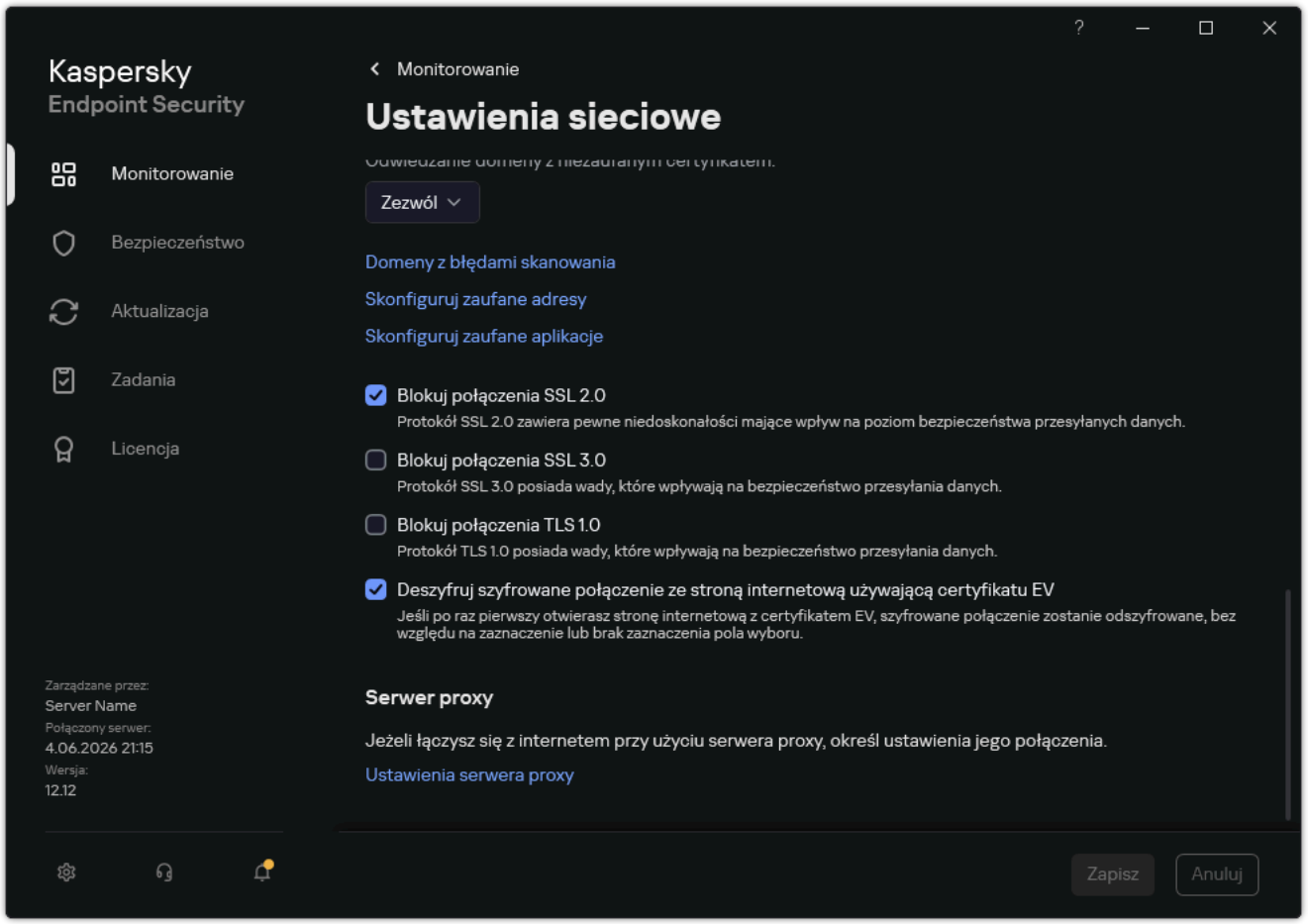
3. W sekcji **Skanowanie połączeń szyfrowanych** wybierz tryb skanowania połączeń szyfrowanych:

   - **Nie skanuj połączeń szyfrowanych**. Kaspersky Endpoint Security nie będzie miał dostępu do zawartości stron internetowych, których adresy zaczynają się od `https://`.
   - **Skanuj połączenia szyfrowane po zgłoszeniach od składników ochrony**. Kaspersky Endpoint Security będzie skanować zaszyfrowany ruch sieciowy tylko na żądanie składników: Ochrona WWW, Ochrona poczty i Kontrola sieci.
   - **Zawsze skanuj połączenia szyfrowane**. Kaspersky Endpoint Security będzie skanował zaszyfrowany ruch sieciowy nawet wtedy, gdy składniki ochrony są wyłączone.

   Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych, które zostały nawiązane przez zaufane aplikacje, dla których skanowanie ruchu sieciowego jest wyłączone. Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych z predefiniowanej listy zaufanych stron internetowych. Predefiniowana lista zaufanych stron internetowych jest tworzona przez ekspertów Kaspersky. Ta lista jest aktualizowana o antywirusowe bazy danych aplikacji. Predefiniowaną listę zaufanych stron internetowych możesz przejrzeć tylko w interfejsie Kaspersky Endpoint Security. Listy nie można przejrzeć w Kaspersky Security Center Console.

4. W razie potrzeby dodaj wyjątki skanowania: zaufane adresy i aplikacje.

5. Skonfiguruj ustawienia skanowania połączeń szyfrowanych (patrz tabela poniżej).



Dodatkowe ustawienia skanowania połączeń szyfrowanych

6. Zapisz swoje zmiany.

Ustawienia skanowania połączeń szyfrowanych

Parametr	Opis
Zaufane certyfikaty główne	Lista zaufanych certyfikatów głównych. Kaspersky Endpoint Security umożliwia zainstalowanie zaufanych certyfikatów głównych na komputerach użytkowników, gdy, na przykład, musisz wdrożyć nowe centrum certyfikacji. Aplikacja umożliwia dodanie certyfikatu do specjalnego magazynu certyfikatów Kaspersky Endpoint Security. W tym przypadku certyfikat jest uznawany za zaufany tylko dla aplikacji Kaspersky Endpoint Security. Innymi słowy, użytkownik może uzyskać dostęp do strony internetowej z nowym certyfikatem w przeglądarce. Jeśli inna aplikacja spróbuje uzyskać dostęp do strony internetowej, może pojawić się błąd połączenia w wyniku problemu z certyfikatem. Aby dodać do systemowego magazynu certyfikatów, możesz użyć zasady grupy Active Directory.
Odwiedzanie domeny z niezaufanym certyfikatem	• **Zezwól**. Podczas odwiedzania domeny z niezaufanym certyfikatem, Kaspersky Endpoint Security zezwoli na połączenie sieciowe. Podczas otwierania domeny z niezaufanym certyfikatem w przeglądarce, Kaspersky Endpoint Security wyświetla stronę HTML pokazującą ostrzeżenie i powód, z jakiego odwiedzenie tej domeny nie jest zalecane. Użytkownik może kliknąć odnośnik ze strony ostrzegającej HTML, aby uzyskać dostęp do żądanego zasobu internetowego. Jeśli usługa lub aplikacja innej firmy nawiąże połączenie z domeną z niezaufanym certyfikatem, Kaspersky Endpoint Security utworzy swój własny certyfikat, aby przeskanować ruch sieciowy. Nowy certyfikat posiada stan *Niezaufane*. To jest konieczne, aby ostrzec aplikację innej firmy przed niezaufanym połączeniem, ponieważ strona HTML nie może zostać wyświetlona w tym przypadku, a połączenie może zostać nawiązane w tle. • **Zablokuj**. Podczas odwiedzania domeny z niezaufanym certyfikatem, Kaspersky Endpoint Security zablokuje połączenie sieciowe. Podczas otwierania domeny z niezaufanym certyfikatem w przeglądarce, Kaspersky Endpoint Security wyświetla stronę HTML pokazującą powód zablokowania tej domeny.
Odwiedzanie domeny z błędem skanowania połączeń szyfrowanych	• **Zablokuj**. Jeśli wystąpi błąd skanowania połączenia szyfrowanego, Kaspersky Endpoint Security zablokuje połączenie sieciowe. • **Zezwól na domenę i dodaj ją do wykluczeń**. Jeśli wystąpi błąd skanowania połączenia szyfrowanego, Kaspersky Endpoint Security doda domenę, w której wystąpił błąd, do listy domen z błędami skanowania i nie będzie monitorował szyfrowanego ruchu sieciowego, gdy ta domena będzie odwiedzana. Możesz przejrzeć listę domen z błędami skanowania połączeń szyfrowanych tylko w lokalnym interfejsie aplikacji. Aby wyczyścić zawartość listy, należy wybrać **Zablokuj**. Kaspersky Endpoint Security także generuje zdarzenie dla błędu skanowania połączenia szyfrowanego.

Parametr	Opis
Blokuj połączenia SSL 2.0	Jeśli pole jest zaznaczone, aplikacja monitoruje i blokuje połączenia sieciowe nawiązane przez protokół SSL 2.0. Jeśli pole jest zaznaczone, aplikacja nie blokuje połączeń sieciowych nawiązanych przez protokół SSL 2.0. Aplikacja nie monitoruje jednak ruchu sieciowego przesyłanego za pośrednictwem tego protokołu.
Blokuj połączenia SSL 3.0	Jeśli pole jest zaznaczone, aplikacja zablokuje połączenia sieciowe nawiązane po protokole SSL 3.0. Jeśli pole jest zaznaczone, aplikacja nie blokuje połączeń sieciowych nawiązanych przez protokół SSL 3.0. Aplikacja monitoruje ruch sieciowy przesyłany za pośrednictwem tego protokołu. Wszystkie komponenty aplikacji działają bez ograniczeń.
Blokuj połączenia TLS 1.0	Jeśli pole jest zaznaczone, aplikacja zablokuje połączenia sieciowe nawiązane po protokole TLS 1.0. Jeśli pole jest zaznaczone, aplikacja nie blokuje połączeń sieciowych nawiązanych przez protokół TLS 1.0. Aplikacja monitoruje ruch sieciowy przesyłany za pośrednictwem tego protokołu. Wszystkie komponenty aplikacji działają bez ograniczeń.
Deszyfruj szyfrowane połączenie ze stroną internetową używającą certyfikatu EV	Certyfikaty EV (Extended Validation Certificate) potwierdzają autentyczność stron internetowych i zwiększają ochronę połączenia. Przeglądarki używają ikony kłódki w paskach adresu, aby pokazać, że strona internetowa posiada certyfikat EV. W przeglądarkach pasek adresu może być częściowo lub całkowicie oznaczony na zielono. Jeśli pole jest zaznaczone, aplikacja deszyfruje i monitoruje połączenia szyfrowane ze stronami internetowymi, które używają certyfikatu EV. Jeśli pole jest odznaczone, aplikacja nie ma dostępu do zawartości ruchu sieciowego HTTPS. Z tego powodu aplikacja monitoruje ruch sieciowy HTTPS tylko w oparciu o adres strony internetowej, na przykład: `https://bing.com`. Jeśli otwierasz stronę internetową z certyfikatem EV po raz pierwszy, zaszyfrowane połączenie zostanie odszyfrowane niezależnie od tego, czy pole jest zaznaczone.

Instalowanie zaufanych certyfikatów głównych

Kaspersky Endpoint Security umożliwia zainstalowanie zaufanych certyfikatów głównych na komputerach użytkowników, gdy, na przykład, musisz wdrożyć nowe centrum certyfikacji. Aplikacja umożliwia dodanie certyfikatu do specjalnego magazynu certyfikatów Kaspersky Endpoint Security. W tym przypadku certyfikat jest uznawany za zaufany tylko dla aplikacji Kaspersky Endpoint Security. Innymi słowy, użytkownik może uzyskać dostęp do strony internetowej z nowym certyfikatem w przeglądarce. Jeśli inna aplikacja spróbuje uzyskać dostęp do strony internetowej, może pojawić się błąd połączenia w wyniku problemu z certyfikatem. Aby dodać do systemowego magazynu certyfikatów, możesz użyć zasady grupy Active Directory.

Zmiana listy zaufanych certyfikatów głównych może zostać zablokowana przez właściwości zasady nadrzędnej. Aby zmienić listę, musisz zezwolić na zmianę ustawień strefy zaufanej w Web Console (kłódka musi być odblokowana).

Strefy zaufane są grupowane w różny sposób w Konsoli administracyjnej (MMC) i Web Console. Sposoby zapobiegania zmianom parametrów strefy zaufanej również mogą się różnić („kłódki" mogą być inne). Zalecamy korzystanie wyłącznie z Web Console do zarządzania aplikacją. Jeśli skonfigurujesz strefę zaufaną w różnych konsolach, wtyczka zarządzająca może przywrócić „kłódkę" do stanu domyślnego.

Jak w Konsoli administracyjnej (MMC) zainstalować zaufane certyfikaty główne?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.

4. W sekcji **Zaufane certyfikaty główne** kliknij przycisk **Dodaj**.
5. To spowoduje otwarcie okna, w którym wybierz zaufany certyfikat główny.
   Kaspersky Endpoint Security obsługuje certyfikaty z rozszerzeniami PEM, DER i CRT.
6. Zapisz swoje zmiany.

Jak w Web Console i Cloud Console zainstalować zaufane certyfikaty główne?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
5. Kliknij odnośnik **Zaufane certyfikaty główne**.
6. To spowoduje otwarcie okna, w którym kliknij **Dodaj** i wybierz zaufany certyfikat główny.
   Kaspersky Endpoint Security obsługuje certyfikaty z rozszerzeniami PEM, DER i CRT.
7. Zapisz swoje zmiany.

Jak w interfejsie aplikacji zainstalować zaufane certyfikaty główne?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
3. W sekcji **Skanowanie połączeń szyfrowanych** kliknij przycisk **Pokaż certyfikaty**.
4. To spowoduje otwarcie okna, w którym kliknij **Dodaj** i wybierz zaufany certyfikat główny.
   Kaspersky Endpoint Security obsługuje certyfikaty z rozszerzeniami PEM, DER i CRT.
5. Zapisz swoje zmiany.

W wyniku tego działania, podczas skanowania ruchu sieciowego, jako dodatek do systemowego magazynu certyfikatów Kaspersky Endpoint Security używa swojego własnego magazynu certyfikatów.

Skanowanie połączeń szyfrowanych z użyciem niezaufanego certyfikatu

Po instalacji Kaspersky Endpoint Security dodaje certyfikat Kaspersky do magazynu systemowego zaufanych certyfikatów (magazyn certyfikatów systemu Windows). Kaspersky Endpoint Security używa tego certyfikatu do skanowania połączeń szyfrowanych. Podczas odwiedzania domeny z niezaufanym certyfikatem możesz zezwolić na lub zablokować dostęp użytkownika do tej domeny (patrz instrukcje poniżej).

Jeśli zezwoliłeś użytkownikowi na odwiedzanie domen z niezaufanymi certyfikatami, Kaspersky Endpoint Security wykona następujące działania:

- Podczas odwiedzania domeny z niezaufanym certyfikatem w *przeglądarce*, Kaspersky Endpoint Security używa certyfikatu Kaspersky do skanowania ruchu sieciowego. Kaspersky Endpoint Security wyświetla stronę HTML z ostrzeżeniem i informacją, dlaczego nie jest zalecane odwiedzenie odpowiedniej domeny (patrz rysunek poniżej). Użytkownik może kliknąć odnośnik ze strony ostrzegającej HTML, aby uzyskać dostęp do żądanego zasobu internetowego. Po kliknięciu tego odnośnika, w ciągu następnej godziny Kaspersky Endpoint Security nie wyświetli ostrzeżeń o niezaufanym certyfikacie podczas odwiedzania innych zasobów na tej samej domenie. Kaspersky Endpoint Security także generuje zdarzenie o nawiązaniu zaszyfrowanego połączenia z niezaufanym certyfikatem.

  W niektórych przypadkach Kaspersky Endpoint Security nie może powodów technicznych wyświetlić w przeglądarce strony HTML z ostrzeżeniem (patrz rysunek poniżej). Na przykład, jeśli zasób sieciowy korzysta z nieaktualnej wersji protokołu sieciowego i niestandardowego portu. W takich przypadkach Kaspersky Endpoint Security blokuje dostęp do danej domeny, a przeglądarka wyświetla standardowe okno `ERR_CONNECTION_RESET`. Aby uzyskać dostęp do zasobu internetowego, można dodać domenę do wykluczeń lub użyć zaufanego certyfikatu.

- Jeśli *usługa lub aplikacja innej firmy* nawiąże połączenie z domeną z niezaufanym certyfikatem, Kaspersky Endpoint Security utworzy swój własny certyfikat, aby przeskanować ruch sieciowy. Nowy certyfikat posiada stan *Niezaufany*. To jest konieczne, aby ostrzec aplikację innej firmy przed niezaufanym połączeniem, ponieważ strona HTML nie może zostać wyświetlona w tym przypadku, a połączenie może zostać nawiązane w tle. Dlatego też, jeśli aplikacja innej firmy ma wbudowane narzędzia do weryfikacji certyfikatu, połączenie może zostać przerwane. W tym przypadku musisz skontaktować się z właścicielem domeny i skonfigurować zaufane połączenie. Jeśli skonfigurowanie zaufanego połączenia nie jest możliwe, możesz dodać tę aplikację innej firmy do listy zaufanych aplikacji. Kaspersky Endpoint Security także generuje zdarzenie o nawiązaniu zaszyfrowanego połączenia z niezaufanym certyfikatem.

Jak w Konsoli administracyjnej (MMC) skonfigurować skanowanie połączeń szyfrowanych z niezaufanym certyfikatem?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
4. W sekcji **Skanowanie połączeń szyfrowanych** kliknij przycisk **Ustawienia zaawansowane**.
5. W oknie, które zostanie otwarte, wybierz tryb działania aplikacji podczas odwiedzania domeny z niezaufanym certyfikatem: **Zezwól** or **Zablokuj**.
6. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console skonfigurować skanowanie połączeń szyfrowanych z niezaufanym certyfikatem?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.

5. W sekcji **Skanowanie połączeń szyfrowanych** kliknij odnośnik **Ustawienia**.

6. W oknie, które zostanie otwarte, wybierz tryb działania aplikacji podczas odwiedzania domeny z niezaufanym certyfikatem: **Zezwól na połączenie** or **Blokuj połączenie**.

7. Zapisz swoje zmiany.

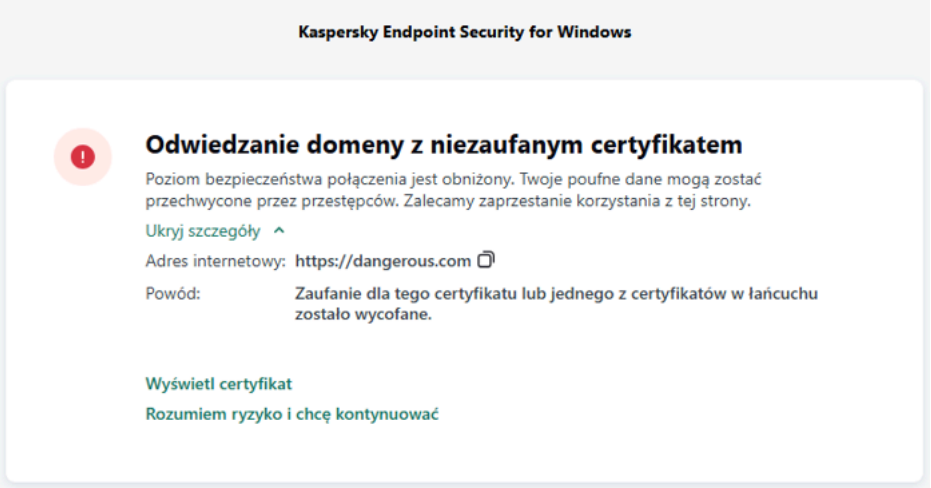
Jak w interfejsie aplikacji skonfigurować skanowanie połączeń szyfrowanych z niezaufanym certyfikatem?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.

3. W bloku **Skanowanie połączeń szyfrowanych** wybierz tryb działania aplikacji podczas odwiedzania domeny z niezaufanym certyfikatem: **Zezwól** lub **Zablokuj**.

4. Zapisz swoje zmiany.



Ostrzeżenie na temat odwiedzania domeny z niezaufanym certyfikatem

Dodawanie certyfikatu Kaspersky do własnego magazynu certyfikatów

Przeglądarki i klienci pocztowi używają certyfikatu do weryfikacji bezpieczeństwa i autentyczności zasobów sieciowych. Certyfikat zapewnia również szyfrowanie danych pomiędzy zasobami sieciowymi a użytkownikiem. Większość przeglądarek i klientów pocztowych korzysta z zaufanego magazynu certyfikatów (magazynu certyfikatów systemu Windows). Na przykład Google Chrome. Niektóre przeglądarki i klienci pocztowi domyślnie korzystają z własnego magazynu certyfikatów zamiast magazynu certyfikatów systemu Windows. Na przykład Firefox i Thunderbird.

Po instalacji Kaspersky Endpoint Security dodaje certyfikat Kaspersky do magazynu systemowego zaufanych certyfikatów (magazyn certyfikatów systemu Windows). Jeśli program Kaspersky Security Center jest zainstalowany w Twojej organizacji, a zasada jest stosowana na komputerze, Kaspersky Endpoint Security automatycznie umożliwia korzystanie z magazynu certyfikatów Windows w przeglądarkach i klientach pocztowych, aby skanować ruch sieciowy tych aplikacji. Jeśli zasada nie jest stosowana na komputerze, możesz wybrać magazyn certyfikatów, który będzie używany przez przeglądarki i klientów pocztowych. W przypadku wyboru własnego magazynu certyfikatów, ręcznie dodaj do magazynu certyfikat Kaspersky. To pomoże uniknąć błędów podczas pracy z ruchem HTTPS.

Aby skanować ruch sieciowy w przeglądarce Mozilla Firefox i kliencie poczty Thunderbird, musisz włączyć Skanowanie połączeń szyfrowanych. Jeśli Skanowanie połączeń szyfrowanych jest wyłączone, aplikacja nie skanuje ruchu sieciowego w przeglądarce Mozilla Firefox oraz w kliencie poczty Thunderbird. Należy także włączyć skanowanie połączeń szyfrowanych, aby skanować ruch sieciowy w klientach pocztowych MyOffice Mail i R7-Office Organizer.

Zanim dodasz certyfikat do własnego magazynu certyfikatów przeglądarki lub agenta poczty, wyeksportuj certyfikat Kaspersky z panelu sterowania systemu Windows (właściwości Internetu). Więcej o dodaniu certyfikatu do magazynu możesz dowiedzieć się np. na stronie pomocy technicznej Mozilla.

Możesz wybrać magazyn certyfikatów tylko w lokalnym interfejsie aplikacji.

W celu wybrania magazynu certyfikatów do skanowania połączeń szyfrowanych w przeglądarkach i klientach pocztowych:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
3. W sekcji **Skanowanie połączeń szyfrowanych** zaznacz pole **Do skanowania szyfrowanych połączeń w aplikacjach z własnym magazynem certyfikatów użyj**.
4. Wybierz magazyn certyfikatów:
   - **Magazyn certyfikatów Windows (zalecane)**. Certyfikat główny Kaspersky zostanie dodany do tego magazynu podczas instalacji Kaspersky Endpoint Security.
   - **Własny magazyn certyfikatów**. Mozilla Firefox i Thunderbird używają swoich własnych magazynów certyfikatów. Jeśli wybrano magazyn certyfikatów aplikacji Mozilla, powinieneś ręcznie dodać certyfikat główny Kaspersky do tego magazynu z poziomu właściwości przeglądarki.

     Klienci pocztowi MyOffice Mail i R7-Office Organizer również korzystają z własnego magazynu certyfikatów.
5. Zapisz swoje zmiany.

Wyłączanie połączeń szyfrowanych ze skanowania

Większość zasobów internetowych korzysta z połączeń szyfrowanych. Eksperci z Kaspersky zalecają włączenie opcji Skanowanie połączeń szyfrowanych. Jeśli skanowanie połączeń szyfrowanych zakłóca czynności związane z pracą, możesz dodać stronę internetową do wykluczeń zwanych *zaufanymi adresami*. W tym przypadku program Kaspersky Endpoint Security nie skanuje ruchu sieciowego HTTPS zaufanych adresów internetowych, gdy komponenty Ochrona WWW, Ochrona poczty, Kontrola sieci wykonują swoją pracę.

Jeśli zaufana aplikacja korzysta z połączenia szyfrowanego, możesz wyłączyć skanowanie połączeń szyfrowanych dla tej aplikacji. Na przykład, można wyłączyć skanowanie połączeń szyfrowanych w poszukiwaniu aplikacji do przechowywania w chmurze, które używają uwierzytelniania dwuskładnikowego z własnym certyfikatem.

Zmiana listy zaufanych adresów może zostać zablokowana przez właściwości zasady nadrzędnej. Aby zmienić listę, musisz zezwolić na zmianę ustawień strefy zaufanej w Web Console (kłódka musi być odblokowana).

Strefy zaufane są grupowane w różny sposób w Konsoli administracyjnej (MMC) i Web Console. Sposoby zapobiegania zmianom parametrów strefy zaufanej również mogą się różnić („kłódki" mogą być inne). Zalecamy korzystanie wyłącznie z Web Console do zarządzania aplikacją. Jeśli skonfigurujesz strefę zaufaną w różnych konsolach, wtyczka zarządzająca może przywrócić „kłódkę" do stanu domyślnego.

Jak wykluczyć adres internetowy ze skanowania połączeń szyfrowanych w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
4. W sekcji **Skanowanie połączeń szyfrowanych** kliknij przycisk **Skonfiguruj zaufane adresy**.
5. Kliknij **Dodaj**.
6. Wprowadź nazwę domeny lub adres IP, jeśli nie chcesz, żeby Kaspersky Endpoint Security skanował połączenia szyfrowane nawiązywane podczas odwiedzania tej domeny.

   Kaspersky Endpoint Security obsługuje znak `*` do wprowadzenia maski w nazwie domeny.

   Kaspersky Endpoint Security nie obsługuje symbolu `*` dla adresów IP. Za pomocą maski podsieci możesz wybrać zakres adresów IP (na przykład: 198.51.100.0/24).

   Na przykład:

   - `domain.com` – wpis jest częścią następujących adresów: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Wpis nie jest częścią poddomen (na przykład: `subdomain.domain.com`).
   - `subdomain.domain.com` – wpis jest częścią następujących adresów: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Wpis nie jest częścią domeny `domain.com`.
   - `*.domain.com` – wpis jest częścią następujących adresów: `https://movies.domain.com`, `https://images.domain.com/page123`. Wpis nie jest częścią domeny `domain.com`.
7. Zapisz swoje zmiany.

Jak wykluczyć adres internetowy ze skanowania połączeń szyfrowanych w usługach Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
5. W sekcji **Skanowanie połączeń szyfrowanych** kliknij przycisk **Zaufane domeny**.
6. Kliknij **Dodaj**.
7. Wprowadź nazwę domeny lub adres IP, jeśli nie chcesz, żeby Kaspersky Endpoint Security skanował połączenia szyfrowane nawiązywane podczas odwiedzania tej domeny.

   Kaspersky Endpoint Security obsługuje znak `*` do wprowadzenia maski w nazwie domeny.

   > Kaspersky Endpoint Security nie obsługuje symbolu `*` dla adresów IP. Za pomocą maski podsieci możesz wybrać zakres adresów IP (na przykład: 198.51.100.0/24).

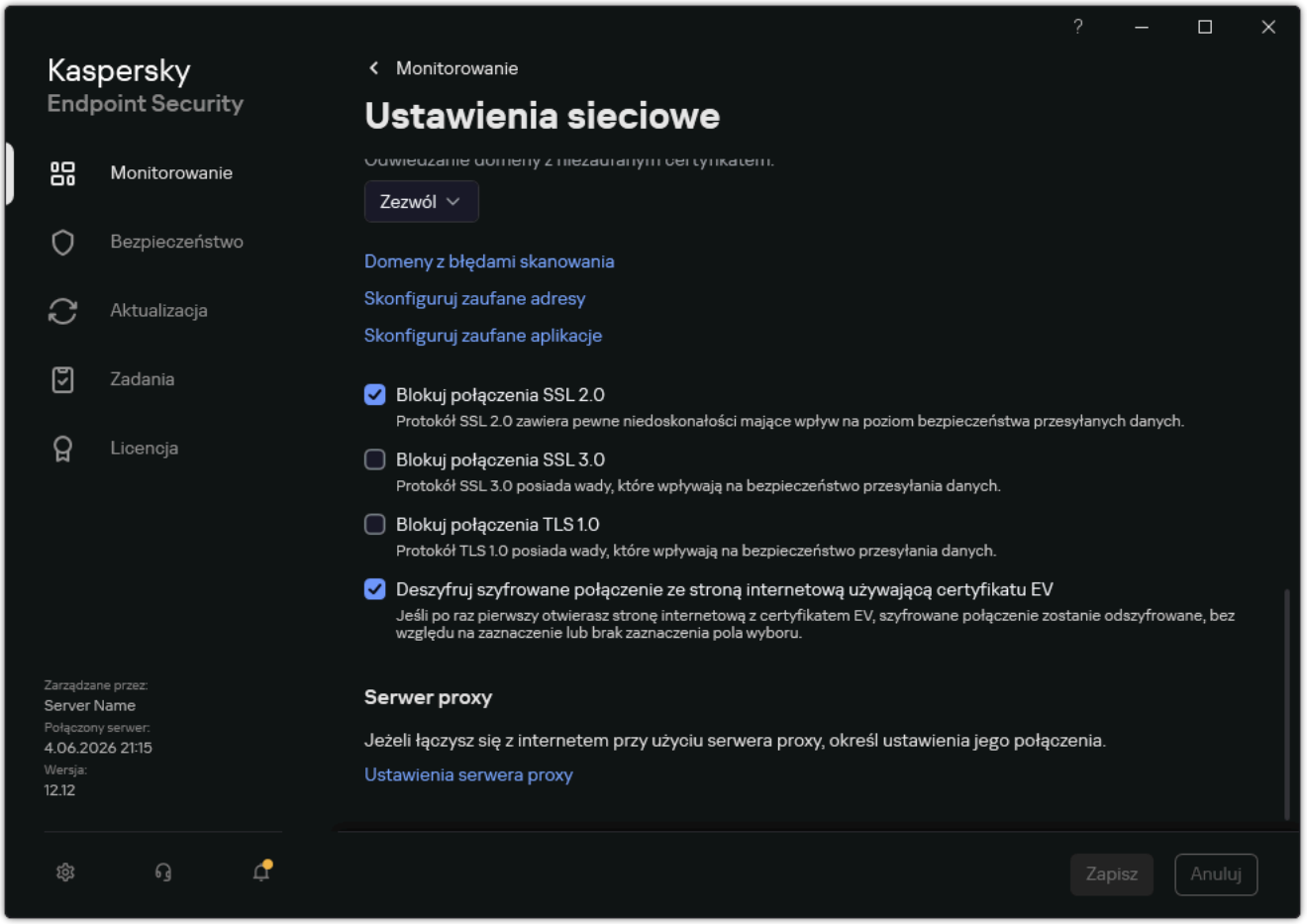
   Na przykład:

   - `domain.com` – wpis jest częścią następujących adresów: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Wpis nie jest częścią poddomen (na przykład: `subdomain.domain.com`).
   - `subdomain.domain.com` – wpis jest częścią następujących adresów: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Wpis nie jest częścią domeny `domain.com`.
   - `*.domain.com` – wpis jest częścią następujących adresów: `https://movies.domain.com`, `https://images.domain.com/page123`. Wpis nie jest częścią domeny `domain.com`.
8. Zapisz swoje zmiany.

Jak wykluczyć adres internetowy ze skanowania połączeń szyfrowanych w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.



Ustawienia sieciowe aplikacji

3. W sekcji **Skanowanie połączeń szyfrowanych** kliknij przycisk **Skonfiguruj zaufane adresy**.

4. Kliknij **Dodaj**.

5. Wprowadź nazwę domeny lub adres IP, jeśli nie chcesz, żeby Kaspersky Endpoint Security skanował połączenia szyfrowane nawiązywane podczas odwiedzania tej domeny.

   Kaspersky Endpoint Security obsługuje znak `*` do wprowadzenia maski w nazwie domeny.

   > Kaspersky Endpoint Security nie obsługuje symbolu `*` dla adresów IP. Za pomocą maski podsieci możesz wybrać zakres adresów IP (na przykład: 198.51.100.0/24).

Na przykład:

- `domain.com` – wpis jest częścią następujących adresów: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Wpis nie jest częścią poddomen (na przykład: `subdomain.domain.com`).
- `subdomain.domain.com` – wpis jest częścią następujących adresów: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Wpis nie jest częścią domeny `domain.com`.
- `*.domain.com` – wpis jest częścią następujących adresów: `https://movies.domain.com`, `https://images.domain.com/page123`. Wpis nie jest częścią domeny `domain.com`.

6. Zapisz swoje zmiany.

Domyślnie Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych w przypadku wystąpienia błędów i dodaje stronę internetową do specjalnej listy *Domeny z błędami skanowania*. Kaspersky Endpoint Security tworzy osobną listę dla każdego użytkownika i nie wysyła danych do Kaspersky Security Center. Możesz włączyć blokowanie połączenia, gdy wystąpi błąd skanowania. Możesz przejrzeć listę domen z błędami skanowania połączeń szyfrowanych tylko w lokalnym interfejsie aplikacji.

W celu wyświetlenia listy domen z błędami skanowania:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
3. W sekcji **Skanowanie połączeń szyfrowanych** kliknij przycisk **Domeny z błędami skanowania**.

   Zostanie otwarta lista domen z błędami skanowania. Aby zresetować listę, włącz blokowanie połączenia w przypadku wystąpienia błędów skanowania w zasadzie, zastosuj zasadę, a następnie zresetuj parametr do wartości początkowej i ponownie zastosuj zasadę.

Specjaliści z Kaspersky sporządzają listę *globalnych wykluczeń* – zaufanych stron internetowych, których Kaspersky Endpoint Security nie sprawdza niezależnie od ustawień aplikacji.

W celu przejrzenia globalnych wykluczeń ze skanowania szyfrowanego ruchu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
3. W sekcji **Skanowanie połączeń szyfrowanych** kliknij odnośnik do listy zaufanych stron internetowych.

   Spowoduje to otwarcie listy stron internetowych utworzonej przez ekspertów z Kaspersky. Kaspersky Endpoint Security nie skanuje chronionych połączeń dla stron internetowych na liście. Ta lista może zostać zaktualizowana, gdy zostaną zaktualizowane bazy danych i moduły Kaspersky Endpoint Security.

Wyczyść dane

Kaspersky Endpoint Security umożliwia korzystanie z zadania do zdalnego usuwania danych z komputerów użytkowników.

Kaspersky Endpoint Security usuwa dane w następujący sposób:

- W trybie cichym;
- Na dyskach twardych i nośnikach wymiennych;
- Dla wszystkich kont użytkownika na komputerze.

Kaspersky Endpoint Security wykonuje zadanie *Wyczyść dane* niezależnie od tego, który typ licencjonowania jest używany, nawet po wygaśnięciu licencji.

Tryby czyszczenia danych

To zadanie umożliwia usuwanie danych w następujących trybach:

- Natychmiastowe usuwanie danych.

  W tym trybie możliwe jest, na przykład, usunięcie przestarzałych danych w celu zwolnienia miejsca na dysku.

- Odroczone usuwanie danych.

  Ten tryb jest przeznaczony, na przykład, do ochrony danych na laptopie w przypadku jego zgubienia lub kradzieży. Możesz skonfigurować automatyczne usuwanie danych, jeśli laptop znajdzie się poza granicami sieci firmowej i nie był zsynchronizowany z Kaspersky Security Center od dłuższego czasu.

Nie można ustawić terminarza usuwania danych we właściwościach zadania. Możesz usunąć dane natychmiast po ręcznym uruchomieniu zadania lub skonfigurować opóźnione usuwanie danych, jeśli nie ma połączenia z Kaspersky Security Center.

Ograniczenia

Czyszczenie danych posiada następujące ograniczenia:

- Tylko administrator Kaspersky Security Center może zarządzać zadaniem *Wyczyść dane*. Nie możesz skonfigurować ani uruchomić zadania w lokalnym interfejsie Kaspersky Endpoint Security.
- W systemie plików NTFS Kaspersky Endpoint Security usuwa tylko nazwy głównych strumieni danych. Alternatywnych nazw strumieni danych nie można usunąć.
- Po usunięciu pliku dowiązania symbolicznego, Kaspersky Endpoint Security usuwa również pliki, których ścieżki są określone w dowiązaniu symbolicznym.

Tworzenie zadania Wyczyść dane

W celu usunięcia danych na komputerach użytkowników:

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Wyczyść dane**.

   c. W polu **Nazwa zadania** wpisz krótki opis, na przykład *Wyczyść dane (ochrona przed kradzieżą)*.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.

   Jeśli nowe komputery są dodawane do grupy administracyjnej w obrębie obszaru zadania, natychmiast zostaje uruchomione zadanie usuwania danych na nowych komputerach tylko wtedy, gdy zadanie zostaje zakończone w ciągu 5 minut od dodania nowych komputerów.

5. Zakończ działanie Kreatora.

   Nowe zadanie zostanie wyświetlone na liście zadań.

6. Kliknij zadanie **Wyczyść dane** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

7. Wybierz zakładkę **Ustawienia aplikacji**.

8. Wybierz metodę usuwania danych:

   - **Usuń za pomocą systemu operacyjnego**. Kaspersky Endpoint Security używa zasobów systemu operacyjnego do usuwania plików bez wysyłania ich do kosza.
   - **Usuń całkowicie, bez możliwości przywrócenia**. Kaspersky Endpoint Security nadpisuje pliki losowymi danymi. Przywrócenie danych po ich usunięciu jest praktycznie niemożliwe.

9. Jeśli chcesz odroczyć usunięcie danych, zaznacz pole **Automatycznie usuwaj dane w przypadku braku połączenia z Kaspersky Security Center dłuższego niż N dni**. Określ liczbę dni.

   Odroczone zadanie usuwania danych zostanie wykonane za każdym razem, gdy nie ma połączenia z Kaspersky Security Center przez określony czas.

Konfigurując odroczone usuwanie danych, należy pamiętać, że pracownicy mogą mieć różne harmonogramy pracy. Należy także uwzględnić terminarz pracy użytkowników offline. Szczegółowe informacje na temat pracy z komputerami offline i użytkownikami mobilnymi można znaleźć w pomocy do Kaspersky Security Center.

Jeśli komputer jest wyłączony i połączenie nie jest dostępne przez czas dłuższy niż skonfigurowany, po ponownym uruchomieniu komputera Kaspersky Endpoint Security nie usunie danych od razu. Aplikacja będzie oczekiwać na synchronizację z Kaspersky Security Center przez godzinę. Jest to konieczne, aby zapobiec nieautoryzowanemu usunięciu danych na komputerach użytkowników, którzy wyłączyli je, np. przed wyjazdem na wakacje.

Jeśli pole jest odznaczone, zadanie zostanie wykonane natychmiast po synchronizacji z Kaspersky Security Center.

10. Utwórz listę usuwanych obiektów:

    - **Foldery**. Kaspersky Endpoint Security usunie wszystkie pliki w folderze i jego podfolderach. Kaspersky Endpoint Security nie obsługuje masek i zmiennych środowiskowych dla wprowadzania ścieżki dostępu do folderu.
    - **Pliki według rozszerzenia**. Kaspersky Endpoint Security wyszukuje pliki z określonymi rozszerzeniami na wszystkich dyskach komputera, w tym dyskach wymiennych. Użyj znaku „`;`” lub „`,`”, aby określić kilka rozszerzeń.
    - **Wstępnie określony obszar**. Kaspersky Endpoint Security usunie pliki z następujących obszarów:
        - **Dokumenty**. Pliki w standardowym folderze *Dokumenty* systemu operacyjnego i jego podfolderach.
        - **Ciasteczka**. Pliki, w których przeglądarka zapisuje dane ze stron internetowych odwiedzonych przez użytkownika (takie jak dane autoryzacyjne użytkownika).
        - **Pulpit**. Pliki w standardowym folderze *Pulpit* systemu operacyjnego i jego podfolderach.
        - **Pliki tymczasowe Internet Explorer**. Pliki tymczasowe związane z działaniem przeglądarki Internet Explorer, takie jak kopie stron internetowych, obrazów i plików multimedialnych.
        - **Pliki tymczasowe**. Pliki tymczasowe związane z działaniem aplikacji zainstalowanych na komputerze. Na przykład, aplikacje Microsoft Office tworzą pliki tymczasowe zawierające kopie zapasowe dokumentów.
        - **Pliki programu Outlook**. Pliki dotyczące działania klienta poczty Outlook: pliki danych (PST), pliki danych offline (OST), pliki książki adresowej offline (OAB) oraz pliki osobistej książki adresowej (PAB).
        - **Profil użytkownika**. Zestaw plików i folderów, które przechowują ustawienia systemu operacyjnego dla lokalnego konta użytkownika.

    Możesz utworzyć listę obiektów do usunięcia na każdej zakładce. Kaspersky Endpoint Security utworzy skonsolidowaną listę i usunie pliki z tej listy po zakończeniu zadania.

    Nie możesz usuwać plików wymaganych do działania Kaspersky Endpoint Security.

11. Zapisz swoje zmiany.

12. Zaznacz pole obok zadania.

13. Kliknij **Uruchom**.

W wyniku tego działania dane na komputerach użytkowników zostaną usunięte zgodnie z wybranym trybem: natychmiast lub gdy nie ma połączenia. Jeśli program Kaspersky Endpoint Security nie może usunąć pliku, gdy, na przykład, użytkownik aktualnie używa pliku, aplikacja nie podejmie kolejnej próby jego usunięcia. Aby zakończyć usuwanie danych, uruchom zadanie ponownie.

Kontrola komputera

Kontrola sieci

Kontrola sieci zarządza dostępem użytkowników zasobów sieciowych. Pomaga to zmniejszyć ruch sieciowy i nieodpowiednie dysponowanie czasem pracy. Gdy użytkownik próbuje otworzyć stronę internetową ograniczoną przez Kontrolę sieci, Kaspersky Endpoint Security zablokuje dostęp lub wyświetli ostrzeżenie (patrz rysunek poniżej).

Aby móc korzystać z Kontroli sieci, należy wykonać początkową konfigurację aplikacji:

- Do monitorowania ruchu HTTPS, włącz skanowanie połączeń szyfrowanych (domyślnie włączone).
- Wybierz porty, które musi monitorować Kaspersky Endpoint Security (domyślnie aplikacja monitoruje wszystkie porty).
- Wybierz aplikacje, których ruch ma być monitorowany za pomocą Kaspersky Endpoint Security. Większość przeglądarek znajduje się już na liście aplikacji zalecanych przez Kaspersky. Jeśli Twojej przeglądarki nie ma na liście, dodaj ją ręcznie.
- Zalecamy wstrzyknąć skrypt interakcji ze stroną internetową do ruchu sieciowego (domyślnie wstrzykiwanie skryptów jest wyłączone). Ten skrypt umożliwia rejestrację zdarzeń Kontroli sieci dla dziennika zdarzeń aplikacji, dziennika zdarzeń systemu operacyjnego i raportów.

Metody zarządzania dostępem do stron internetowych

Kontrola sieci umożliwia konfigurowanie dostępu do stron internetowych przy użyciu następujących metod:

- **Kategoria strony internetowej**. Strony internetowe są kategoryzowane zgodnie z usługą chmury Kaspersky Security Network, analizą heurystyczną i bazą danych znanych stron internetowych (znajdującą się w bazach danych aplikacji). Na przykład, możesz ograniczyć dostęp użytkownika do kategorii *Sieci społecznościowe* lub do innych kategorii.
- **Typ danych**. Na przykład, możesz ograniczyć dostęp użytkowników do danych na stronie internetowej i ukryć zawartość graficzną. Kaspersky Endpoint Security określa typ danych w oparciu o format pliku, a nie w oparciu o jego rozszerzenie.

  > Kaspersky Endpoint Security nie skanuje plików w archiwach. Na przykład, jeśli pliki obrazów zostały umieszczone w archiwum, Kaspersky Endpoint Security identyfikuje typ danych *Archiwa*, a nie *Grafika*.

- **Określony adres**. Możesz wprowadzić adres internetowy lub użyć masek.

Możesz jednocześnie użyć kilku metod do regulowania dostępu do stron internetowych. Na przykład, możesz ograniczyć dostęp do typu danych *Pliki aplikacji pakietu Office* tylko dla kategorii stron internetowych *Poczta elektroniczna przez WWW*.

Reguły dostępu do stron internetowych

Kontrola sieci zarządza dostępem użytkowników do stron internetowych przy użyciu *reguł dostępu*. Możesz skonfigurować następujące zaawansowane ustawienia reguły dostępu do stron internetowych:

- Użytkowników, do których stosowana jest reguła.

  Na przykład, możesz ograniczyć dostęp do internetu poprzez przeglądarkę dla wszystkich użytkowników firmy, za wyjątkiem działu IT.

- Terminarz reguły.

  Na przykład, możesz ograniczyć dostęp do internetu poprzez przeglądarkę tylko w trakcie godzin pracy.

Priorytety reguł dostępu

Każda reguła posiada priorytet. Im wyżej reguła znajduje się na liście reguł, tym wyższy priorytet posiada. Jeśli strona internetowa została dodana do kilku reguł, Kontrola sieci reguluje dostęp do strony internetowej w oparciu o regułę z najwyższym priorytetem. Na przykład, Kaspersky Endpoint Security może identyfikować portal firmowy jako sieć społecznościową. Aby ograniczyć dostęp do sieci społecznościowych i zapewnić dostęp do firmowego portalu internetowego, utwórz dwie reguły: jedną regułę blokady dla kategorii stron internetowych *Sieci społecznościowe* i jedną regułę zezwalającą dla firmowego portalu internetowego. Reguła dostępu dla firmowego portalu internetowego musi posiadać wyższy priorytet niż reguła dostępu dla sieci społecznościowych.





Wiadomości Kontroli sieci

Dodawanie reguły dostępu do zasobu sieciowego

Reguła dostępu do zasobu sieciowego jest zestawem filtrów i działań, które program Kaspersky Endpoint Security stosuje, gdy użytkownicy odwiedzają zasoby sieciowe. Reguły dostępu mogą zawierać terminarz reguły.

Nie jest zalecane tworzenie więcej niż 1 000 reguł dostępu do zasobów internetowych, gdyż może to spowodować niestabilność systemu.

Reguła dostępu do zasobu sieciowego jest zestawem filtrów i działań, które program Kaspersky Endpoint Security wykonuje podczas odwiedzania przez użytkownika zasobów sieciowych opisanych w regule w przedziale czasu wskazanym w terminarzu reguły. Filtry umożliwiają dokładne określenie puli zasobów sieciowych, do których dostęp jest kontrolowany przez moduł Kontrola sieci.

Dostępne są następujące filtry:

- **Filtruj według zawartości**. Kontrola sieci kategoryzuje zasoby sieciowe według zawartości i typu danych. Możesz kontrolować dostęp użytkownika do zasobów sieciowych z zawartością i danymi należącymi do typów zdefiniowanych przez te kategorie. Podczas odwiedzania zasobów sieciowych należących do wybranej kategorii zawartości i / lub kategorii typu danych, program Kaspersky Endpoint Security wykonuje akcję określoną w regule.

- **Filtruj według adresów zasobów sieciowych**. Możesz kontrolować dostęp użytkownika do wszystkich adresów zasobów sieciowych lub do pojedynczego adresu zasobu sieciowego i / lub grup adresów zasobów sieciowych.

  Jeżeli wybrano filtrowanie według zawartości i filtrowanie według adresów zasobów sieciowych, a określone adresy zasobów sieciowych i / lub grupy adresów zasobów sieciowych należą do wybranej kategorii zawartości lub kategorii typu danych, program Kaspersky Endpoint Security nie będzie monitorował dostępu do wszystkich zasobów sieciowych w wybranej kategorii zawartości i / lub kategorii typu danych. Zamiast tego aplikacja będzie monitorowała dostęp tylko do określonych adresów zasobów sieciowych i / lub grup adresów zasobów sieciowych.

- **Filtruj według nazw użytkowników i grup użytkowników**. Możesz określić nazwy użytkowników i / lub grup użytkowników z dostępem do zasobów sieciowych, które są kontrolowane zgodnie z regułą.

- **Terminarz reguły**. Możesz określić terminarz reguły. Terminarz reguły określa przedział czasu, podczas którego Kaspersky Endpoint Security monitoruje dostęp do zasobów sieciowych, dla których stosowana jest reguła.

Po zainstalowaniu Kaspersky Endpoint Security lista reguł modułu Kontrola sieci nie jest pusta. Opcja *Reguła domyślna* jest wstępnie ustawiona. Ta reguła jest stosowana do wszelkich zasobów internetowych, które nie są objęte innymi regułami, i zezwala na lub blokuje dostęp do tych zasobów internetowych wszystkim użytkownikom.

Każda reguła posiada priorytet. Im wyżej reguła znajduje się na liście reguł, tym wyższy priorytet posiada. Jeśli strona internetowa została dodana do kilku reguł, Kontrola sieci reguluje dostęp do strony internetowej w oparciu o regułę z najwyższym priorytetem. Na przykład, Kaspersky Endpoint Security może identyfikować portal firmowy jako sieć społecznościową. Aby ograniczyć dostęp do sieci społecznościowych i zapewnić dostęp do firmowego portalu internetowego, utwórz dwie reguły: jedną regułę blokady dla kategorii stron internetowych *Sieci społecznościowe* i jedną regułę zezwalającą dla firmowego portalu internetowego. Reguła dostępu dla firmowego portalu internetowego musi posiadać wyższy priorytet niż reguła dostępu dla sieci społecznościowych.

Jak dodawać reguły dostępu do zasobów sieciowych w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Kontrola zabezpieczeń → Kontrola sieci**.

4. Zaznacz pole **Kontrola sieci**.

5. W sekcji **Ustawienia Kontroli sieci** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Reguła dostępu do zasobów sieciowych**.

6. Skonfiguruj regułę dostępu do zasobu sieciowego (patrz poniższa tabela).

7. Jeśli chcesz, aby Kontrola sieci zakończyła połączenie z zabronionym zasobem internetowym natychmiast po zastosowaniu zasad, zaznacz pole wyboru **Przerwij aktywne sesje przeglądarki użytkownika po zastosowaniu zasady**.

   > Kontrola sieci pozwala na natychmiastowe rozłączanie zasobów sieciowych wyłącznie w przeglądarkach. W innych aplikacjach Kontrola sieci ogranicza tylko nowe połączenia.

   Jeśli pole wyboru jest odznaczone, Kontrola sieci ogranicza nowe połączenia tylko do zabronionych zasobów sieciowych. Kontrola sieci nie kończy aktywnych połączeń.

8. Zapisz swoje zmiany.

Jak dodać regułę dostępu do zasobu sieciowego w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Kontrola zabezpieczeń → Kontrola sieci**.

5. Włącz przełącznik **Kontrola sieci WŁĄCZONA**.

6. W sekcji **Lista reguł** kliknij przycisk **Dodaj**.

7. Skonfiguruj regułę dostępu do zasobu sieciowego (patrz poniższa tabela).

8. Jeśli chcesz, aby Kontrola sieci zakończyła połączenie z zabronionym zasobem internetowym natychmiast po zastosowaniu zasad, zaznacz pole wyboru **Przerwij aktywne sesje przeglądarki użytkownika po zastosowaniu zasady**.

   > Kontrola sieci pozwala na natychmiastowe rozłączanie zasobów sieciowych wyłącznie w przeglądarkach. W innych aplikacjach Kontrola sieci ogranicza tylko nowe połączenia.

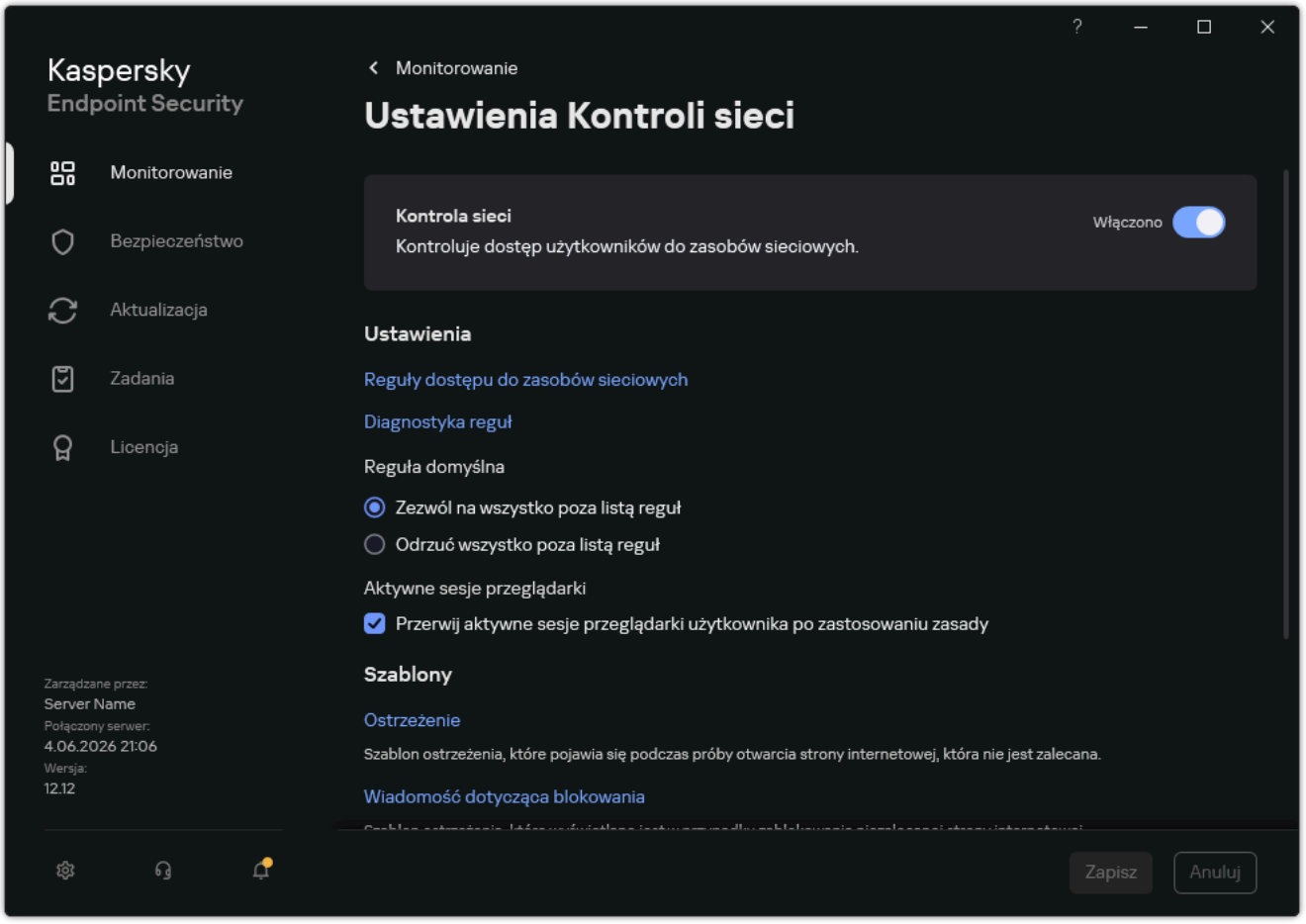
   Jeśli pole wyboru jest odznaczone, Kontrola sieci ogranicza nowe połączenia tylko do zabronionych zasobów sieciowych. Kontrola sieci nie kończy aktywnych połączeń.

9. Zapisz swoje zmiany.

Jak dodawać reguły dostępu do zasobów sieciowych w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń → Kontrola sieci**.



Ustawienia komponentu Kontrola sieci

3. Włącz przełącznik **Kontrola sieci**.

4. W sekcji **Ustawienia** kliknij przycisk **Reguły dostępu do zasobów sieciowych**.

5. W otwartym oknie kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Reguła dostępu do zasobów sieciowych**.

6. Skonfiguruj regułę dostępu do zasobu sieciowego (patrz poniższa tabela).

7. Jeśli chcesz, aby Kontrola sieci zakończyła połączenie z zabronionym zasobem internetowym natychmiast po zastosowaniu zasad, zaznacz pole wyboru **Przerwij aktywne sesje przeglądarki użytkownika po zastosowaniu zasady**.

   > Kontrola sieci pozwala na natychmiastowe rozłączanie zasobów sieciowych wyłącznie w przeglądarkach. W innych aplikacjach Kontrola sieci ogranicza tylko nowe połączenia.

   Jeśli pole wyboru jest odznaczone, Kontrola sieci ogranicza nowe połączenia tylko do zabronionych zasobów sieciowych. Kontrola sieci nie kończy aktywnych połączeń.

8. Zapisz swoje zmiany.

Nowa reguła Kontroli sieci zostanie dodana do listy. W razie potrzeby zmień priorytet reguły Kontroli sieci. Możesz też użyć przełącznika, aby wyłączyć regułę dostępu do zasobu sieciowego w dowolnym momencie. Dzięki temu nie musisz jej usuwać z listy.

Parametry reguły Kontroli sieci

Parametr	Opis
Nazwa reguły	Nazwa reguły Kontroli sieci.
Stan	• **Włączono**. • **Wyłączono**. Możesz użyć przełącznika do wyłączenia reguły dostępu do zasobu sieciowego w dowolnym momencie.
Akcja	• **Zezwól**. Kontrola sieci umożliwia uzyskiwanie dostępu do zasobów sieciowych, które spełniają parametry reguły. • **Zablokuj**. Kontrola sieci umożliwia blokowanie dostępu do zasobów sieciowych, które spełniają parametry reguły. Po zablokowaniu wyświetlany jest komunikat o odmowie dostępu do witryny. • **Ostrzegaj**. Kiedy użytkownik próbuje uzyskać dostęp do zasobu sieciowego spełniającego parametry reguły, Kontrola sieci wyświetla ostrzeżenie, że nie zaleca się odwiedzania zasobu sieciowego. Korzystając z odnośników znajdujących się w wiadomości ostrzegającej, użytkownik może uzyskać dostęp do żądanego zasobu sieciowego.
Zawartość filtra	• **Według kategorii zawartości**. Możesz kontrolować dostęp użytkownika do zasobów internetowych według kategorii (na przykład: kategoria *Sieci społecznościowe*). • **Według typu danych**. Możesz kontrolować dostęp użytkownika do zasobów internetowych w oparciu o określony typ danych opublikowanych w nich danych (na przykład: *Grafika*).
Adresy	• **Dla wszystkich adresów**. Kontrola sieci nie będzie filtrowała zasobów sieciowych według adresu. • **Dla określonych adresów**. Kontrola sieci będzie filtrowała tylko adresy zasobów internetowych z listy. Możesz wprowadzić adres internetowy lub użyć masek. Możesz także wyeksportować listę adresów zasobów internetowych z pliku TXT. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny. Jeśli Skanowanie połączeń szyfrowanych jest wyłączone, dla protokołu HTTPS możesz filtrować tylko według nazwy serwera.
Użytkownicy	• **Dla wszystkich użytkowników**. Kontrola sieci nie będzie filtrowała zasobów sieciowych dla określonych użytkowników. • **Dla użytkowników indywidualnych i / lub grup**. Kontrola sieci będzie filtrował zasoby internetowe tylko dla określonych użytkowników. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.
Harmonogram reguły	Terminarz reguły określa przedział czasu, podczas którego Kaspersky Endpoint Security monitoruje dostęp do zasobów sieciowych, dla których stosowana jest reguła. Na przykład, możesz ograniczyć dostęp do internetu poprzez przeglądarkę tylko w trakcie godzin pracy.

Filtrowanie według adresów zasobów sieciowych

Aby kontrolować dostęp do poszczególnych zasobów sieciowych, musisz utworzyć regułę Kontroli sieci, utworzyć listę adresów internetowych i wybrać czynność Kontroli sieci. Podczas tworzenia listy adresów internetowych możesz wprowadzać adresy URL lub używać masek.

Reguły mogą zawierać terminarz reguły i listę użytkowników, do których stosowana jest reguła. Na przykład możesz ograniczyć dostęp do stron internetowych tylko w godzinach pracy lub zezwolić na odwiedzanie witryn użytkownikom z pewnych grup.

Jak włączyć filtr adresów zasobów sieciowych w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
4. Zaznacz pole **Kontrola sieci**.
5. W sekcji **Ustawienia Kontroli sieci** kliknij przycisk **Dodaj**.
   Zostanie otwarte okno **Reguła dostępu do zasobów sieciowych**.
6. Konfigurowanie reguły dostępu do zasobu sieciowego:
   a. W polu **Nazwa** wprowadź nazwę reguły.
   b. Z listy rozwijalnej **Zastosuj dla adresów** wybierz **Dla określonych adresów**.
   c. Utwórz listę adresów zasobów sieciowych. Możesz wprowadzić adres internetowy lub użyć masek. Możesz także wyeksportować listę adresów zasobów internetowych z pliku TXT.

      Jeśli Skanowanie połączeń szyfrowanych jest wyłączone, dla protokołu HTTPS możesz filtrować tylko według nazwy serwera.

   d. Z listy rozwijalnej **Zastosuj dla użytkowników** wybierz odpowiedni filtr dla użytkowników:
      - **Dla wszystkich użytkowników**. Kontrola sieci nie będzie filtrowała zasobów sieciowych według adresu.
      - **Dla użytkowników indywidualnych lub grup**. Kontrola sieci będzie filtrowała tylko adresy zasobów internetowych z listy. Możesz wprowadzić adres internetowy lub użyć masek. Możesz także wyeksportować listę adresów zasobów internetowych z pliku TXT. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

e. Z listy rozwijalnej **Akcja** wybierz opcję:

- **Zezwól**. Kontrola sieci umożliwia uzyskiwanie dostępu do zasobów sieciowych, które spełniają parametry reguły.
- **Blokuj**. Kontrola sieci umożliwia blokowanie dostępu do zasobów sieciowych, które spełniają parametry reguły. Po zablokowaniu wyświetlany jest komunikat o odmowie dostępu do witryny.
- **Ostrzegaj**. Kiedy użytkownik próbuje uzyskać dostęp do zasobu sieciowego spełniającego parametry reguły, Kontrola sieci wyświetla ostrzeżenie, że nie zaleca się odwiedzania zasobu sieciowego. Korzystając z odnośników znajdujących się w wiadomości ostrzegającej, użytkownik może uzyskać dostęp do żądanego zasobu sieciowego.

f. Z listy rozwijalnej **Terminarz reguły** wybierz terminarz lub utwórz nowy harmonogram.

7. Jeśli chcesz, aby Kontrola sieci zakończyła połączenie z zabronionym zasobem internetowym natychmiast po zastosowaniu zasad, zaznacz pole wyboru **Przerwij aktywne sesje przeglądarki użytkownika po zastosowaniu zasady**.

   Kontrola sieci pozwala na natychmiastowe rozłączanie zasobów sieciowych wyłącznie w przeglądarkach. W innych aplikacjach Kontrola sieci ogranicza tylko nowe połączenia.

   Jeśli pole wyboru jest odznaczone, Kontrola sieci ogranicza nowe połączenia tylko do zabronionych zasobów sieciowych. Kontrola sieci nie kończy aktywnych połączeń.

8. Zapisz swoje zmiany.

Jak włączyć filtr adresów zasobów sieciowych w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
5. Włącz przełącznik **Kontrola sieci WŁĄCZONA**.
6. W sekcji **Lista reguł** kliknij przycisk **Dodaj**.
7. Konfigurowanie reguły dostępu do zasobu sieciowego:

   a. W polu **Nazwa reguły** wprowadź nazwę reguły.

   b. Wybierz stan **Włączono** dla reguły dostępu do zasobu internetowego.

   Możesz użyć przełącznika, aby wyłączyć regułę dostępu do zasobu sieciowego w dowolnym momencie. Dzięki temu nie musisz jej usuwać z listy.

c. W sekcji **Akcja** wybierz żądaną opcję:

- **Zezwól**. Kontrola sieci umożliwia uzyskiwanie dostępu do zasobów sieciowych, które spełniają parametry reguły.
- **Zablokuj**. Kontrola sieci umożliwia blokowanie dostępu do zasobów sieciowych, które spełniają parametry reguły. Po zablokowaniu wyświetlany jest komunikat o odmowie dostępu do witryny.
- **Powiadom**. Kiedy użytkownik próbuje uzyskać dostęp do zasobu sieciowego spełniającego parametry reguły, Kontrola sieci wyświetla ostrzeżenie, że nie zaleca się odwiedzania zasobu sieciowego. Korzystając z odnośników znajdujących się w wiadomości ostrzegającej, użytkownik może uzyskać dostęp do żądanego zasobu sieciowego.

d. W obszarze **Zakres** wybierz **Pojedyncze strony internetowe**.

e. Skonfiguruj filtr zawartości:

- **Indywidualny adres**. Utwórz listę adresów zasobów sieciowych. Możesz wprowadzić adres internetowy lub użyć masek. Możesz także wyeksportować listę adresów zasobów internetowych z pliku TXT.

  > Jeśli Skanowanie połączeń szyfrowanych jest wyłączone, dla protokołu HTTPS możesz filtrować tylko według nazwy serwera.

- **Typ danych**. Możesz kontrolować dostęp użytkownika do zasobów internetowych w oparciu o określony typ danych opublikowanych w nich danych (na przykład: *Grafika*).

f. W obszarze **Użytkownik lub grupa** wybierz użytkowników, do których chcesz, aby Kontrola sieci zastosował regułę.

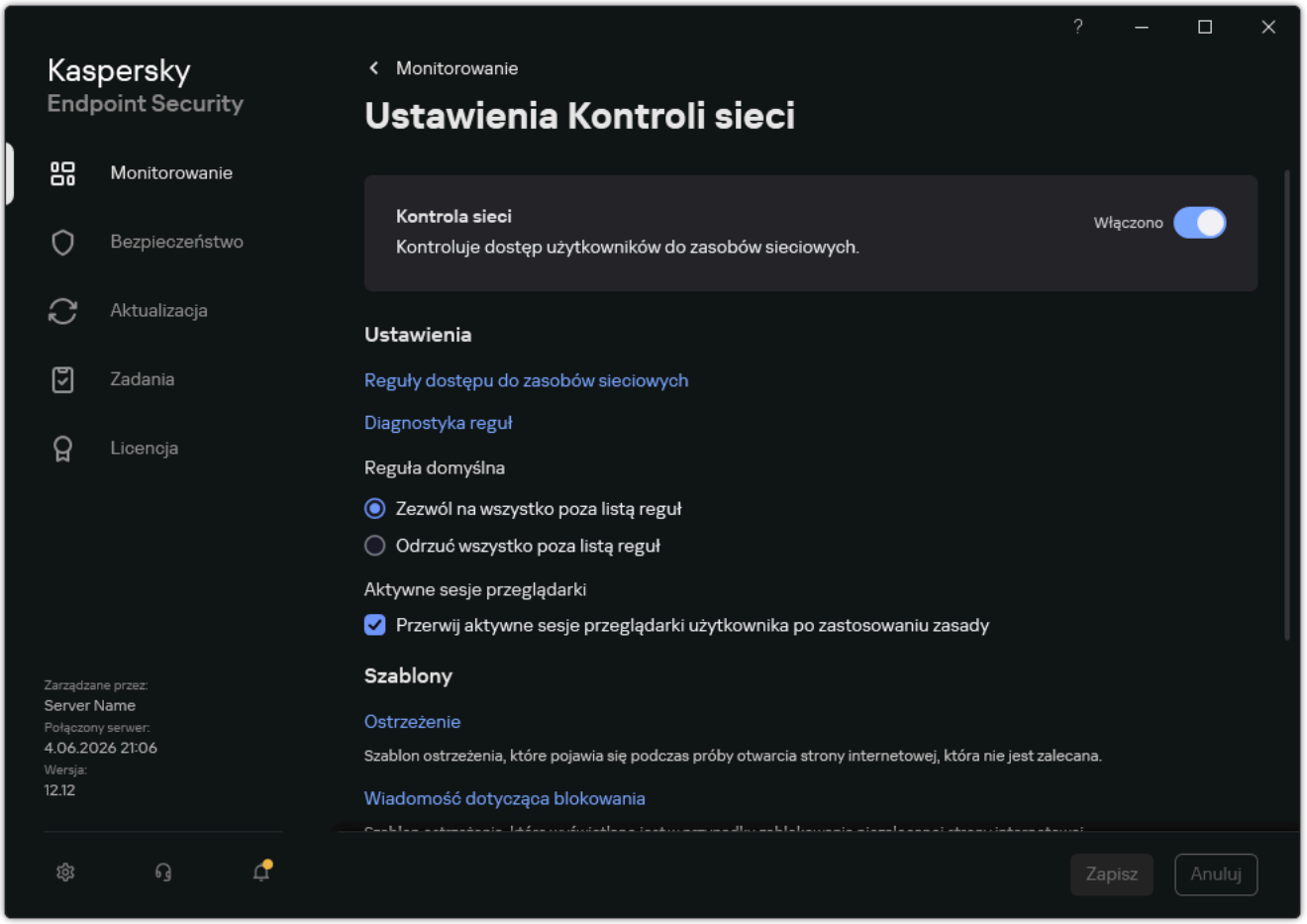
Kontrola sieci będzie filtrowała tylko adresy zasobów internetowych z listy. Możesz wprowadzić adres internetowy lub użyć masek. Możesz także wyeksportować listę adresów zasobów internetowych z pliku TXT. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

g. W bloku **Terminarz dostępu** wybierz terminarz lub utwórz nowy harmonogram.

8. Zapisz swoje zmiany.

Jak włączyć filtr adresów zasobów sieciowych w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń → Kontrola sieci**.



Ustawienia komponentu Kontrola sieci

3. W sekcji **Ustawienia** kliknij przycisk **Reguły dostępu do zasobów sieciowych**.
4. W otwartym oknie kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Reguła dostępu do zasobów sieciowych**.
5. W polu **Nazwa reguły** wprowadź nazwę reguły.
6. Wybierz stan **Włączono** dla reguły dostępu do zasobu internetowego.

   Możesz użyć przełącznika do wyłączenia reguły dostępu do zasobu sieciowego w dowolnym momencie.
7. W sekcji **Akcja** wybierz żądaną opcję:

   - **Zezwól**. Kontrola sieci umożliwia uzyskiwanie dostępu do zasobów sieciowych, które spełniają parametry reguły.
   - **Zablokuj**. Kontrola sieci umożliwia blokowanie dostępu do zasobów sieciowych, które spełniają parametry reguły. Po zablokowaniu wyświetlany jest komunikat o odmowie dostępu do witryny.
   - **Ostrzegaj**. Kiedy użytkownik próbuje uzyskać dostęp do zasobu sieciowego spełniającego parametry reguły, Kontrola sieci wyświetla ostrzeżenie, że nie zaleca się odwiedzania zasobu sieciowego. Korzystając z odnośników znajdujących się w wiadomości ostrzegającej, użytkownik może uzyskać dostęp do żądanego zasobu sieciowego.

8. W obszarze **Adresy** wybierz **Dla określonych adresów**.

   Utwórz listę adresów zasobów sieciowych. Możesz wprowadzić adres internetowy lub użyć masek. Możesz także wyeksportować listę adresów zasobów internetowych z pliku TXT.

   > Jeśli Skanowanie połączeń szyfrowanych jest wyłączone, dla protokołu HTTPS możesz filtrować tylko według nazwy serwera.

9. W sekcji **Użytkownicy** wybierz odpowiedni filtr dla użytkowników:

   - **Dla wszystkich użytkowników**. Kontrola sieci nie będzie filtrowała zasobów sieciowych dla określonych użytkowników.
   - **Dla użytkowników indywidualnych i / lub grup**. Kontrola sieci będzie filtrowała tylko adresy zasobów internetowych z listy. Możesz wprowadzić adres internetowy lub użyć masek. Możesz także wyeksportować listę adresów zasobów internetowych z pliku TXT. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

10. Z listy rozwijalnej **Harmonogram reguły** wybierz terminarz lub utwórz nowy harmonogram.

11. Jeśli chcesz, aby Kontrola sieci zakończyła połączenie z zabronionym zasobem internetowym natychmiast po zastosowaniu zasad, zaznacz pole wyboru **Przerwij aktywne sesje przeglądarki użytkownika po zastosowaniu zasady**.

    > Kontrola sieci pozwala na natychmiastowe rozłączanie zasobów sieciowych wyłącznie w przeglądarkach. W innych aplikacjach Kontrola sieci ogranicza tylko nowe połączenia.

    Jeśli pole wyboru jest odznaczone, Kontrola sieci ogranicza nowe połączenia tylko do zabronionych zasobów sieciowych. Kontrola sieci nie kończy aktywnych połączeń.

12. Zapisz swoje zmiany.

Nowa reguła Kontroli sieci zostanie dodana do listy. W razie potrzeby zmień priorytet reguły Kontroli sieci. Możesz też użyć przełącznika, aby wyłączyć regułę dostępu do zasobu sieciowego w dowolnym momencie. Dzięki temu nie musisz jej usuwać z listy.

Filtrowanie według zawartości zasobów sieciowych

Aby kontrolować dostęp według zawartości zasobu sieciowego, Kontrola sieci udostępnia filtr kategorii i filtr typu danych.

Strony internetowe są kategoryzowane zgodnie z usługą chmury Kaspersky Security Network, analizą heurystyczną i bazą danych znanych stron internetowych (znajdującą się w bazach danych aplikacji). Na przykład, możesz ograniczyć dostęp użytkownika do kategorii *Sieci społecznościowe* lub do innych kategorii.

Możesz ograniczyć dostęp użytkownika do witryny na podstawie typu danych, aby przykładowo ukryć obrazy. Kaspersky Endpoint Security określa typ danych w oparciu o format pliku, a nie w oparciu o jego rozszerzenie. Kontrola sieci obsługuje następujące typy danych:

- Pliki wideo
- Dźwięk
- Pliki aplikacji pakietu Office
- Pliki wykonywalne
- Archiwa
- Grafika
- Skrypty

Kaspersky Endpoint Security nie skanuje plików w archiwach. Na przykład, jeśli pliki obrazów zostały umieszczone w archiwum, Kaspersky Endpoint Security identyfikuje typ danych *Archiwa*, a nie *Grafika*.

Reguły mogą zawierać terminarz reguły i listę użytkowników, do których stosowana jest reguła. Na przykład możesz ograniczyć dostęp do stron internetowych tylko w godzinach pracy lub zezwolić na odwiedzanie witryn użytkownikom z pewnych grup.

Jak włączyć filtr zawartości zasobów sieciowych w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
4. Zaznacz pole **Kontrola sieci**.
5. W sekcji **Ustawienia Kontroli sieci** kliknij przycisk **Dodaj**.
   Zostanie otwarte okno **Reguła dostępu do zasobów sieciowych**.
6. Konfigurowanie reguły dostępu do zasobu sieciowego:
   a. W polu **Nazwa** wprowadź nazwę reguły.
   b. Z listy rozwijalnej **Filtruj zawartość** wybierz odpowiedni filtr zawartości:
      - **Według kategorii zawartości**. Możesz kontrolować dostęp użytkownika do zasobów internetowych według kategorii (na przykład: kategoria *Sieci społecznościowe*).
      - **Według typu danych**. Możesz kontrolować dostęp użytkownika do zasobów internetowych w oparciu o określony typ danych opublikowanych w nich danych (na przykład: *Grafika*).
      - **Według kategorii zawartości, typu danych**. Filtrowanie według kategorii zawartości i typów danych jest włączone.

   Po wybraniu filtrów skonfiguruj ich parametry.

c. Z listy rozwijalnej **Zastosuj dla użytkowników** wybierz odpowiedni filtr dla użytkowników:

- **Dla wszystkich użytkowników**. Kontrola sieci nie będzie filtrowała zasobów sieciowych według adresu.
- **Dla użytkowników indywidualnych lub grup**. Kontrola sieci będzie filtrowała tylko adresy zasobów internetowych z listy. Możesz wprowadzić adres internetowy lub użyć masek. Możesz także wyeksportować listę adresów zasobów internetowych z pliku TXT. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

d. Z listy rozwijalnej **Akcja** wybierz opcję:

- **Zezwól**. Kontrola sieci umożliwia uzyskiwanie dostępu do zasobów sieciowych, które spełniają parametry reguły.
- **Blokuj**. Kontrola sieci umożliwia blokowanie dostępu do zasobów sieciowych, które spełniają parametry reguły. Po zablokowaniu wyświetlany jest komunikat o odmowie dostępu do witryny.
- **Ostrzegaj**. Kiedy użytkownik próbuje uzyskać dostęp do zasobu sieciowego spełniającego parametry reguły, Kontrola sieci wyświetla ostrzeżenie, że nie zaleca się odwiedzania zasobu sieciowego. Korzystając z odnośników znajdujących się w wiadomości ostrzegającej, użytkownik może uzyskać dostęp do żądanego zasobu sieciowego.

e. Z listy rozwijalnej **Terminarz reguły** wybierz terminarz lub utwórz nowy harmonogram.

7. Jeśli chcesz, aby Kontrola sieci zakończyła połączenie z zabronionym zasobem internetowym natychmiast po zastosowaniu zasad, zaznacz pole wyboru **Przerwij aktywne sesje przeglądarki użytkownika po zastosowaniu zasady**.

   Kontrola sieci pozwala na natychmiastowe rozłączanie zasobów sieciowych wyłącznie w przeglądarkach. W innych aplikacjach Kontrola sieci ogranicza tylko nowe połączenia.

   Jeśli pole wyboru jest odznaczone, Kontrola sieci ogranicza nowe połączenia tylko do zabronionych zasobów sieciowych. Kontrola sieci nie kończy aktywnych połączeń.

8. Zapisz swoje zmiany.

Jak włączyć filtr zawartości zasobów sieciowych w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
5. Włącz przełącznik **Kontrola sieci WŁĄCZONA**.
6. W sekcji **Lista reguł** kliknij przycisk **Dodaj**.

7. Konfigurowanie reguły dostępu do zasobu sieciowego:

   a. W polu **Nazwa reguły** wprowadź nazwę reguły.

   b. Wybierz stan **Włączono** dla reguły dostępu do zasobu internetowego.

      Możesz użyć przełącznika do wyłączenia reguły dostępu do zasobu sieciowego w dowolnym momencie.

   c. W sekcji **Akcja** wybierz żądaną opcję:

      - **Zezwól**. Kontrola sieci umożliwia uzyskiwanie dostępu do zasobów sieciowych, które spełniają parametry reguły.
      - **Zablokuj**. Kontrola sieci umożliwia blokowanie dostępu do zasobów sieciowych, które spełniają parametry reguły. Po zablokowaniu wyświetlany jest komunikat o odmowie dostępu do witryny.
      - **Powiadom**. Kiedy użytkownik próbuje uzyskać dostęp do zasobu sieciowego spełniającego parametry reguły, Kontrola sieci wyświetla ostrzeżenie, że nie zaleca się odwiedzania zasobu sieciowego. Korzystając z odnośników znajdujących się w wiadomości ostrzegającej, użytkownik może uzyskać dostęp do żądanego zasobu sieciowego.

   d. W obszarze **Zakres** wybierz **Kategoria zawartości**.

   e. Skonfiguruj filtr zawartości:

      - **Kategoria zawartości**. Możesz kontrolować dostęp użytkownika do zasobów internetowych według kategorii (na przykład: kategoria *Sieci społecznościowe*).
      - **Typ danych**. Możesz kontrolować dostęp użytkownika do zasobów internetowych w oparciu o określony typ danych opublikowanych w nich danych (na przykład: *Grafika*).

   f. W obszarze **Użytkownik lub grupa** wybierz użytkowników, do których chcesz, aby Kontrola sieci zastosował regułę.

      Kontrola sieci będzie filtrowała tylko adresy zasobów internetowych z listy. Możesz wprowadzić adres internetowy lub użyć masek. Możesz także wyeksportować listę adresów zasobów internetowych z pliku TXT. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

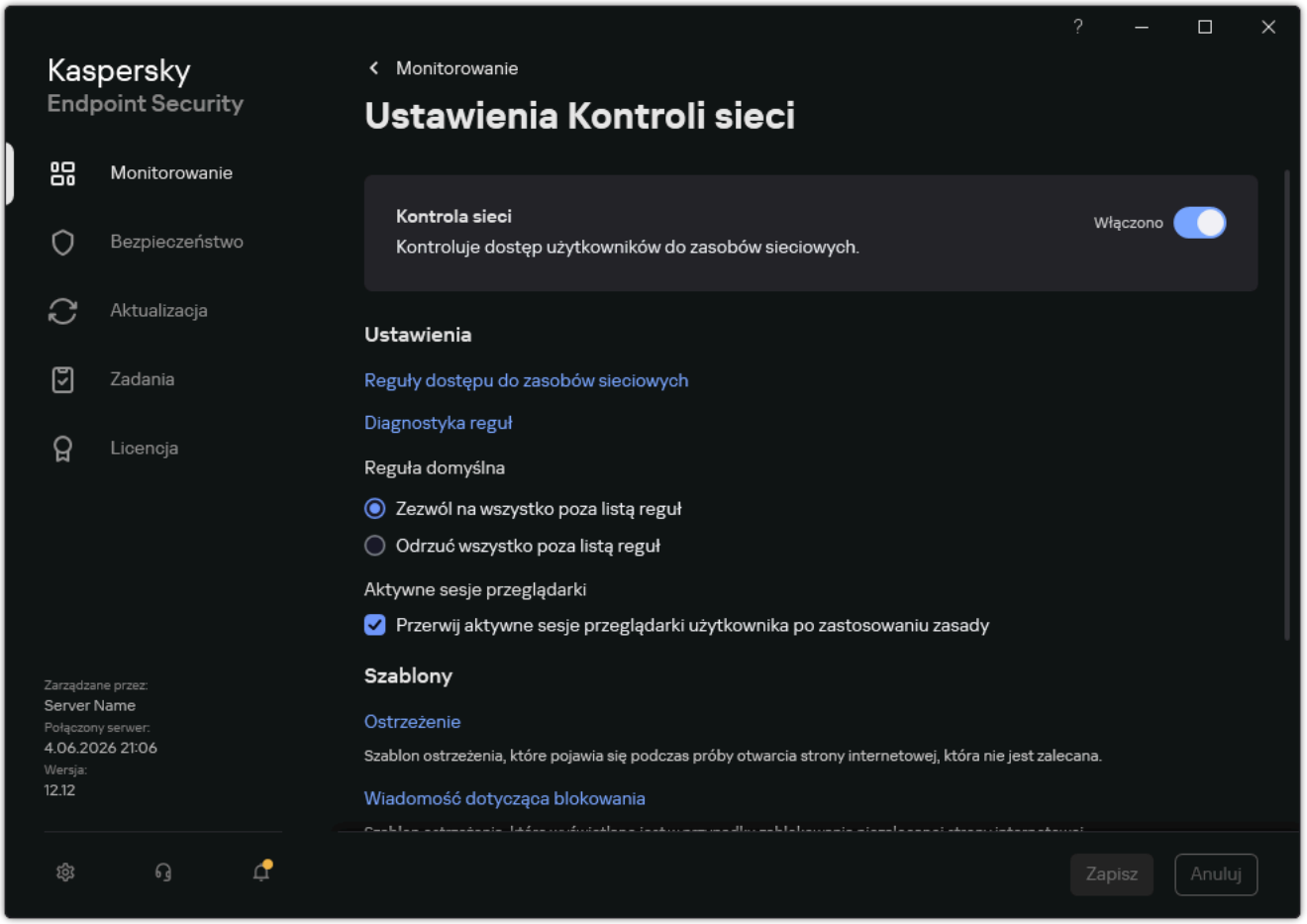
   g. W bloku **Terminarz dostępu** wybierz terminarz lub utwórz nowy harmonogram.

8. Zapisz swoje zmiany.

Jak włączyć filtr zawartości zasobów sieciowych w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń → Kontrola sieci**.



Ustawienia komponentu Kontrola sieci

3. W sekcji **Ustawienia** kliknij przycisk **Reguły dostępu do zasobów sieciowych**.

4. W otwartym oknie kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Reguła dostępu do zasobów sieciowych**.

5. W polu **Nazwa reguły** wprowadź nazwę reguły.

6. Wybierz stan **Włączono** dla reguły dostępu do zasobu internetowego.

   Możesz użyć przełącznika do wyłączenia reguły dostępu do zasobu sieciowego w dowolnym momencie.

7. W sekcji **Akcja** wybierz żądaną opcję:

   - **Zezwól**. Kontrola sieci umożliwia uzyskiwanie dostępu do zasobów sieciowych, które spełniają parametry reguły.

   - **Zablokuj**. Kontrola sieci umożliwia blokowanie dostępu do zasobów sieciowych, które spełniają parametry reguły. Po zablokowaniu wyświetlany jest komunikat o odmowie dostępu do witryny.

   - **Ostrzegaj**. Kiedy użytkownik próbuje uzyskać dostęp do zasobu sieciowego spełniającego parametry reguły, Kontrola sieci wyświetla ostrzeżenie, że nie zaleca się odwiedzania zasobu sieciowego. Korzystając z odnośników znajdujących się w wiadomości ostrzegającej, użytkownik może uzyskać dostęp do żądanego zasobu sieciowego.

8. W sekcji **Zawartość filtra** wybierz odpowiedni filtr zawartości:

   - **Według kategorii zawartości**. Możesz kontrolować dostęp użytkownika do zasobów internetowych według kategorii (na przykład: kategoria *Sieci społecznościowe*).

   - **Według typu danych**. Możesz kontrolować dostęp użytkownika do zasobów internetowych w oparciu o określony typ danych opublikowanych w nich danych (na przykład: *Grafika*).

   W celu skonfigurowania filtra zawartości:

   a. Kliknij odnośnik **Ustawienia**.

   b. Zaznacz pola obok nazw wymaganych kategorii zawartości i / lub kategorii typu danych.

   Zaznaczenie pola obok nazwy kategorii zawartości i / lub kategorii typu danych oznacza, że Kaspersky Endpoint Security będzie stosować regułę kontrolowania dostępu do zasobów sieciowych należących do wybranych kategorii zawartości i / lub kategorii typu danych.

   c. Wróć do okna konfiguracji reguły dostępu do zasobu internetowego.

9. W sekcji **Użytkownicy** wybierz odpowiedni filtr dla użytkowników:

   - **Dla wszystkich użytkowników**. Kontrola sieci nie będzie filtrowała zasobów sieciowych według adresu.

   - **Dla użytkowników indywidualnych i / lub grup**. Kontrola sieci będzie filtrowała tylko adresy zasobów internetowych z listy. Możesz wprowadzić adres internetowy lub użyć masek. Możesz także wyeksportować listę adresów zasobów internetowych z pliku TXT. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny. W celu utworzenia listy użytkowników, do których chcesz zastosować regułę:

     a. Kliknij **Dodaj**.

     b. W otwartym oknie wybierz użytkowników lub grupy użytkowników, do których chcesz zastosować regułę dostępu do zasobu sieciowego.

     c. Wróć do okna konfiguracji reguły dostępu do zasobu internetowego.

10. Z otwartej listy rozwijalnej **Harmonogram reguły** wybierz żądany terminarz lub utwórz nowy oparty na wybranym terminarzu reguły. W tym celu:

    a. Kliknij **Edytuj lub dodaj nowy**.

    b. W otwartym oknie kliknij przycisk **Dodaj**.

    c. W otwartym oknie wprowadź nazwę terminarza reguły.

    d. Konfiguruj terminarz dostępu do zasobu sieciowego dla użytkowników.

    e. Wróć do okna konfiguracji reguły dostępu do zasobu internetowego.

11. Jeśli chcesz, aby Kontrola sieci zakończyła połączenie z zabronionym zasobem internetowym natychmiast po zastosowaniu zasad, zaznacz pole wyboru **Przerwij aktywne sesje przeglądarki użytkownika po zastosowaniu zasady**.

Kontrola sieci pozwala na natychmiastowe rozłączanie zasobów sieciowych wyłącznie w przeglądarkach. W innych aplikacjach Kontrola sieci ogranicza tylko nowe połączenia.

Jeśli pole wyboru jest odznaczone, Kontrola sieci ogranicza nowe połączenia tylko do zabronionych zasobów sieciowych. Kontrola sieci nie kończy aktywnych połączeń.

12. Zapisz swoje zmiany.

Nowa reguła Kontroli sieci zostanie dodana do listy. W razie potrzeby zmień priorytet reguły Kontroli sieci. Możesz też użyć przełącznika, aby wyłączyć regułę dostępu do zasobu sieciowego w dowolnym momencie. Dzięki temu nie musisz jej usuwać z listy.

Testowanie reguł dostępu do zasobów sieciowych

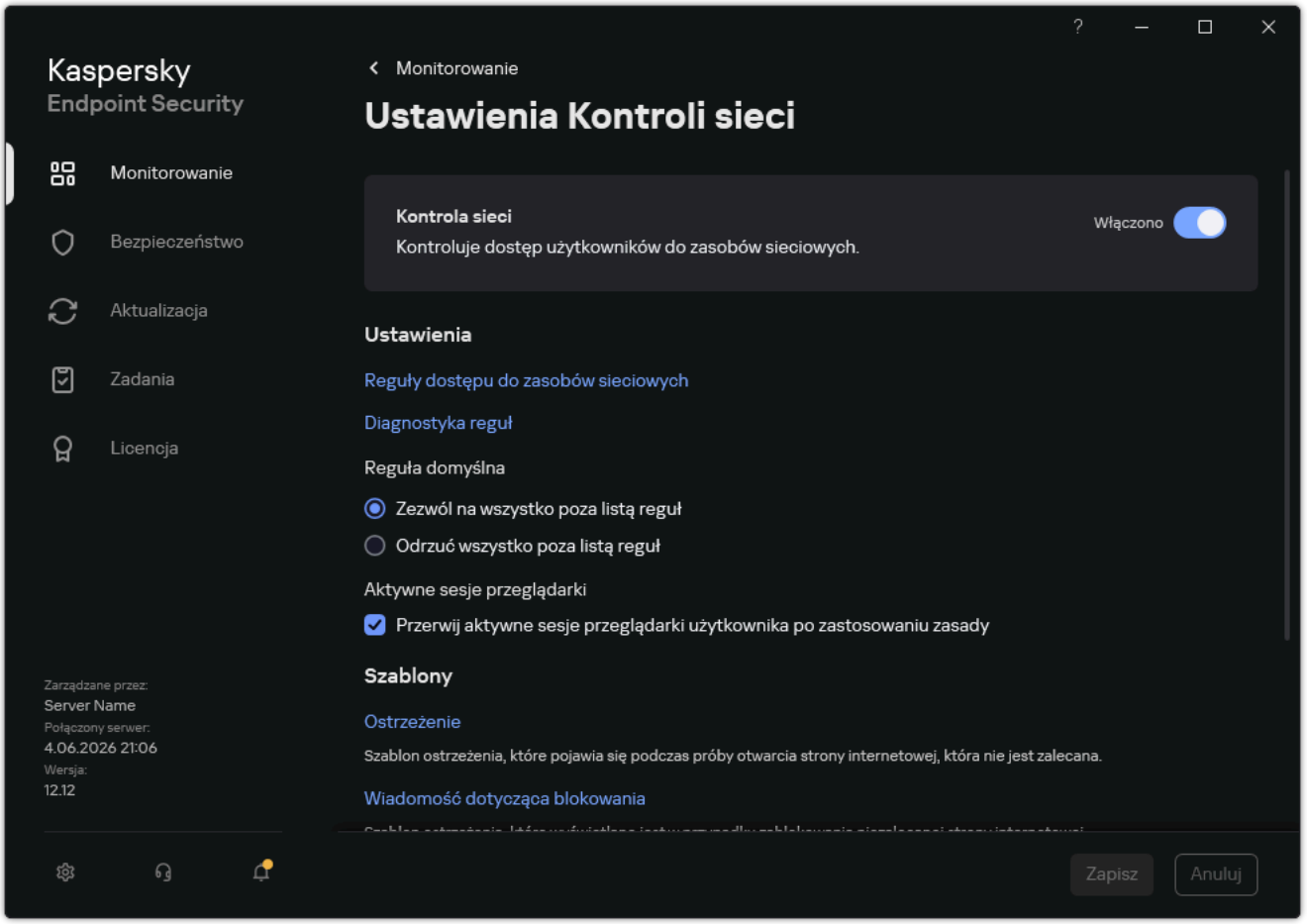
Podczas konfigurowania Kontroli sieci możesz przypadkowo zablokować dostęp do zasobów sieciowych, których użytkownicy potrzebują do pracy. Aby sprawdzić, która reguła Kontroli sieci blokuje dostęp do zasobów sieciowych, możesz użyć narzędzia *Diagnostyka reguł Kontroli sieci*. Diagnostyka reguł Kontroli sieci jest dostępna tylko w interfejsie Kaspersky Endpoint Security. Informacji o regułach Kontroli sieci obejmujących dany zasób nie można znaleźć w konsoli Kaspersky Security Center.

Jeśli użytkownik sądzi, że zasób sieciowy został zablokowany przez pomyłkę, może kliknąć odnośnik w wiadomości informującej o zablokowaniu zasobu sieciowego w celu wysłania wcześniej wygenerowanej wiadomości do administratora firmowej sieci lokalnej.

W celu przetestowania reguły dostępu do zasobu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń → Kontrola sieci**.



Ustawienia komponentu Kontrola sieci

3. W sekcji **Ustawienia** kliknij odnośnik **Diagnostyka reguł**.

   Zostanie otwarte okno **Diagnostyka reguł**.

4. Jeśli chcesz przetestować reguły wykorzystywane przez Kaspersky Endpoint Security do kontrolowania dostępu do określonego zasobu sieciowego, zaznacz pole **Określ adres**. Wprowadź adres zasobu internetowego w polu poniżej.

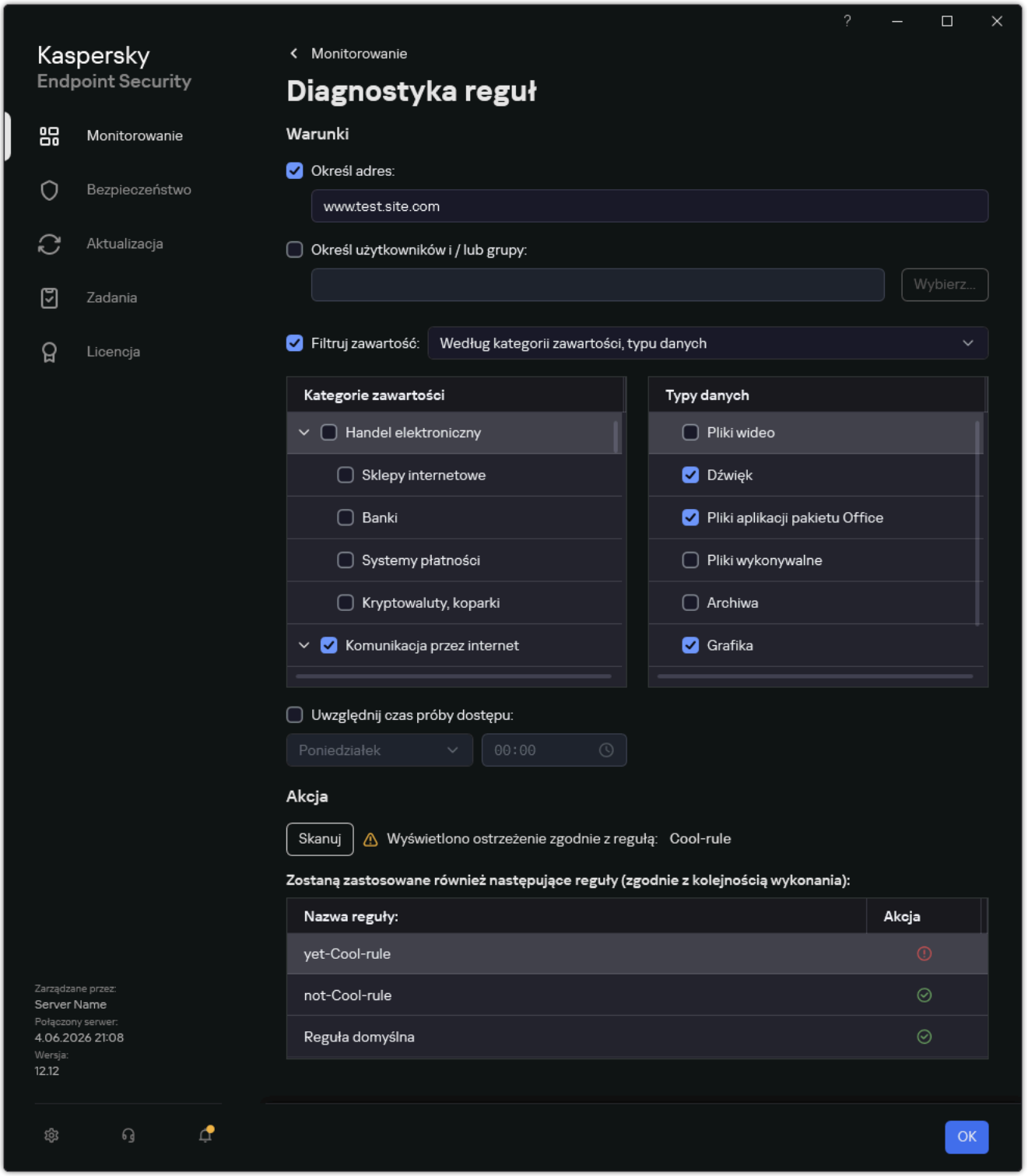
5. Jeśli chcesz przetestować reguły wykorzystywane przez Kaspersky Endpoint Security do kontrolowania dostępu do zasobów sieciowych dla określonych użytkowników i / lub grup użytkowników, określ listę użytkowników i / lub grup użytkowników.

6. Jeśli chcesz przetestować reguły wykorzystywane przez Kaspersky Endpoint Security do kontrolowania dostępu do zasobów sieciowych o pewnych kategoriach zawartości i/lub kategoriach typu danych, zaznacz pole **Filtruj zawartość** i wybierz odpowiednią opcję z listy rozwijalnej (**Według kategorii zawartości**, **Według typu danych** lub **Według kategorii zawartości, typu danych**).

7. Jeśli chcesz przetestować reguły biorąc pod uwagę godzinę i dzień tygodnia, w którym podejmowana jest próba uzyskania dostępu do zasobów sieciowych określonych w warunkach diagnostyki, zaznacz pole **Uwzględnij czas próby dostępu**. Następnie określ dzień tygodnia i czas.

8. Kliknij **Skanuj**.

Po zakończeniu testu wyświetlana jest wiadomość o akcji podjętej przez Kaspersky Endpoint Security, zgodnej z pierwszą regułą wyzwoloną przy próbie dostępu do określonego zasobu sieciowego (akceptuj, zablokuj lub ostrzeżenie). Pierwsza wyzwolona reguła to ta zajmująca wyższą pozycję na liście reguł Kontroli sieci niż reszta reguł spełniających warunki diagnostyki. Wiadomość jest wyświetlana po prawej stronie przycisku **Skanuj**. Następująca tabela wyświetla pozostałe wyzwolone reguły, określając akcję wykonaną przez Kaspersky Endpoint Security. Reguły uszeregowane są malejąco według priorytetu.



Wyniki testu dostępu do zasobu sieciowego

Eksportowanie i importowanie reguł kontroli sieci

Możesz wyeksportować listę reguł Kontroli sieci do pliku XML lub JSON. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę adresów tego samego typu. Możesz użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy reguł Kontroli sieci lub przeniesienia listy na inny serwer.

Jak w Konsoli administracyjnej (MMC) wyeksportować i zaimportować listę reguł Kontroli sieci?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń → Kontrola sieci**.
4. W celu wyeksportowania listy reguł Kontroli sieci:
   a. Wybierz reguły, które chcesz zmienić. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
      Jeśli nie wybrałeś żadnej reguły, Kaspersky Endpoint Security wyeksportuje wszystkie reguły.
   b. Kliknij odnośnik **Eksportuj**.
   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę reguł, i wybierz folder, w którym chcesz zapisać ten plik.
   d. Zapisz plik.
      Kaspersky Endpoint Security eksportuje listę reguł do pliku XML.
5. W celu zaimportowania listy reguł Kontroli sieci:
   a. Kliknij odnośnik **Importuj**.
      W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.
   b. Otwórz plik.
      Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
6. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console wyeksportować i zaimportować listę reguł Kontroli sieci?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń → Kontrola sieci**.

5. W celu wyeksportowania listy reguł w sekcji **Lista reguł**:

   a. Wybierz reguły, które chcesz zmienić.

   b. Kliknij przycisk → **Eksportuj**.

      Kaspersky Endpoint Security eksportuje listę reguł do pliku JSON w domyślnym folderze do pobrania.

6. W celu zaimportowania listy reguł w sekcji **Lista reguł**:

   a. Kliknij przycisk → **Importuj**.

      W oknie, które zostanie otwarte, wybierz plik JSON, z którego chcesz zaimportować listę reguł.

   b. Otwórz plik.

      Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku JSON.

7. Zapisz swoje zmiany.

Eksportowanie i importowanie adresów zasobu sieciowego z reguły Kontroli sieci

Jeżeli w regule dostępu do zasobu sieciowego utworzyłeś listę adresów zasobów sieciowych, będziesz mógł ją wyeksportować do pliku:

- W formacie TXT w konsoli administracyjnej (MMC)
- W formacie CSV w interfejsie aplikacji

Możliwe będzie również zaimportowanie listy z tego pliku, dzięki czemu podczas konfigurowania reguły dostępu nie będzie konieczne tworzenie nowej listy. Opcja eksportowania i importowania listy adresów dostępu do zasobów sieciowych jest użyteczna, gdy, na przykład, tworzysz reguły dostępu z tymi samymi parametrami.

Możesz też wyeksportować/zaimportować wszystkie reguły Kontroli sieci, a nie tylko adresy zasobów sieciowych poszczególnych reguł.

Nie możesz eksportować/importować adresów zasobów sieciowych reguł Kontroli sieci w Web Console ani Cloud Console.

Jak eksportować/importować adresy zasobów sieciowych reguły Kontroli sieci w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
4. W bloku **Ustawienia Kontroli sieci** wybierz regułę, której listę adresów zasobów sieciowych chcesz wyeksportować lub zaimportować.

   Zostaną wyświetlone właściwości reguły Kontroli sieci.

5. Aby wyeksportować listę zasobów sieciowych, na liście adresów wykonaj następujące czynności:

   a. Wybierz adresy, które chcesz wyeksportować.

      Jeśli nie wybrałeś żadnego adresu, Kaspersky Endpoint Security wyeksportuje wszystkie adresy.

   b. Kliknij przycisk .

   c. W otwartym oknie wprowadź nazwę pliku TXT, do którego chcesz wyeksportować listę adresów zasobów internetowych i wybierz folder, w którym chcesz zapisać ten plik.

   d. Zapisz plik.

      Kaspersky Endpoint Security eksportuje listę adresów zasobów internetowych do pliku TXT.

6. Aby zaimportować listę zasobów sieciowych, na liście adresów wykonaj następujące czynności:

   a. Kliknij przycisk .

      W oknie, które zostanie otwarte, wybierz plik TXT, z którego chcesz zaimportować listę zasobów sieciowych.

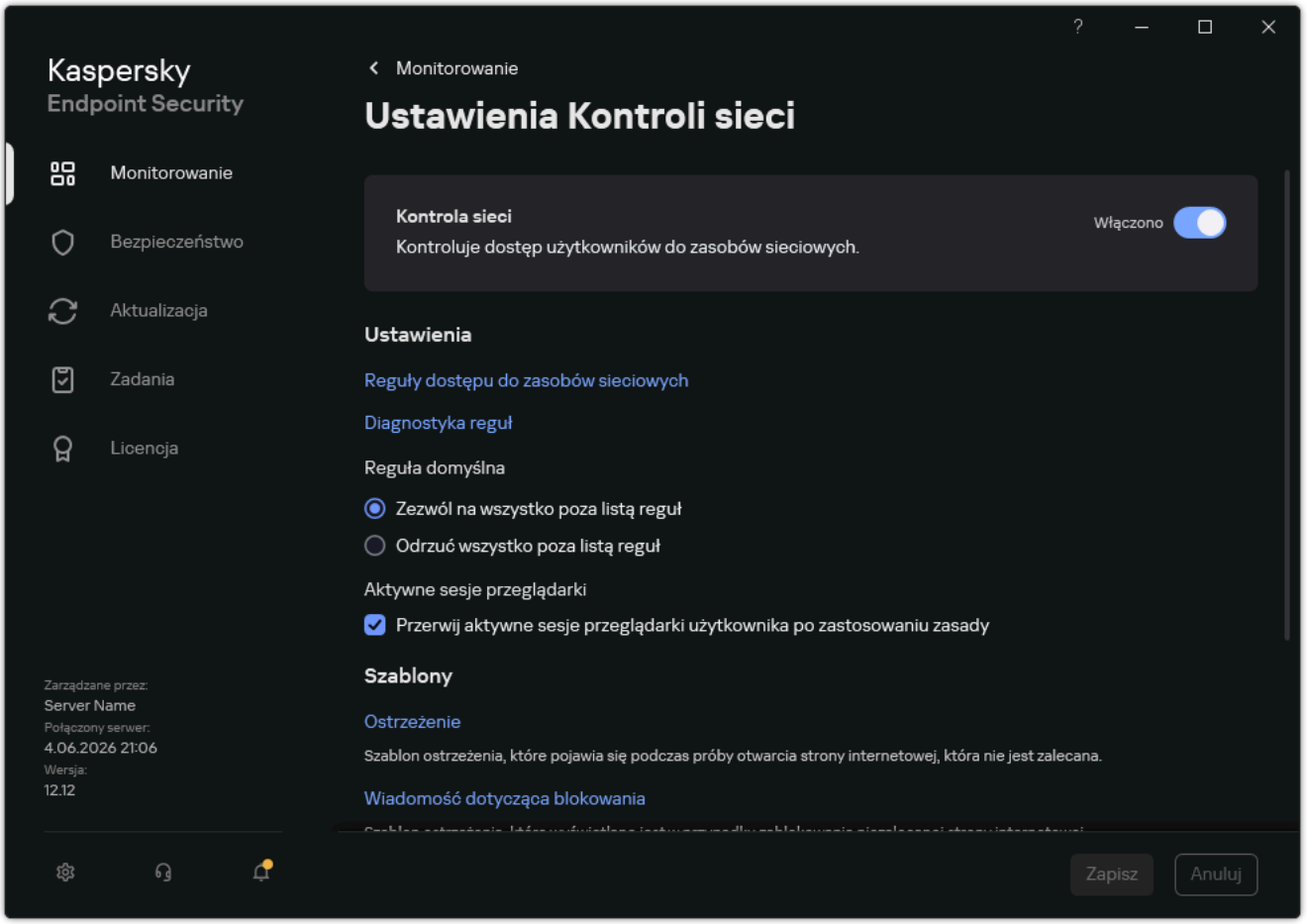
   b. Otwórz plik.

      Jeśli komputer ma już listę zaufanych adresów, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku TXT.

7. Zapisz swoje zmiany.

Jak eksportować/importować adresy zasobów sieciowych reguły Kontroli sieci w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń → Kontrola sieci**.



Ustawienia komponentu Kontrola sieci

3. W sekcji **Ustawienia** kliknij przycisk **Reguły dostępu do zasobów sieciowych**.
4. Wybierz regułę, której listę adresów zasobów sieciowych chcesz wyeksportować lub zaimportować.
5. W celu wyeksportowania listy zaufanych adresów sieciowych, w sekcji **Adresy** wykonaj następujące czynności:
   a. Wybierz adresy, które chcesz wyeksportować.
      Jeśli nie wybrałeś żadnego adresu, Kaspersky Endpoint Security wyeksportuje wszystkie adresy.
   b. Kliknij **Eksportuj**.
   c. W otwartym oknie wprowadź nazwę pliku CSV, do którego chcesz wyeksportować listę adresów zasobów internetowych i wybierz folder, w którym chcesz zapisać ten plik.
   d. Zapisz plik.
      Kaspersky Endpoint Security eksportuje listę adresów zasobów internetowych do pliku CSV.
6. W celu zaimportowania listy zasobów sieciowych, w sekcji **Adresy** wykonaj następujące czynności:
   a. Kliknij **Importuj**.
      W oknie, które zostanie otwarte, wybierz plik CSV, z którego chcesz zaimportować listę zasobów sieciowych.

b. Otwórz plik.

Jeśli komputer ma już listę zaufanych adresów, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku CSV.

7. Zapisz swoje zmiany.

Monitorowanie aktywności użytkownika w internecie

Kaspersky Endpoint Security umożliwia zapisywanie danych dotyczących odwiedzin użytkownika na wszystkich stronach internetowych, w tym dozwolonych stronach internetowych. Umożliwia to uzyskanie pełnej historii wyświetleń przeglądarki. Kaspersky Endpoint Security wysyła zdarzenia dotyczące aktywności użytkownika do Kaspersky Security Center, do lokalnego raportu Kaspersky Endpoint Security, a także do dziennika zdarzeń systemu Windows. Aby uzyskać zdarzenia w Kaspersky Security Center, należy skonfigurować ustawienia zdarzeń w zasadzie w Konsoli administracyjnej lub w Web Console. Można także skonfigurować przesyłanie zdarzeń Web Control za pośrednictwem poczty elektronicznej oraz wyświetlanie powiadomień na komputerze użytkownika.

Przeglądarki obsługujące funkcję monitorowania: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Monitorowanie aktywności użytkownika nie działa w innych przeglądarkach.

Kaspersky Endpoint Security tworzy następujące zdarzenia aktywności użytkownika w internecie:

- Zablokuj status witryny (*Krytyczny*).
- Odwiedzenie niezalecanej strony internetowej (stan *Ostrzeżenie*).
- Odwiedzenie dozwolonej strony internetowej (stan *Informacja*).

Przed włączeniem monitorowania aktywności użytkownika w internecie należy wykonać następujące czynności:

- Wstrzykuj skrypt do ruchu sieciowego w celu interakcji ze stronami sieciowymi (patrz instrukcje poniżej). Skrypt włącza rejestrację zdarzeń Kontroli sieci.
- Dla monitorowania ruchu HTTPS należy włączyć skanowanie zaszyfrowanych połączeń.

Wprowadzenie skryptu interakcji ze stronami internetowymi

Jak wprowadzić skrypt interakcji ze stronami internetowymi do ruchu sieciowego w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
4. W sekcji **Skanowanie połączeń szyfrowanych** zaznacz pole **Wstrzykuj skrypt do ruchu sieciowego w celu interakcji ze stronami internetowymi**.
5. Zapisz swoje zmiany.

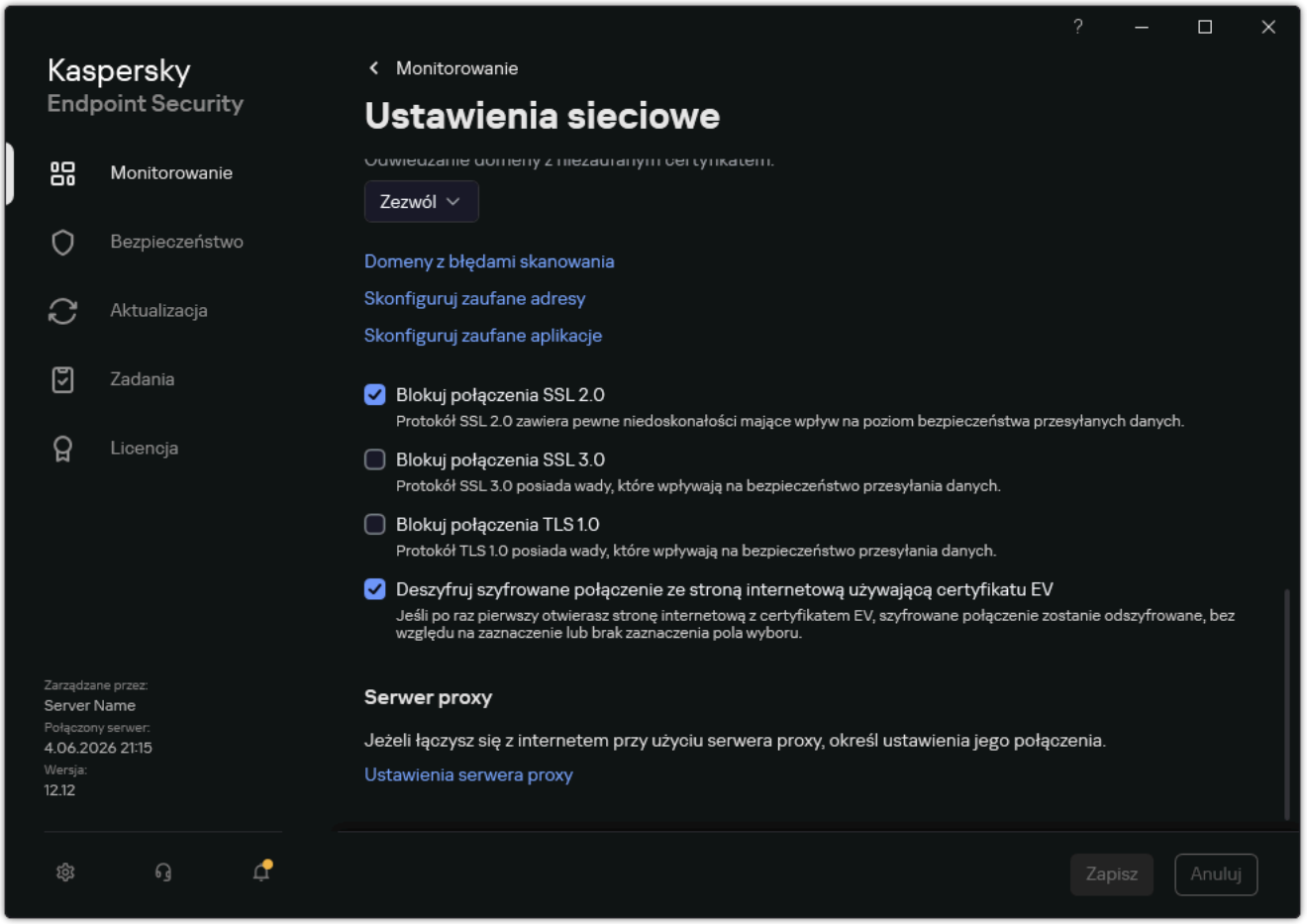
Jak wprowadzić skrypt interakcji ze stronami internetowymi do ruchu sieciowego w konsoli Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
5. W menu **Monitorowanie połączeń internetowych** włącz przełącznik **Monitorowanie połączeń internetowych WŁĄCZONE**.
6. Zapisz swoje zmiany.

Sposób wprowadzenia skryptu interakcji ze stronami internetowymi do ruchu sieciowego w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.



Ustawienia sieciowe aplikacji

3. W sekcji **Przetwarzanie ruchu sieciowego** zaznacz pole **Wstrzykuj skrypt do ruchu sieciowego w celu interakcji ze stronami internetowymi**.
4. Zapisz swoje zmiany.

W rezultacie Kaspersky Endpoint Security wstrzyknie skrypt interakcji ze stronami internetowymi do ruchu sieciowego. Ten skrypt umożliwia rejestrację zdarzeń Kontroli sieci dla dziennika zdarzeń aplikacji, dziennika zdarzeń systemu operacyjnego i raportów.

Konfigurowanie rejestrowania zdarzeń Kontroli sieci

W celu skonfigurowania rejestrowania zdarzeń Kontroli sieci na komputerze użytkownika:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Interfejs**.
3. W sekcji **Powiadomienia** kliknij przycisk **Skonfiguruj powiadomienia**.
4. W otwartym oknie wybierz sekcję **Kontrola sieci**.

   Spowoduje to otwarcie tabeli zdarzeń Kontroli sieci i metod powiadamiania.
5. Skonfiguruj metodę powiadamiania dla każdego zdarzenia: **Zapisz w raporcie lokalnym** lub **Zapisz w dzienniku zdarzeń Windows**.

   Aby zapisywać zdarzenia dotyczące odwiedzania dozwolonych stron internetowych, należy skonfigurować Kontrolę sieci (zapoznaj się z poniższymi instrukcjami).

   W tabeli zdarzeń można także włączyć powiadomienia ekranowe i powiadomienia e-mail. Aby powiadomienia były wysyłane w wiadomościach e-mail, należy skonfigurować ustawienia serwera SMTP. Więcej informacji o wysyłaniu powiadomień za pośrednictwem poczty elektronicznej znajdziesz w pomocy do Kaspersky Security Center.
6. Zapisz swoje zmiany.

W wyniku tego Kaspersky Endpoint Security rozpocznie rejestrowanie zdarzeń dotyczących aktywności użytkownika w internecie.

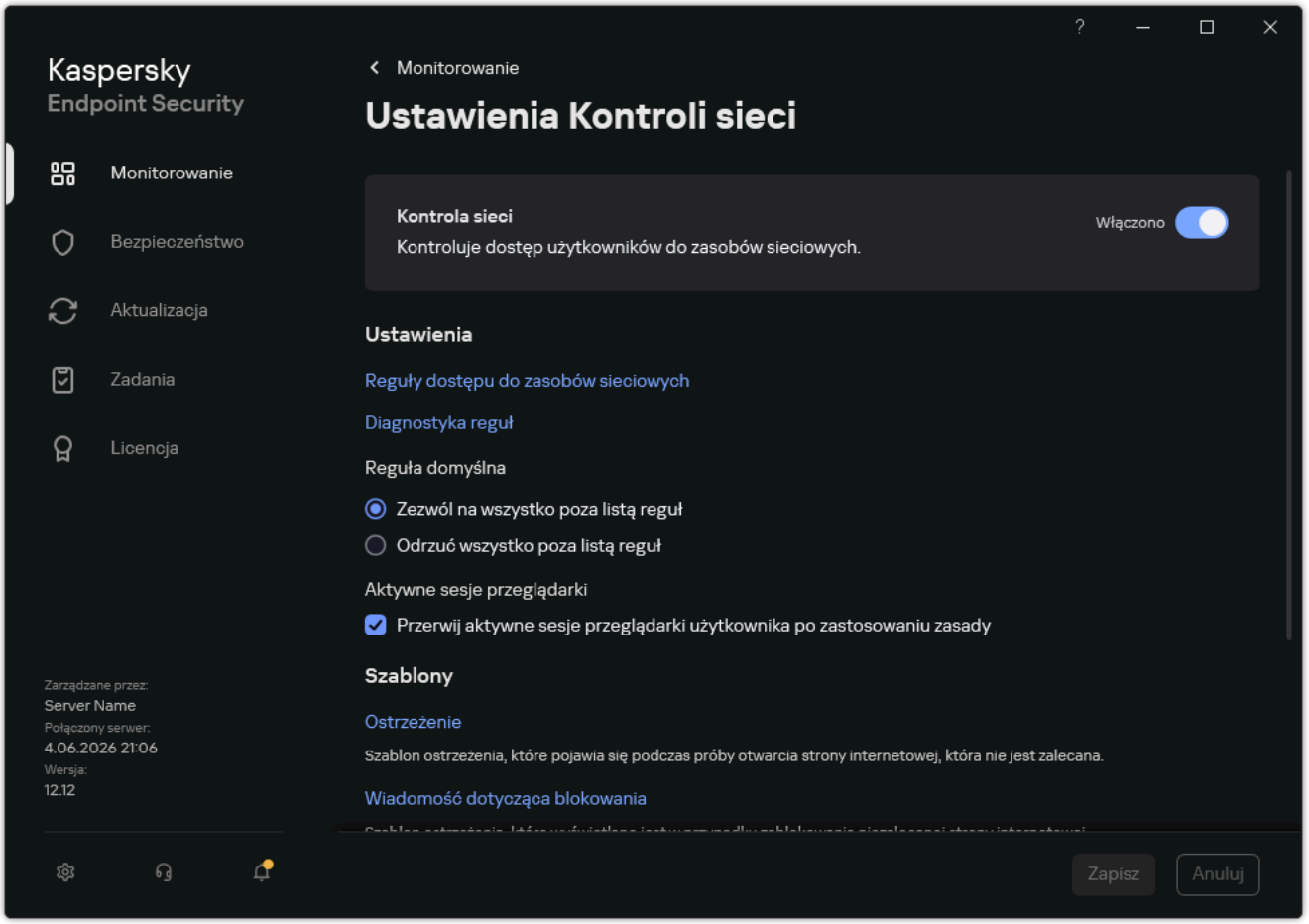
Kontrola sieci wysyła zdarzenia aktywności użytkownika do Kaspersky Security Center w następujący sposób:

- Jeśli używasz Kaspersky Security Center, Kontrola sieci wysyła zdarzenia dla wszystkich obiektów tworzących stronę internetową. Z tego powodu kilka zdarzeń może zostać utworzonych po zablokowaniu strony. Na przykład, podczas blokowania strony http://www.example.com, Kaspersky Endpoint Security może przesłać zdarzenia dla następujących obiektów: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js, itd.
- Jeśli korzystasz z Kaspersky Security Center Cloud Console, Kontrola sieci grupuje zdarzenia i wysyła tylko protokół i domenę witryny. Na przykład, jeśli użytkownik otworzy niezalecane strony internetowe http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, Kaspersky Endpoint Security wyśle tylko jedno zdarzenie z obiektem http://www.example.com.

Rejestrowanie zdarzeń podczas odwiedzania dozwolonych witryn

Aby włączyć zapisywanie zdarzeń podczas odwiedzania dozwolonych witryn:

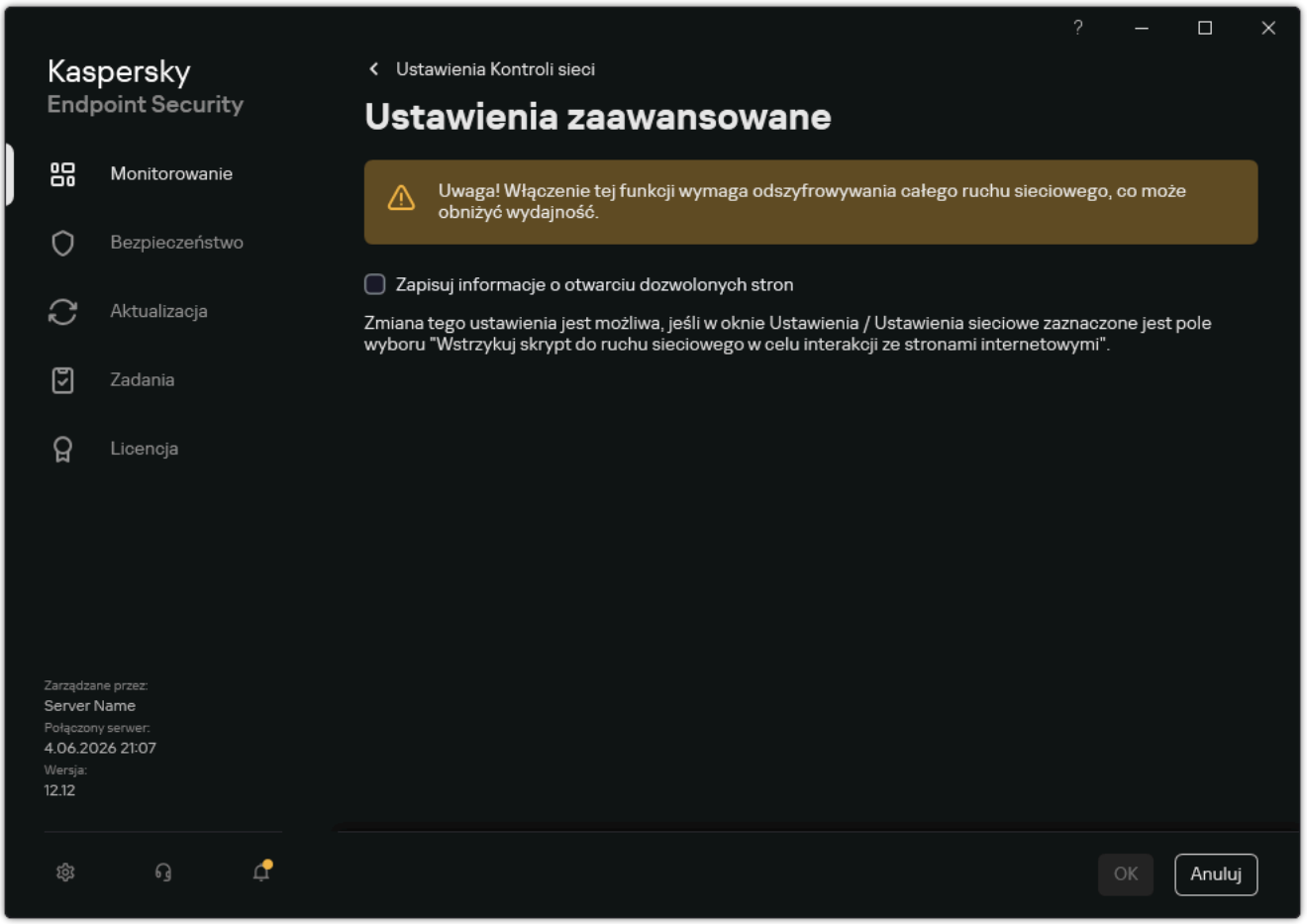
1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.



Ustawienia komponentu Kontrola sieci

3. W sekcji **Dodatkowe** kliknij przycisk **Ustawienia zaawansowane**.

4. W otwartym oknie zaznacz pole **Zapisuj informacje o otwarciu dozwolonych stron**.



Ustawienia komponentu zaawansowanego Kontrola sieci

5. Zapisz swoje zmiany.

W rezultacie możliwe będzie przejrzenie całej historii przeglądania.

Modyfikowanie szablonów wiadomości Kontroli sieci

W zależności od typu akcji określonej we właściwościach reguł Kontroli sieci, przy próbie dostępu użytkowników do zasobów internetowych Kaspersky Endpoint Security wyświetla wiadomość o jednym z następujących typów (zamiast odpowiedzi serwera HTTP aplikacja dostarcza stronę HTML z wiadomością):

- Ostrzeżenie. Taka wiadomość ostrzega użytkownika, że odwiedzenie zasobu sieciowego nie jest zalecane i/lub narusza politykę bezpieczeństwa firmy. Kaspersky Endpoint Security wyświetla ostrzeżenie, jeśli w ustawieniach reguły opisującej ten zasób sieciowy wybrano opcję **Ostrzegaj**.

  Jeśli użytkownik sądzi, że ostrzeżenie jest pomyłką, może kliknąć odnośnik w ostrzeżeniu w celu wysłania wcześniej wygenerowanej wiadomości do administratora lokalnej sieci firmowej.

- Wiadomość informująca o zablokowaniu zasobu sieciowego. Kaspersky Endpoint Security wyświetla wiadomość informującą o zablokowaniu zasobu (patrz rysunek poniżej), jeśli w ustawieniach reguły opisującej ten zasób sieciowy wybrano opcję **Zablokuj**.

Jeśli użytkownik sądzi, że zasób sieciowy został zablokowany przez pomyłkę, może kliknąć odnośnik w wiadomości informującej o zablokowaniu zasobu sieciowego w celu wysłania wcześniej wygenerowanej wiadomości do administratora lokalnej sieci firmowej.



Komunikat o blokowaniu zasobów sieciowych

Dostępne są specjalne szablony dla wiadomości ostrzegającej, informującej o zablokowaniu zasobu sieciowego i zgłoszenia wysyłanego do administratora sieci LAN. Do zarządzania szablonami wiadomości dostępne są zmienne specjalne (na przykład %USER_NAME%). Zmienne umożliwiają stosowanie tego samego szablonu wiadomości na różnych komputerach. Podczas generowania wiadomości program Kaspersky Endpoint Security pobiera wartość zmiennej z ustawień systemu operacyjnego i wstawia ją do wiadomości odpowiedniej dla danego komputera, użytkownika i zdarzenia.

Jak zmienić szablon wiadomości kontroli sieci w konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
4. W sekcji **Ustawienia szablonu wiadomości** kliknij przycisk **Szablony**.

5. Skonfiguruj szablony wiadomości kontroli sieci:

   - **Ostrzeżenie**. Pole do wprowadzenia danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła ostrzegająca o próbach uzyskania dostępu do niechcianych zasobów sieciowych.

   - **Wiadomość dotycząca blokowania**. To pole do wprowadzania danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła blokująca dostęp do zasobu sieciowego.

   - **Wiadomość do administratora**. Szablon wiadomości wysyłanej do administratora sieci LAN, gdy użytkownik uważa blokadę za pomyłkę. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania dostępu do strony internetowej**. Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkownika**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

   Aby dodać zmienną do tekstu szablonu, umieść kursor w odpowiednim miejscu, kliknij przycisk **Zmienna** i wybierz wymaganą zmienną z listy dostępnych opcji.

   Możesz również przywrócić domyślny tekst szablonu za pomocą przycisku **Domyślny**.

6. Zapisz swoje zmiany.

Jak zmienić szablon wiadomości kontroli sieci w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.

5. W sekcji **Szablony wiadomości** kliknij odnośnik **Wiadomość dotycząca blokowania strony internetowej** i skonfiguruj szablony dla wiadomości Kontroli sieci:

   - **Ostrzegawczy**. Pole do wprowadzenia danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła ostrzegająca o próbach uzyskania dostępu do niechcianych zasobów sieciowych.

   - **Wiadomość dotycząca blokowania**. To pole do wprowadzania danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła blokująca dostęp do zasobu sieciowego.

   - **Wiadomość do administratora**. Szablon wiadomości wysyłanej do administratora sieci LAN, gdy użytkownik uważa blokadę za pomyłkę. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania dostępu do strony internetowej**. Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkownika**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

   Aby dodać zmienną do tekstu szablonu, umieść kursor w odpowiednim miejscu, kliknij przycisk **Dodaj zmienną** i wybierz wymaganą zmienną z listy dostępnych opcji.

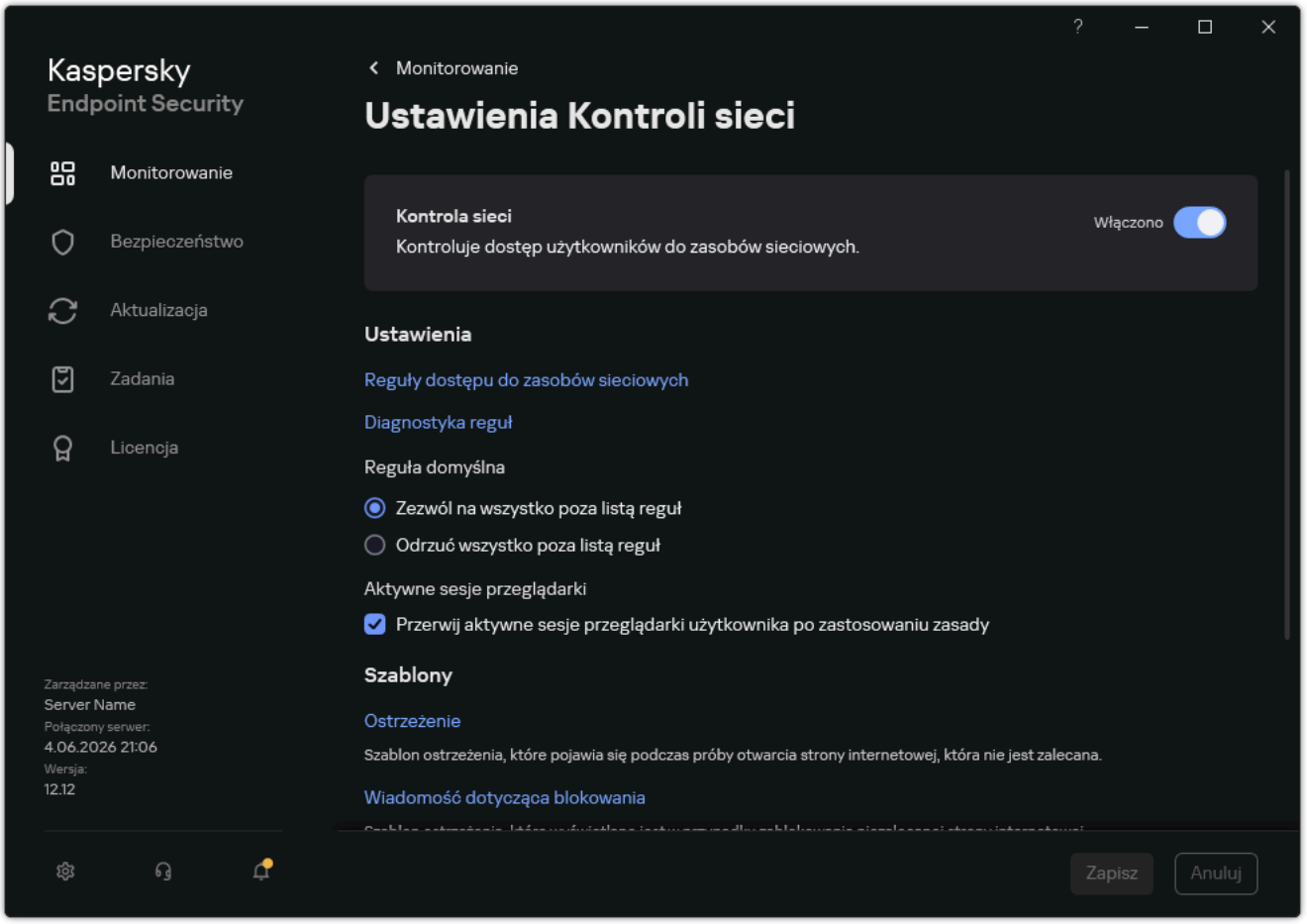
Możesz również przywrócić domyślny tekst szablonu za pomocą przycisku **Resetuj do ustawień domyślnych**.

6. Zapisz swoje zmiany.

Jak zmienić szablon wiadomości kontroli sieci w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń → Kontrola sieci**.



Ustawienia komponentu Kontrola sieci

3. W sekcji **Szablony** skonfiguruj szablony dla wiadomości Kontroli sieci:

   - **Ostrzeżenie**. Pole do wprowadzenia danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła ostrzegająca o próbach uzyskania dostępu do niechcianych zasobów sieciowych.

   - **Wiadomość dotycząca blokowania**. To pole do wprowadzania danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła blokująca dostęp do zasobu sieciowego.

   - **Wiadomość do administratora**. Szablon wiadomości wysyłanej do administratora sieci LAN, gdy użytkownik uważa blokadę za pomyłkę. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania dostępu do strony internetowej**. Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkownika**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

   Aby dodać zmienną do tekstu szablonu, umieść kursor w odpowiednim miejscu, kliknij przycisk **Dodaj zmienną** i wybierz wymaganą zmienną z listy dostępnych opcji.

Możesz również przywrócić domyślny tekst szablonu za pomocą przycisku **Resetuj**.

4. Zapisz swoje zmiany.

Modyfikowanie masek adresów zasobów sieciowych

Korzystanie z *maski adresu zasobu sieciowego* (nazywanej również „maską adresu") może być użyteczne, gdy podczas tworzenia reguły dostępu do zasobu sieciowego wprowadzasz kilka podobnych adresów zasobów sieciowych. Jedna maska adresu może odpowiadać większej liczbie adresów zasobów sieciowych.

Podczas tworzenia maski adresu postępuj zgodnie z następującymi regułami:

1. Symbol `*` zastępuje dowolną sekwencję zawierającą zero lub więcej znaków.

   Na przykład, gdy wprowadzisz maskę adresu `*abc*`, reguła dostępu będzie stosowana do wszystkich zasobów sieciowych zawierających sekwencję znaków `abc`. Na przykład: `http://www.example.com/page_0-9abcdef.html`.

2. Sekwencja znaków `*.` (znana jako *maska domeny*) umożliwia wybranie wszystkich domen adresu. Maska domeny `*.` reprezentuje dowolną nazwę domeny, nazwę poddomeny lub pusty wiersz.

   Na przykład: maska `*.example.com` reprezentuje następujące adresy:

   - `http://pictures.example.com`. Maska domeny `*.` reprezentuje `pictures.`.
   - `http://user.pictures.example.com`. Maska domeny `*.` reprezentuje `pictures.` i `user.`.
   - `http://example.com`. Maska domeny `*.` Jest interpretowana jako pusty wierszy.

3. Sekwencja znaków `www.` na początku maski adresu jest interpretowana jako sekwencja `*.`.

   Przykład: maska adresu `www.example.com` jest traktowana jako `*.example.com`. Ta maska obejmuje adresy `www2.example.com` i `www.pictures.example.com`.

4. Jeżeli maska adresu nie rozpoczyna się od znaku `*`, wówczas zawartość maski adresu będzie odpowiadała tej samej zawartości z przedrostkiem `*.`.

5. Jeśli maska adresu kończy się znakiem innym niż `/` lub `*`, zawartość maski adresu jest traktowana jak ta sama zawartość z przyrostkiem `/*`.

   Na przykład: maska adresu `http://www.example.com` odpowiada adresowi `http://www.example.com/abc`, gdzie `a`, `b` i `c` są dowolnymi znakami.

6. Jeżeli maska adresu kończy się znakiem `/`, wówczas zawartość maski adresu będzie odpowiadała tej samej zawartości z przyrostkiem `/*`.

7. Sekwencja znaku `/*` na końcu maski adresu jest interpretowana jako `/*` lub pusty ciąg znaków.

8. Adresy zasobów sieciowych są weryfikowane na podstawie maski adresu z uwzględnieniem protokołu (http lub https):

   - Jeżeli maska adresu nie zawiera protokołu sieciowego, będzie ona odpowiadała adresom z dowolnym protokołem sieciowym.

     Przykład: maska adresu `example.com` obejmuje adresy `http://example.com` i `https://example.com`.

- Jeżeli maska adresu zawiera protokół sieciowy, będzie ona odpowiadała tylko adresowi z tym samym protokołem sieciowym.

  Na przykład: maska adresu `http://*.example.com` odpowiada adresowi `http://www.example.com`, ale nie adresowi `https://www.example.com`.

9. Maska adresu podana w podwójnych cudzysłowach jest przetwarzana bez brania pod uwagę dodatkowych zamienników, za wyjątkiem znaku `*`, jeśli został włączony w skład maski adresu. Reguły 5 i 7 nie są stosowane do masek adresów umieszczonych w podwójnym cudzysłowie (przykłady 14 – 18 w tabeli poniżej).

10. Podczas porównywania z maską adresu zasobu sieciowego nie jest brana pod uwagę nazwa użytkownika i hasło, port połączenia oraz wielkość znaków.

Przykłady użycia reguł tworzenia masek adresów

Nr	Maska adresu	Sprawdzany adres zasobu sieciowego	Zastępowanie adresu przez maskę adresu	Komentarz
1	*.example.com	http://www.123example.com	Nie	Patrz reguła 1.
2	*.example.com	http://www.123.example.com	Tak	Patrz reguła 2.
3	*example.com	http://www.123example.com	Tak	Patrz reguła 1.
4	*example.com	http://www.123.example.com	Tak	Patrz reguła 1.
5	http://www.*.example.com	http://www.123example.com	Nie	Patrz reguła 1.
6	www.example.com	http://www.example.com	Tak	Patrz reguły 3, 2, 1.
7	www.example.com	https://www.example.com	Tak	Patrz reguły 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Tak	Patrz reguły 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Tak	Patrz reguły 3, 5, 1.
10	example.com	http://www.example.com	Tak	Patrz reguły 3, 1.
11	http://example.com/	http://example.com/abc	Tak	Patrz reguła 6.
12	http://example.com/*	http://example.com	Tak	Patrz reguła 7.
13	http://example.com	https://example.com	Nie	Patrz reguła 8.
14	"example.com"	http://www.example.com	Nie	Patrz reguła 9.
15	"http://www.example.com"	http://www.example.com/abc	Nie	Patrz reguła 9.
16	"*.example.com"	http://www.example.com	Tak	Patrz reguły 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Tak	Patrz reguły 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Tak	Patrz reguły 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Nie	Maska adresu zawiera więcej informacji niż adres zasobu sieciowego.

Kontrola sieci dla maszyn wirtualnych

Kontrola sieci kontroluje ruch na komputerze, a także na maszynie wirtualnej, która jest lokalnie wdrożona na komputerze. Działa to bez konieczności instalowania aplikacji Kaspersky Endpoint Security na lokalnej maszynie wirtualnej. Oznacza to, że jeśli użytkownik spróbuje otworzyć w przeglądarce stronę internetową blokowaną przez regułę kontroli sieci *maszyna wirtualna*, aplikacja zainstalowana w systemie operacyjnym hosta *komputera* odmawia dostępu do tej witryny.

Kontrola sieci działa różnie w przypadku różnych maszyn wirtualnych.

Oracle VM VirtualBox

Kaspersky Endpoint Security obsługuje reguły Kontroli sieci na maszynach wirtualnych Oracle VM VirtualBox bez ograniczeń. Aplikacja może kontrolować cały ruch maszyny wirtualnej. Jeśli w regułach Kontroli sieci skonfigurowany jest filtr według użytkownika, aplikacja działa poprawnie, ponieważ wszystkie procesy maszyn wirtualnych są uruchamiane przez użytkownika lokalnego.

VMware Workstation

Kaspersky Endpoint Security obsługuje reguły kontroli sieci na maszynach wirtualnych VMware Workstation z ograniczeniami. Aplikacja nie obsługuje reguł ze skonfigurowanym filtrem według użytkownika. Procesy maszyny wirtualnej działają w ramach użytkownika systemowego (SYSTEM). Uniemożliwia to identyfikację użytkownika próbującego otworzyć stronę na maszynie wirtualnej.

Microsoft Hyper-V

Kaspersky Endpoint Security nie obsługuje reguł kontroli sieci na maszynach wirtualnych Microsoft Hyper-V.

Zmienne w szablonach komunikatów komponentu Kontrola sieci

W szablonach wiadomości użytkownika lub szablonach wiadomości administratora można używać następujących zmiennych:

- **Użytkownik** – `%USER_NAME%`.

  Nazwa bieżącego konta użytkownika na komputerze, na którym wygenerowano wiadomość, w formacie `<device name>\<user alias>` (na przykład `DESKTOP-123\John.Smith`).

- **Adres zasobu sieciowego** – `%CANONIC_REQUEST_URL%`.

  Adres zablokowanego zasobu sieciowego.

- **Nazwa reguły** – `%RULE%`.

  Nazwa reguły, która zablokowała zasób sieciowy.

- **Adres e-mail do wysłania wiadomości** – `%COMPLAIN_EMAIL%`.

  Adres e-mail do przesyłania opinii na temat bloków zasobów sieciowych. Po kliknięciu adresu e-mail otwiera się okno, w którym użytkownik może napisać wiadomość do administratora.

- **Nazwa kategorii zawartości** – `%CONTENT_CATEGORY_LIST%`.

  Kategoria witryny, do której należy zablokowany zasób (na przykład *Systemy płatności*).

- **Nazwa kategorii typu danych** – `%TYPE_CATEGORY_LIST%`.

  Kategoria typu danych w zablokowanym zasobie sieciowym (na przykład *Pliki graficzne*).

- **Odnośnik do żądanego zasobu sieciowego** – `%CONTINUE_PAGE%`.

  Link do żądanej strony internetowej (na przykład `http://www.example.com/pagename.html`).

- **Odnośnik do strony internetowej** – `%CONTINUE_SITE%`.

  Link do witryny zawierającej żądaną stronę internetową (na przykład `http://www.example.com/`).

- **Odnośnik dostępu do domen** – `%CONTINUE_DOMAIN%`.

  Link, który można kliknąć, aby uzyskać dostęp do wszystkich istniejących stron internetowych danej nazwy domeny. Na przykład, jeśli adres zablokowanej strony internetowej to `http://www.example.com`, zmienna `%CONTINUE_DOMAIN%` jest zastępowana linkiem `http://*.example.com`. Kliknięcie tego linku umożliwia dostęp do wszystkich adresów internetowych domeny bazowej `http://www.example.com/`, w tym do poddomen, na przykład `http://start.example.com/*` lub `http://domain.domain.example.com/*`, gdzie `*` znak oznacza dowolny ciąg znaków (w tym pusty ciąg).

Kontrola urządzeń

Kontrola urządzeń zarządza dostępem użytkownika do urządzeń, które są instalowane na komputerze lub są podłączone do komputera (na przykład: dyski twarde, kamery lub moduły Wi-Fi). Umożliwia to ochronę komputera przed infekcją, gdy takie urządzenia są podłączone, oraz zapobieganie utracie lub wyciekowi danych.

Jeśli komponent Kontrola urządzeń jest włączony, aplikacja przekazuje informacje o podłączonych urządzeniach do Kaspersky Security Center. Listę podłączonych urządzeń można przejrzeć w Kaspersky Security Center, w folderze **Zaawansowane** → **Repozytoria** → **Sprzęt**.

Poziomy dostępu do urządzenia

Kontrola urządzeń kontroluje dostęp na następujących poziomach:

- **Typ urządzenia**. Na przykład: drukarki, dyski wymienne oraz płyty CD/DVD.

  Dostęp urządzenia możesz skonfigurować w następujący sposób:

  - Zezwól – .
  - Blokuj – .
  - Zgodnie z regułami (tylko drukarki i urządzenia przenośne) – .
  - W zależności od magistrali połączenia (z wyłączeniem Wi-Fi) – .
  - Blokuj z wyjątkami (Tylko Wi-Fi) – .

- **Magistrala połączeń**. *Magistrala połączeń* to interfejs używany do podłączania urządzeń do komputera (na przykład: USB lub FireWire). Jeśli tryb **W zależności od magistrali połączenia** jest wybrany dla typu urządzenia, aplikacja zezwala lub odmawia dostępu do urządzenia w zależności od interfejsu połączenia (np. USB).

Dostęp urządzenia możesz skonfigurować w następujący sposób:

- Zezwól – ✓.
- Blokuj – ⊘.

- **Zaufane urządzenia**. *Zaufane urządzenia* są urządzeniami, do których użytkownicy, określeni w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

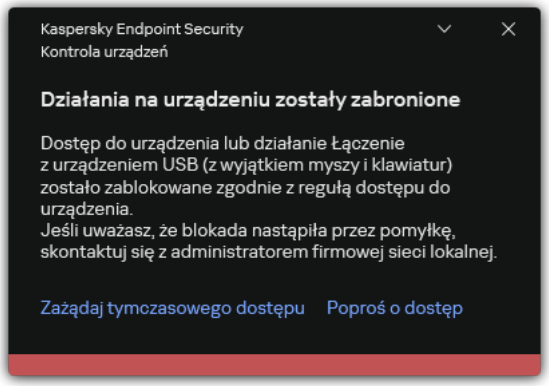
  Możesz dodać zaufane urządzenia w oparciu o następujące dane:

  - **Urządzenia według ID**. Każde urządzenie posiada unikatowy identyfikator (identyfikator sprzętu lub HWID). Możesz sprawdzić identyfikator we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Przykładowy identyfikator urządzenia: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Dodawanie urządzeń według identyfikatora jest wygodne, jeśli chcesz dodać kilka określonych urządzeń.
  - **Urządzenia według modelu**. Każde urządzenie posiada identyfikator producenta (VID) oraz identyfikator produktu (PID). Możesz sprawdzić identyfikatory we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Szablon do wprowadzenia VID i PID: `VID_1234&PID_5678`. Dodawanie urządzeń według modelu jest wygodne, jeśli w swojej organizacji używasz urządzeń pewnego modelu. W ten sposób możesz dodać wszystkie urządzenia tego modelu.
  - **Urządzenia według maski ID**. Jeśli używasz kilku urządzeń z podobnymi identyfikatorami, możesz dodać urządzenia do listy zaufanych, korzystając z maski. Znak `*` zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku `?` podczas wprowadzania maski. Na przykład, `WDC_C*`.
  - **Urządzenia według maski modelu**. Jeśli używasz kilku urządzeń z podobnymi numerami VID lub PID (na przykład, urządzeń od tego samego producenta), możesz dodać urządzenia do listy zaufanych przy użyciu masek. Znak `*` zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku `?` podczas wprowadzania maski. Na przykład, `VID_05AC&PID_*`.

Kontrola urządzeń reguluje dostęp użytkownika do urządzeń przy użyciu *reguł dostępu*. Kontrola urządzeń umożliwia także zapisywanie zdarzeń podłączenia/odłączenia urządzenia. Aby zapisać zdarzenia, musisz skonfigurować rejestrację zdarzeń w profilu.

Jeśli dostęp do urządzenia zależy od magistrali połączenia (stan ◔), Kaspersky Endpoint Security nie zapisuje zdarzeń podłączenia/odłączenia urządzenia. Aby umożliwić Kaspersky Endpoint Security zapisywanie zdarzeń podłączenia/odłączenia urządzenia, zezwól na dostęp do odpowiedniego typu urządzenia (stan ✓) lub dodaj urządzenie do listy zaufanych.

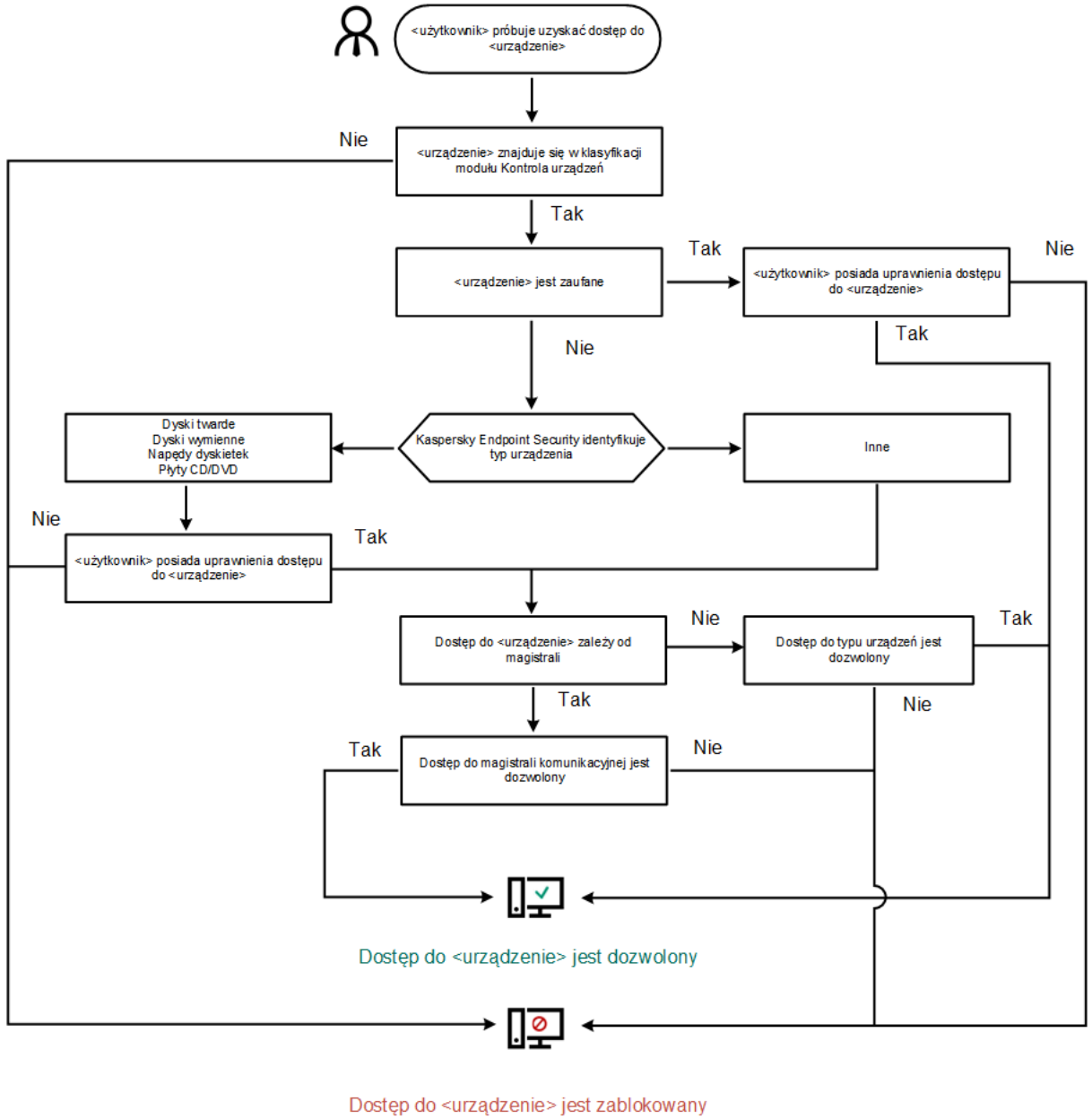
Jeśli urządzenie, które jest zablokowane przez Kontrolę urządzeń, zostanie podłączone do komputera, Kaspersky Endpoint Security zablokuje dostęp i wyświetli komunikat (patrz rysunek poniżej).



Komunikat Kontroli urządzeń

Algorytm działania Kontroli urządzeń

Kaspersky Endpoint Security podejmuje decyzję dotyczącą zezwolenia na dostęp do urządzenia po podłączeniu urządzenia do komputera przez użytkownika (patrz rysunek poniżej).



Algorytm działania Kontroli urządzeń

Jeśli urządzenie jest podłączone i dostęp jest dozwolony, możesz edytować regułę dostępu i zablokować dostęp. W tym przypadku, kolejnym razem, gdy ktoś spróbuje uzyskać dostęp do urządzenia (np. przejrzeć drzewo folderów lub wykonać operacje odczytu lub zapisu), Kaspersky Endpoint Security zablokuje dostęp. Urządzenie bez systemu plików jest blokowane dopiero przy następnym podłączeniu.

Jeśli użytkownik komputera, na którym jest zainstalowany program Kaspersky Endpoint Security, poprosi o dostęp do urządzenia, które uważa, że zostało zablokowane przez pomyłkę, wyślij do użytkownika instrukcje wysyłania pliku żądania dostępu.

Informacje o regułach dostępu

Reguła dostępu do urządzenia to grupa ustawień, które określają, którzy użytkownicy mogą uzyskać dostęp do urządzeń zainstalowanych na lub podłączonych do komputera. Te ustawienia obejmują dostęp do określonego urządzenia, dostęp do terminarza oraz uprawnienia odczytu i zapisu. Nie możesz dodać urządzenia, które znajduje się poza klasyfikacją Kontroli urządzeń. Dostęp do takich urządzeń jest dozwolony dla wszystkich użytkowników.

Reguły dostępu do urządzenia

Grupa ustawień dla reguły dostępu różni się w zależności od typu urządzenia (patrz tabela poniżej).

Ustawienia reguły dostępu

Urządzenia	Kontrola dostępu	Terminarz dostępu do urządzenia	Przydzielanie użytkowników i/lub grup użytkowników	Priorytet	Uprawnienie do odczytu/zapisu
Dyski twarde	✓	✓	✓	✓	✓
Dyski wymienne (w tym dyski flash USB)	✓	✓	✓	✓	✓
Napędy dyskietek	✓	✓	✓	✓	✓
Płyty CD/DVD	✓	✓	✓	✓	✓
Urządzenia przenośne (MTP)	✓	✓	✓	✓	✓
Drukarki lokalne	✓	–	✓	✓	–
Drukarki sieciowe	✓	–	✓	✓	–
Modemy	✓	–	–	–	–
Urządzenia taśmowe	✓	–	–	–	–
Urządzenia wielofunkcyjne	✓	–	–	–	–
Czytniki kart inteligentnych	✓	–	–	–	–
Urządzenia Windows CE USB ActiveSync	✓	–	–	–	–
Zewnętrzne karty sieciowe	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Aparaty fotograficzne i skanery	✓	–	–	–	–

Reguły dostępu dla sieci Wi-Fi

Reguła dostępu do sieci Wi-Fi określa, czy użycie sieci Wi-Fi jest dozwolone (stan ✓) lub zabronione (stan ⊘). Możesz dodać *zaufaną sieć Wi-Fi* (stan) do reguły. Użycie zaufanej sieci Wi-Fi jest dozwolone bez ograniczeń. Domyślnie, reguła dostępu do sieci Wi-Fi zezwala na dostęp do dowolnej sieci Wi-Fi.

Reguły dostępu do magistrali połączeń

Jeśli wartość **W zależności od magistrali połączenia** jest wybrana dla reguły dostępu według typu urządzenia, aplikacja zezwala lub odmawia dostępu do urządzenia w zależności od interfejsu połączenia. Reguły zezwalające na dostęp do magistral domyślnie są tworzone dla wszystkich magistral połączeń, które znajdują się w klasyfikacji modułu Kontrola urządzeń.

Reguły dostępu do magistrali połączeń określają, czy podłączenie urządzeń jest dozwolone (stan ✓) lub zabronione (stan ⊘). Priorytet reguł dostępu do typu urządzenia jest wyższy niż priorytet reguł dostępu do magistrali połączeń.

Klawiatury i myszy nie można zablokować za pomocą modułu Kontrola urządzeń. Jeśli zabronisz dostępu do magistrali połączenia USB, użytkownik będzie kontynuował pracę z klawiaturą i myszą podłączoną przez USB. Komponent Ochrona przed atakami BadUSB została zaprojektowana do zapobiegania podłączeniu do komputera zainfekowanych urządzeń USB imitujących klawiaturę.

Zarządzanie dostępem do urządzeń według typu

Kontrola urządzeń umożliwia zarządzanie dostępem do urządzeń według typu. Typ urządzenia jest ustalany przez system operacyjny w momencie podłączenia urządzenia. Typ urządzenia możesz sprawdzić za pomocą narzędzia Menedżer urządzeń wbudowanego w system operacyjny. Aby zarządzać dostępem do urządzeń, należy skonfigurować reguły. *Reguła dostępu do urządzenia* to grupa ustawień, które określają, którzy użytkownicy mogą uzyskać dostęp do urządzeń zainstalowanych na lub podłączonych do komputera. Te ustawienia obejmują dostęp do określonego urządzenia, dostęp do terminarza oraz uprawnienia odczytu i zapisu. Nie możesz dodać urządzenia, które znajduje się poza klasyfikacją Kontroli urządzeń. Dostęp do takich urządzeń jest dozwolony dla wszystkich użytkowników.

Domyślnie Kontrola urządzeń umożliwia wszystkim użytkownikom dostęp do wszystkich urządzeń.

Dostęp do urządzeń można skonfigurować w następujący sposób:

- **Zezwól**.

  Kaspersky Endpoint Security przyznaje wszystkim użytkownikom pełny dostęp do urządzeń.

- **Zablokuj**.

  Kaspersky Endpoint Security blokuje połączenia z urządzeniami. Aplikacja pozwala połączyć tylko zaufane urządzenia.

- **W zależności od magistrali połączenia**.

  Kaspersky Endpoint Security określa interfejs połączenia urządzeń i ogranicza dostęp do urządzeń zgodnie ze stanem ich połączenia z magistralą. Aplikacja pozwala również połączyć zaufane urządzenia.

- **Zgodnie z regułami**.

  W przypadku niektórych typów urządzeń możesz wyznaczyć poszczególnych użytkowników lub grupy użytkowników, którzy będą mogli korzystać z urządzeń, skonfigurować harmonogram dostępu do urządzeń oraz skonfigurować uprawnienia odczytu i zapisu. Aplikacja pozwala również połączyć zaufane urządzenia.

Należy zachować ostrożność podczas konfigurowania dostępu do urządzeń typu **Dyski twarde**. Jeśli zablokujesz dostęp do dysku systemowego, aplikacja może spowodować awarię (BSOD) podczas uruchamiania systemu operacyjnego.

Jeśli urządzenie nie pasuje do schematu klasyfikacji Kontroli urządzeń, dostępu do takiego urządzenia nie można ograniczyć.

Jak zarządzać dostępem do urządzeń według typu w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
5. W menu **Ustawienia Kontroli urządzeń**, Wybierz zakładkę **Typy urządzeń**.

   W zakładce **Typy urządzeń** wyświetlą się reguły dostępu dla wszystkich urządzeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.
6. Skonfiguruj reguły dostępu dla urządzeń:

   a. Wybierz tryb dostępu: **Zezwól**, **Blokuj**, **W zależności od magistrali połączenia**, **Zgodnie z regułami**.

   W celu wybrania trybu dostępu **Zgodnie z regułami** kliknij dwukrotnie, aby otworzyć właściwości reguły dostępu.

   b. Jeśli wybierzesz tryb dostępu **W zależności od magistrali połączenia**, należy skonfigurować reguły dostępu dla interfejsów połączeń w zakładce **Magistrale**.

   c. W przypadku urządzeń pamięci masowej (na przykład nośników wymiennych) można skonfigurować uprawnienia dostępu dla poszczególnych użytkowników. Można także ustalić harmonogram dostępu do urządzeń oraz skonfigurować uprawnienia odczytu i zapisu.

   Możesz dodać te urządzenia do listy zaufanych. *Zaufane urządzenia* są urządzeniami, do których użytkownicy, określeni w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

   d. W razie potrzeby skonfiguruj reguły drukowania.

   e. W razie potrzeby skonfiguruj reguły dostępu do urządzenia Bluetooth.

   f. W razie potrzeby skonfiguruj reguły połączenia komputera z Wi-Fi.
7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak zarządzać dostępem do urządzeń według typu w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
5. W menu **Reguły dostępu do urządzenia**, Wybierz zakładkę **Urządzenia i sieci Wi-Fi**.

   Tabela zawiera reguły dostępu do wszystkich urządzeń, które są obecne w klasyfikacji komponentu Kontrola urządzeń.
6. Skonfiguruj reguły dostępu dla urządzeń:

   a. Wybierz tryb dostępu: **Zezwól**, **Zablokuj**, **W zależności od magistrali**, **Niestandardowe**.

   Jeśli w menu rozwijanym brakuje trybu dostępu, otwórz właściwości reguły dostępu, klikając dwukrotnie typ urządzenia.

   b. Jeśli wybierzesz tryb dostępu **W zależności od magistrali**, należy skonfigurować reguły dostępu dla interfejsów połączeń w zakładce **Magistrale**.

   c. W przypadku urządzeń pamięci masowej (na przykład nośników wymiennych) można skonfigurować uprawnienia dostępu dla poszczególnych użytkowników. Można także ustalić harmonogram dostępu do urządzeń oraz skonfigurować uprawnienia odczytu i zapisu.

   Możesz dodać te urządzenia do listy zaufanych. *Zaufane urządzenia* są urządzeniami, do których użytkownicy, określeni w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

   d. W razie potrzeby skonfiguruj reguły drukowania.

   e. W razie potrzeby skonfiguruj reguły dostępu do urządzenia Bluetooth.

   f. W razie potrzeby skonfiguruj reguły połączenia komputera z Wi-Fi.
7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak zarządzać dostępem do urządzeń w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij odnośnik **Urządzenia i sieci Wi-Fi**.

   Tabela zawiera reguły dostępu do wszystkich urządzeń, które są obecne w klasyfikacji komponentu Kontrola urządzeń.
4. Skonfiguruj reguły dostępu dla urządzeń:

   a. Wybierz tryb dostępu: **Zezwól**, **Zablokuj**, **W zależności od magistrali połączenia**, **Zgodnie z regułami**.

   Jeśli w menu rozwijanym brakuje trybu dostępu, otwórz właściwości reguły dostępu, klikając dwukrotnie typ urządzenia.

b. Jeśli wybierzesz tryb dostępu **W zależności od magistrali połączenia**, należy skonfigurować reguły dostępu dla interfejsów połączeń w zakładce **Magistrale**.

c. W przypadku urządzeń pamięci masowej (na przykład nośników wymiennych) można skonfigurować uprawnienia dostępu dla poszczególnych użytkowników. Można także ustalić harmonogram dostępu do urządzeń oraz skonfigurować uprawnienia odczytu i zapisu.

Możesz dodać te urządzenia do listy zaufanych. *Zaufane urządzenia* są urządzeniami, do których użytkownicy, określeni w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

d. W razie potrzeby skonfiguruj reguły drukowania.

e. W razie potrzeby skonfiguruj reguły dostępu do urządzenia Bluetooth.

f. W razie potrzeby skonfiguruj reguły połączenia komputera z Wi-Fi.

5. Zapisz swoje zmiany.

W wyniku tego działania, gdy użytkownik spróbuje uzyskać dostęp do urządzenia, aplikacja zablokuje dostęp zgodnie z regułami. Kaspersky Endpoint Security zarejestruje również odpowiednie zdarzenie. Jeśli chcesz przyznać dostęp poszczególnym urządzeniom, dodaj te urządzenia do listy zaufanych urządzeń.

Zarządzanie dostępem do urządzeń za pomocą magistrali połączeniowej

W celu zmodyfikowania reguły dostępu do magistrali połączeń:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij przycisk **Magistrale**.

   Otwarte okno wyświetla reguły dostępu dla wszystkich magistral połączeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.
4. Wybierz regułę dostępu, którą chcesz zmienić.
5. W kolumnie **Dostęp** wybierz, czy chcesz zezwolić na dostęp do magistrali połączeń: **Zezwól** lub **Zablokuj**.

   Jeśli zmieniono dostęp do magistrali połączeń **Port szeregowy** (COM) lub **Port równoległy** (LPT), musisz ponownie uruchomić komputer, aby aktywować regułę dostępu.
6. Zapisz swoje zmiany.

Różnicowanie praw dostępu użytkowników do urządzeń

Możesz skonfigurować prawa dostępu użytkowników do zaufanych urządzeń lub według typu urządzenia.

Różnicowanie praw dostępu użytkownika według typu urządzenia

Kontrola urządzeń umożliwia konfigurację praw dostępu użytkownika do *urządzeń pamięci masowej*. W przypadku takich urządzeń można skonfigurować uprawnienia zapisu i odczytu. Kontrola urządzeń obsługuje następujące typy *urządzeń pamięci masowej*:

- Dyski twarde.
- Dyski wymienne (w tym dyski flash USB).
- Napędy dyskietek.
- Płyty CD/DVD.
- Urządzenia przenośne (MTP). Urządzenia przenośne (MTP) obejmują na przykład urządzenia mobilne, aparaty fotograficzne, odtwarzacze multimedialne itp.

W ten sposób możesz np. zezwolić na korzystanie z nośników wymiennych tylko grupie administratorów. W przypadku innych typów urządzeń możesz zezwolić lub odmówić dostępu wszystkim użytkownikom. Możesz także skonfigurować prawa dostępu użytkownika do korzystania z drukarek.

Jak skonfigurować prawa dostępu użytkownika do danych na urządzeniach pamięci masowej w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
5. W menu **Ustawienia Kontroli urządzeń**, Wybierz zakładkę **Typy urządzeń**.

   W zakładce **Typy urządzeń** wyświetlą się reguły dostępu dla wszystkich urządzeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.
6. Aby skonfigurować reguły dostępu do urządzenia pamięci masowej, kliknij dwukrotnie, aby otworzyć listę reguł.
7. Skonfiguruj regułę dostępu do urządzenia pamięci masowej:

   a. W sekcji **Reguły dostępu** kliknij przycisk **Dodaj**.

      Spowoduje to otwarcie okna dodania nowej reguły dostępu do urządzenia pamięci masowej.

   b. W polu **Priorytet reguły** ustaw priorytet *zapisu reguły*. Reguła zawiera następujące atrybuty: konto użytkownika, terminarz, uprawnienia (zezwól/zablokuj) i priorytet.

      Reguła posiada określony priorytet. Jeśli użytkownik został dodany do kilku grup, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o regułę z najwyższym priorytetem. Kaspersky Endpoint Security umożliwia użytkownikowi przypisanie priorytetu od 0 do 10 000. Im większa wartość, tym większy priorytet. Innymi słowy, wpis z wartością 0 posiada najniższy priorytet.

      Na przykład, możesz nadać uprawnienia tylko do odczytu grupie Każdy oraz nadać uprawnienia do odczytu/zapisu grupie administracyjnej. Aby to zrobić, przypisz priorytet 1 dla grupy administratorów oraz przypisz priorytet 0 dla grupy Każdy.

Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Innymi słowy, jeśli użytkownik został dodany do kilku grup, a priorytet wszystkich reguł jest taki sam, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o dowolną istniejącą regułę blokowania.

c. W menu **Reguła dla użytkowników i grup**, wybierz użytkowników lub grupy użytkowników. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

d. Kliknij **OK**.

8. W menu **Terminarze dla wybranej reguły dostępu** skonfiguruj terminarz dostępu do urządzenia pamięci masowej dla użytkowników.

   Możesz na przykład zezwolić użytkownikom na korzystanie z urządzeń pamięci masowej tylko w godzinach pracy.

9. Skonfiguruj uprawnienia dostępu użytkowników do urządzeń pamięci masowej w menedżerze plików (**Odczyt** / **Zapisz**).

10. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak skonfigurować prawa dostępu użytkowników do danych na urządzeniach pamięci masowej w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.

5. W sekcji **Reguły dostępu do urządzenia**, w tabeli reguł dostępu, otwórz właściwości reguł dostępu dla urządzeń pamięci masowej.

6. W bloku **Reguły dostępu do urządzenia** wybierz **Niestandardowe**.

7. Skonfiguruj regułę dostępu do urządzenia pamięci masowej:

   a. W sekcji **Użytkownicy i ich uprawnienia** kliknij przycisk **Dodaj**.

   Spowoduje to otwarcie okna dodania nowej reguły dostępu do urządzenia pamięci masowej.

   b. W polu **Priorytet** ustaw priorytet *zapisu reguły*. Reguła zawiera następujące atrybuty: konto użytkownika, terminarz, uprawnienia (zezwól/zablokuj) i priorytet.

   Reguła posiada określony priorytet. Jeśli użytkownik został dodany do kilku grup, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o regułę z najwyższym priorytetem. Kaspersky Endpoint Security umożliwia użytkownikowi przypisanie priorytetu od 0 do 10 000. Im większa wartość, tym większy priorytet. Innymi słowy, wpis z wartością 0 posiada najniższy priorytet.

   Na przykład, możesz nadać uprawnienia tylko do odczytu grupie Każdy oraz nadać uprawnienia do odczytu/zapisu grupie administracyjnej. Aby to zrobić, przypisz priorytet 1 dla grupy administratorów oraz przypisz priorytet 0 dla grupy Każdy.

   Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Innymi słowy, jeśli użytkownik został dodany do kilku grup, a priorytet wszystkich reguł jest taki sam, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o dowolną istniejącą regułę blokowania.

c. W menu **Użytkownik lub grupa**, wybierz użytkowników lub grupy użytkowników. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

d. W menu **Terminarz dostępu** skonfiguruj terminarz dostępu do urządzenia pamięci masowej dla użytkowników.

Możesz na przykład zezwolić użytkownikom na korzystanie z urządzeń pamięci masowej tylko w godzinach pracy.

e. Skonfiguruj uprawnienia dostępu użytkowników do urządzeń pamięci masowej w menedżerze plików (**Odczyt / Zapis**).

f. Kliknij **Zapisz**.

8. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak skonfigurować prawa dostępu użytkownika do danych na urządzeniach pamięci masowej w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń → Kontrola urządzeń**.

3. W sekcji **Ustawienia dostępu** kliknij odnośnik **Urządzenia i sieci Wi-Fi**.

Tabela zawiera reguły dostępu do wszystkich urządzeń, które są obecne w klasyfikacji komponentu Kontrola urządzeń.

4. Aby skonfigurować reguły dostępu do urządzenia pamięci masowej, kliknij prawym przyciskiem myszy, aby otworzyć listę reguł.

5. Skonfiguruj regułę dostępu do urządzenia pamięci masowej:

a. W sekcji **Uprawnienia użytkowników** kliknij przycisk **Dodaj**.

Spowoduje to otwarcie okna dodania nowej reguły dostępu do urządzenia pamięci masowej.

b. W polu **Priorytet** ustaw priorytet *zapisu reguły*. Reguła zawiera następujące atrybuty: konto użytkownika, terminarz, uprawnienia (zezwól/zablokuj) i priorytet.

Reguła posiada określony priorytet. Jeśli użytkownik został dodany do kilku grup, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o regułę z najwyższym priorytetem. Kaspersky Endpoint Security umożliwia użytkownikowi przypisanie priorytetu od 0 do 10 000. Im większa wartość, tym większy priorytet. Innymi słowy, wpis z wartością 0 posiada najniższy priorytet.

Na przykład, możesz nadać uprawnienia tylko do odczytu grupie Każdy oraz nadać uprawnienia do odczytu/zapisu grupie administracyjnej. Aby to zrobić, przypisz priorytet 1 dla grupy administratorów oraz przypisz priorytet 0 dla grupy Każdy.

Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Innymi słowy, jeśli użytkownik został dodany do kilku grup, a priorytet wszystkich reguł jest taki sam, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o dowolną istniejącą regułę blokowania.

c. W menu **Użytkownicy**, wybierz użytkowników lub grupy użytkowników. Możesz wybrać użytkowników w grupie Active Directory lub ręcznie wprowadzić lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

d. Kliknij **OK**.

6. W menu **Terminarz dostępu do urządzeń** skonfiguruj terminarz dostępu do urządzenia pamięci masowej dla użytkowników.

   Możesz na przykład zezwolić użytkownikom na korzystanie z urządzeń pamięci masowej tylko w godzinach pracy.

7. Skonfiguruj uprawnienia dostępu użytkowników do urządzeń pamięci masowej w menedżerze plików (**Odczyt** / **Zapis**).

8. Zapisz swoje zmiany.

Różnicowanie praw dostępu użytkowników do zaufanych urządzeń

Zaufane urządzenia są urządzeniami, do których użytkownicy, określeni w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu. Aby pracować z zaufanymi urządzeniami, możesz przyznać dostęp do pojedynczego użytkownika, grupy użytkowników lub wszystkich użytkowników organizacji. Możesz skonfigurować prawa dostępu użytkownika we właściwościach zaufanego urządzenia.

Zarządzanie dostępem do urządzeń mobilnych

Kaspersky Endpoint Security umożliwia kontrolę dostępu do danych na urządzeniach mobilnych z systemami Android i iOS. Urządzenia mobilne należą do kategorii urządzeń przenośnych (MTP). Dlatego, aby skonfigurować dostęp do danych na urządzeniach mobilnych, należy edytować ustawienia dostępu dla urządzeń przenośnych (MTP).

Jeśli urządzenie mobilne jest podłączone do komputera, system operacyjny określa typ urządzenia. Jeśli na komputerze są zainstalowane aplikacje Android Debug Bridge (ADB), iTunes lub ich odpowiedniki, system operacyjny identyfikuje urządzenia mobilne jako urządzenia ADB lub iTunes. We wszystkich pozostałych przypadkach system operacyjny może zidentyfikować typ urządzenia mobilnego jako urządzenie przenośne (MTP) dla transferu plików, urządzenie PTP (kamera) dla transferu obrazów lub inne urządzenie. Typ urządzenia zależy od modelu urządzenia mobilnego i wybranego trybu połączenia USB. Kaspersky Endpoint Security umożliwia konfigurowanie indywidualnych uprawnień dostępu do danych na urządzeniach mobilnych w aplikacjach ADB, iTunes lub menedżerze plików. We wszystkich innych przypadkach Kontrola urządzeń umożliwia dostęp do urządzeń mobilnych zgodnie z regułami dostępu do urządzeń przenośnych (MTP).

Dostęp do urządzeń mobilnych

Urządzenia mobilne należą do kategorii urządzeń przenośnych (MTP), dlatego ich ustawienia są takie same. Możesz wybrać jeden z poniższych trybów dostępu do urządzeń mobilnych:

- **Zezwól** ✓. Kaspersky Endpoint Security umożliwia pełny dostęp do urządzeń mobilnych. Możesz otwierać, tworzyć, modyfikować, kopiować lub usuwać pliki na urządzeniach mobilnych za pomocą menedżera plików lub aplikacji ADB i iTunes. Baterię urządzenia można również naładować podłączając urządzenie mobilne do portu USB komputera.

- **Blokuj** ⊘. Kaspersky Endpoint Security ogranicza dostęp do urządzeń mobilnych w menedżerze plików oraz aplikacjach ADB i iTunes. Aplikacja umożliwia dostęp tylko do zaufanych urządzeń mobilnych. Baterię urządzenia można również naładować podłączając urządzenie mobilne do portu USB komputera.

- **W zależności od magistrali połączenia**. Kaspersky Endpoint Security umożliwia łączenie się z urządzeniami mobilnymi zgodnie ze stanem połączenia USB (**Zezwól** lub **Blokuj**).

- **Zgodnie z regułami**. Kaspersky Endpoint Security ogranicza dostęp do urządzeń mobilnych zgodnie z regułami. W regułach możesz skonfigurować uprawnienia dostępu (odczyt/zapis), wybrać użytkowników lub grupę użytkowników, którzy mogą mieć dostęp do urządzeń mobilnych, oraz skonfigurować terminarz dostępu dla urządzeń mobilnych. Możesz także ograniczyć dostęp do danych na urządzeniach mobilnych poprzez aplikacje ADB i iTunes.

Konfigurowanie reguł dostępu do urządzeń mobilnych

Reguły dostępu dla urządzeń przenośnych (MTP), urządzeń ADB i urządzeń iTunes są konfigurowane w inny sposób. W przypadku urządzeń przenośnych (MTP) i urządzeń ADB można skonfigurować reguły dla poszczególnych użytkowników lub grup użytkowników oraz utworzyć terminarz obowiązywania reguł. W przypadku urządzeń iTunes nie można tego zrobić. Możesz zezwolić lub odmówić dostępu do danych tylko za pośrednictwem aplikacji iTunes dla wszystkich użytkowników.

Jak skonfigurować reguły dostępu do urządzeń mobilnych w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
4. W menu **Ustawienia Kontroli urządzeń**, Wybierz zakładkę **Typy urządzeń**.

   Tabela zawiera reguły dostępu do wszystkich urządzeń, które są obecne w klasyfikacji komponentu Kontrola urządzeń.
5. W menu kontekstowym typu urządzenia **Urządzenia przenośne (MTP)**, skonfiguruj tryb dostępu do urządzenia mobilnego: **Zezwól**, **Blokuj**, lub **W zależności od magistrali połączenia**.
6. Aby skonfigurować reguły dostępu do urządzenia mobilnego, kliknij dwukrotnie, aby otworzyć listę reguł.
7. Skonfiguruj regułę dostępu do urządzenia mobilnego:

   a. W sekcji **Reguły dostępu** kliknij przycisk **Dodaj**.

      Spowoduje to otwarcie okna dodania nowej reguły dostępu do urządzenia mobilnego.

   b. W polu **Priorytet** ustaw priorytet zapisu reguły. Reguła zawiera następujące atrybuty: konto użytkownika, terminarz, uprawnienia (odczyt / zapis / dostęp ADB) i priorytet.

      Reguła posiada określony priorytet. Jeśli użytkownik został dodany do kilku grup, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o regułę z najwyższym priorytetem. Kaspersky Endpoint Security umożliwia użytkownikowi przypisanie priorytetu od 0 do 10 000. Im większa wartość, tym większy priorytet. Innymi słowy, wpis z wartością 0 posiada najniższy priorytet.

      Na przykład, możesz nadać uprawnienia tylko do odczytu grupie Każdy oraz nadać uprawnienia do odczytu/zapisu grupie administracyjnej. Aby to zrobić, przypisz priorytet 1 dla grupy administratorów oraz przypisz priorytet 0 dla grupy Każdy.

      Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Innymi słowy, jeśli użytkownik został dodany do kilku grup, a priorytet wszystkich reguł jest taki sam, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o dowolną istniejącą regułę blokowania.

c. W menu **Reguła dla użytkowników i grup**, wybierz użytkowników lub grupy użytkowników. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

d. Kliknij **OK**.

8. W menu **Terminarze dla wybranej reguły dostępu**, skonfiguruj terminarz dostępu do urządzenia dla użytkowników.

Skonfigurowanie osobnego harmonogramu dostępu do urządzeń ADB nie jest możliwe. Możesz skonfigurować wspólny harmonogram dostępu do urządzeń ADB i urządzeń przenośnych (MTP).

9. Skonfiguruj uprawnienia dostępu użytkowników do urządzeń mobilnych w menedżerze plików (**Odczyt**/**Zapis**).

10. Skonfiguruj dostęp do danych na urządzeniu mobilnym poprzez aplikację ADB za pomocą pola wyboru **Dostęp przez ADB**.

Jeśli pole wyboru nie jest zaznaczone, gdy urządzenie mobilne jest podłączone, aplikacja ADB nie może wykryć urządzenia.

11. W obszarze **Dostęp przez iTunes** skonfiguruj dostęp do danych na urządzeniu mobilnym poprzez aplikację iTunes.

Kaspersky Endpoint Security stosuje ustawienia dostępu do urządzenia mobilnego za pośrednictwem aplikacji iTunes dla wszystkich użytkowników. Skonfigurowanie osobnego harmonogramu dostępu do urządzeń iTunes nie jest możliwe.

12. Zapisz swoje zmiany.

W jaki sposób skonfigurować reguły dostępu do urządzeń mobilnych w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.

5. W sekcji **Reguły dostępu do urządzenia** kliknij odnośnik **Urządzenia i sieci Wi-Fi**.

Tabela zawiera reguły dostępu do wszystkich urządzeń, które są obecne w klasyfikacji komponentu Kontrola urządzeń.

6. Wybierz typ urządzenia **Urządzenia przenośne (MTP)**.

Spowoduje to otwarcie praw dostępu do urządzeń przenośnych (MTP).

7. Skonfiguruj tryb dostępu do urządzeń mobilnych: **Zezwól**, **Zablokuj**, **W zależności od magistrali** lub **Niestandardowe**.

8. Za pomocą przełącznika **Dostęp przez iTunes dla wszystkich użytkowników WŁĄCZONY** skonfiguruj dostęp do danych na urządzeniu mobilnym poprzez aplikację iTunes.

   Kaspersky Endpoint Security stosuje ustawienia dostępu do urządzenia mobilnego za pośrednictwem aplikacji iTunes dla wszystkich użytkowników. Skonfigurowanie osobnego harmonogramu dostępu do urządzeń iTunes nie jest możliwe.

9. Jeśli wybierzesz tryb **Niestandardowe**, należy dodać reguły drukowania na drukarkach. Aby to zrobić, w menu **Użytkownicy i ich uprawnienia** kliknij przycisk **Dodaj** i skonfiguruj regułę dostępu do urządzenia mobilnego:

   a. W polu **Priorytet** ustaw priorytet zapisu reguły. Reguła zawiera następujące atrybuty: konto użytkownika, terminarz, uprawnienia (odczyt / zapis / dostęp ADB) i priorytet.

      Reguła posiada określony priorytet. Jeśli użytkownik został dodany do kilku grup, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o regułę z najwyższym priorytetem. Kaspersky Endpoint Security umożliwia użytkownikowi przypisanie priorytetu od 0 do 10 000. Im większa wartość, tym większy priorytet. Innymi słowy, wpis z wartością 0 posiada najniższy priorytet.

      Na przykład, możesz nadać uprawnienia tylko do odczytu grupie Każdy oraz nadać uprawnienia do odczytu/zapisu grupie administracyjnej. Aby to zrobić, przypisz priorytet 1 dla grupy administratorów oraz przypisz priorytet 0 dla grupy Każdy.

      Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Innymi słowy, jeśli użytkownik został dodany do kilku grup, a priorytet wszystkich reguł jest taki sam, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o dowolną istniejącą regułę blokowania.

   b. W menu **Użytkownik lub grupa** wybierz użytkowników lub grupy użytkowników, aby umożliwić dostęp do urządzeń mobilnych. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

   c. W menu **Terminarz dostępu**, skonfiguruj terminarz dostępu do urządzenia dla użytkowników.

      Skonfigurowanie osobnego harmonogramu dostępu do urządzeń ADB nie jest możliwe. Możesz skonfigurować wspólny harmonogram dostępu do urządzeń ADB i urządzeń przenośnych (MTP).

   d. Skonfiguruj uprawnienia dostępu użytkowników do urządzeń mobilnych w menedżerze plików (**Odczyt**/**Zapis**).

   e. Skonfiguruj dostęp do danych na urządzeniu mobilnym poprzez aplikację ADB za pomocą pola wyboru **Dostęp przez ADB**.

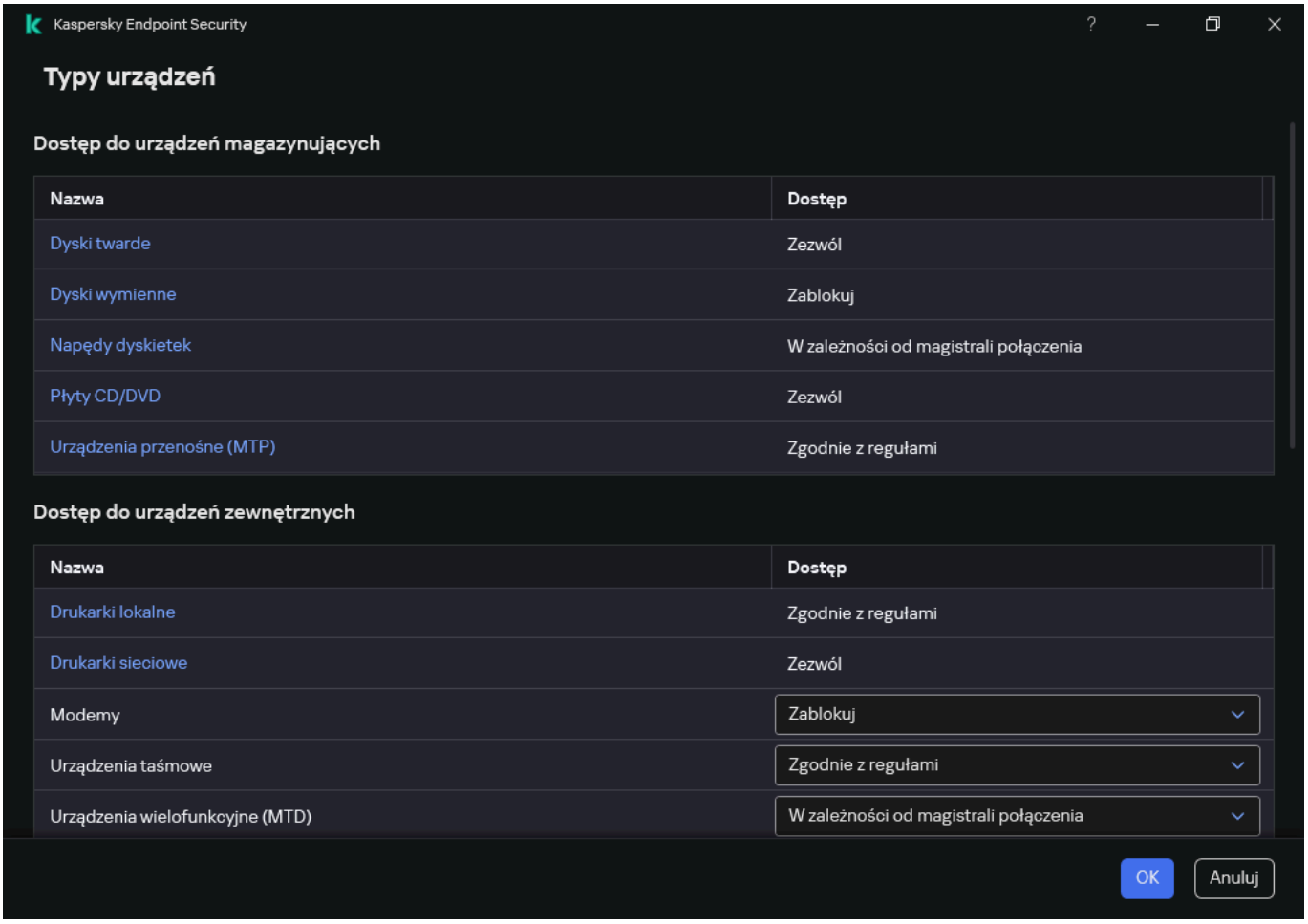
      Jeśli pole wyboru nie jest zaznaczone, gdy urządzenie mobilne jest podłączone, aplikacja ADB nie może wykryć urządzenia.

10. Zapisz swoje zmiany.

Jak skonfigurować reguły dostępu do urządzeń mobilnych w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij przycisk **Urządzenia i sieci Wi-Fi**.

Otwarte okno wyświetla reguły dostępu dla wszystkich urządzeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.



Typy urządzeń w komponencie Kontrola urządzeń

4. W sekcji **Dostęp do urządzeń magazynujących** kliknij odnośnik **Urządzenia przenośne (MTP)**.

   Spowoduje to otwarcie okna zawierającego reguły dostępu do urządzeń przenośnych (MTP).

5. W menu **Dostęp**, skonfiguruj tryb dostępu do urządzeń mobilnych: **Zezwól**, **Zablokuj**, **W zależności od magistrali połączenia**, lub **Zgodnie z regułami**.

6. Jeśli wybierzesz tryb **Zgodnie z regułami**, należy dodać reguły drukowania na drukarkach:

   a. W sekcji **Uprawnienia użytkowników** kliknij przycisk **Dodaj**.

      Spowoduje to otwarcie okna dodania nowej reguły dostępu do urządzenia mobilnego.

   b. W polu **Priorytet** ustaw priorytet zapisu reguły. Reguła zawiera następujące atrybuty: konto użytkownika, terminarz, uprawnienia (odczyt / zapis / dostęp ADB) i priorytet.

      Reguła posiada określony priorytet. Jeśli użytkownik został dodany do kilku grup, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o regułę z najwyższym priorytetem. Kaspersky Endpoint Security umożliwia użytkownikowi przypisanie priorytetu od 0 do 10 000. Im większa wartość, tym większy priorytet. Innymi słowy, wpis z wartością 0 posiada najniższy priorytet.

      Na przykład, możesz nadać uprawnienia tylko do odczytu grupie Każdy oraz nadać uprawnienia do odczytu/zapisu grupie administracyjnej. Aby to zrobić, przypisz priorytet 1 dla grupy administratorów oraz przypisz priorytet 0 dla grupy Każdy.

      Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Innymi słowy, jeśli użytkownik został dodany do kilku grup, a priorytet wszystkich reguł jest taki sam, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o dowolną istniejącą regułę blokowania.

c. W menu **Stan** włącz regułę dostępu do urządzenia mobilnego.

d. W menu **Reguły dostępu** skonfiguruj uprawnienia dostępu do urządzeń mobilnych dla użytkowników.

- Skonfiguruj uprawnienia dostępu użytkowników do urządzeń mobilnych w menedżerze plików (**Odczyt**/**Zapis**).
- Skonfiguruj dostęp do danych na urządzeniu mobilnym poprzez aplikację ADB za pomocą pola wyboru **Dostęp przez ADB**.

  Jeśli pole wyboru nie jest zaznaczone, gdy urządzenie mobilne jest podłączone, aplikacja ADB nie może wykryć urządzenia.

e. W menu **Użytkownicy** wybierz użytkowników lub grupy użytkowników, aby umożliwić dostęp do urządzeń mobilnych. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

f. W menu **Terminarz dostępu do urządzeń** skonfiguruj terminarz dostępu do urządzenia dla użytkowników.

> Skonfigurowanie osobnego harmonogramu dostępu do urządzeń ADB nie jest możliwe. Możesz skonfigurować wspólny harmonogram dostępu do urządzeń ADB i urządzeń przenośnych (MTP).

g. W obszarze **Dostęp przez iTunes** skonfiguruj dostęp do danych na urządzeniu mobilnym poprzez aplikację iTunes.

> Kaspersky Endpoint Security stosuje ustawienia dostępu do urządzenia mobilnego za pośrednictwem aplikacji iTunes dla wszystkich użytkowników. Skonfigurowanie osobnego harmonogramu dostępu do urządzeń iTunes nie jest możliwe.

7. Zapisz swoje zmiany.

W rezultacie dostęp użytkowników do urządzeń mobilnych jest ograniczony zgodnie z zasadami. Jeśli zablokowano dostęp do urządzeń mobilnych w aplikacjach ADB i iTunes, po podłączeniu urządzenia mobilnego aplikacje ADB i iTunes mogą nie wykryć urządzenia mobilnego.

Zaufane urządzenia mobilne

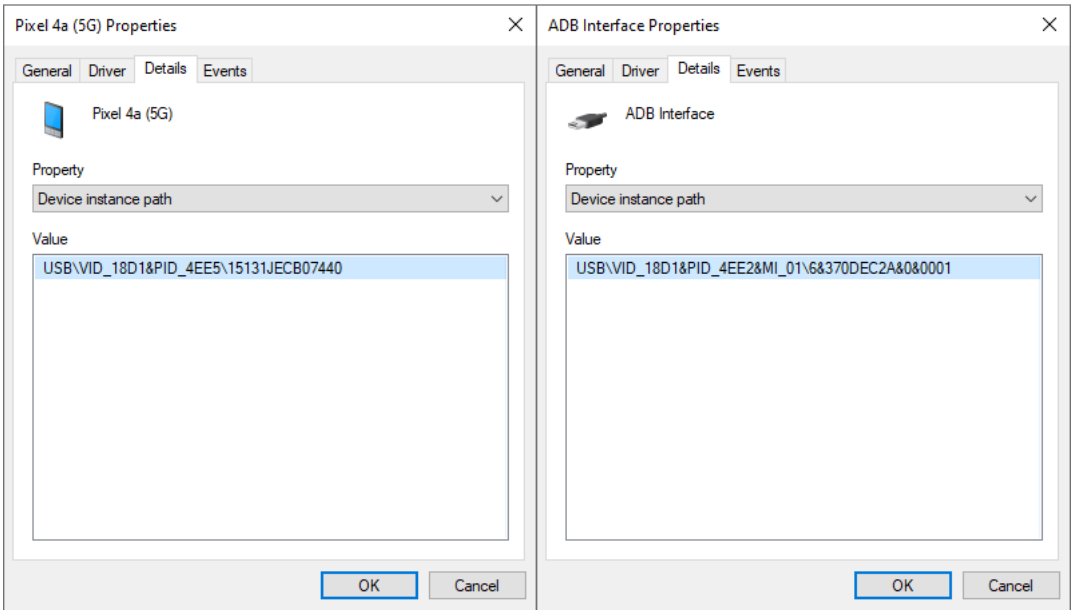
Zaufane urządzenia są urządzeniami, do których użytkownicy, określeni w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

Procedura dodawania urządzenia mobilnego jest dokładnie taka sama, jak w przypadku innych typów zaufanych urządzeń. Możesz dodać urządzenie mobilne według identyfikatora lub modelu urządzenia.

Aby dodać zaufane urządzenie mobilne za pomocą identyfikatora, będziesz potrzebować unikalnego identyfikatora (Hardware ID – HWID). Identyfikator można znaleźć we właściwościach urządzenia za pomocą narzędzi systemu operacyjnego (patrz rysunek poniżej). Można to zrobić poprzez narzędzie Menedżer urządzeń. Identyfikatory urządzeń przenośnych (MTP) i urządzeń ADB oraz iTunes są różne nawet w przypadku tego samego urządzenia mobilnego. Identyfikator urządzenia przenośnego (MTP) może wyglądać następująco: `15131JECB07440`. Identyfikator urządzenia ADB może wyglądać następująco: `6&370DEC2A&0&0001`. Dodawanie urządzeń według identyfikatora jest wygodne, jeśli chcesz dodać kilka określonych urządzeń. Możesz także użyć masek.

Jeśli zainstalowano aplikacje ADB lub iTunes po podłączeniu urządzenia do komputera, unikatowy identyfikator urządzenia może zostać zresetowany. Oznacza to, że Kaspersky Endpoint Security zidentyfikuje to urządzenie jako nowe urządzenie. Jeśli urządzenie jest zaufane, ponownie dodaj urządzenie do listy zaufanych.

Aby dodać zaufane urządzenie mobilne według modelu urządzenia, będą Ci potrzebne jego Vendor ID (VID) i Product ID (PID). Identyfikatory można znaleźć we właściwościach urządzenia za pomocą narzędzi systemu operacyjnego (patrz rysunek poniżej). Szablon do wprowadzenia VID i PID: `VID_18D1&PID_4EE5`. Dodawanie urządzeń według modelu jest wygodne, jeśli w swojej organizacji używasz urządzeń pewnego modelu. W ten sposób możesz dodać wszystkie urządzenia tego modelu.



Identyfikator urządzenia w Menedżerze urządzeń

Zarządzanie dostępem do urządzeń Bluetooth.

Kaspersky Endpoint Security umożliwia zarządzanie dostępem do urządzeń Bluetooth. Do urządzeń Bluetooth zaliczają się bezprzewodowe klawiatury, myszy, zestawy słuchawkowe, drukarki itp. Bluetootha można także używać do komunikacji np. z urządzeniem mobilnym.

Gdy urządzenia Bluetooth są podłączone lub odłączone, aplikacja może utworzyć wiele zdarzeń dotyczących urządzenia. Powodem jest to, że system operacyjny może wykryć urządzenie Bluetooth jako wiele urządzeń różnych typów. Kaspersky Endpoint Security zarządza także adapterem Bluetooth, przez który urządzenie jest podłączone jako osobne urządzenie. Dlatego aplikacja tworzy zdarzenie dla każdego z wykrytych urządzeń.

Możesz wybrać jeden z poniższych trybów dostępu do urządzeń Bluetooth:

- **Zezwól i nie zapisuj w dzienniku** . Kaspersky Endpoint Security umożliwia podłączenie dowolnych urządzeń Bluetooth i nie zapisuje informacji o połączeniu w dzienniku zdarzeń. Możesz podłączyć urządzenia wejściowe Bluetooth (klawiatury, myszy itp.), wysyłać dane przez Bluetooth, zarządzać innymi urządzeniami Bluetooth (zestawem słuchawkowym, słuchawkami itp.).

- **Zezwól** . Kaspersky Endpoint Security umożliwia podłączenie dowolnych urządzeń Bluetooth. Możesz podłączyć urządzenia wejściowe Bluetooth (klawiatury, myszy itp.), wysyłać dane przez Bluetooth, zarządzać innymi urządzeniami Bluetooth (zestawem słuchawkowym, słuchawkami itp.).

- **Blokuj** Kaspersky Endpoint Security ogranicza dostęp do urządzeń Bluetooth. Możesz zezwolić na podłączanie tylko urządzeń wejściowych Bluetooth (klasy Human Interface Devices). Urządzenia te obejmują klawiatury, myszy, joysticki itp.

Nie można utworzyć listy zaufanych urządzeń Bluetooth. Jeśli masz ograniczony dostęp do urządzeń Bluetooth, możesz podłączyć tylko urządzenia wejściowe Bluetooth.

Konfiguracja zasad dostępu do urządzeń mobilnych w Konsoli Administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
5. W menu **Ustawienia Kontroli urządzeń**, Wybierz zakładkę **Typy urządzeń**.

   Tabela zawiera reguły dostępu do wszystkich urządzeń, które są obecne w klasyfikacji komponentu Kontrola urządzeń.
6. W menu kontekstowym typu urządzenia **Bluetooth**, skonfiguruj tryb dostępu do urządzenia mobilnego: **Zezwól** , **Blokuj** , lub **Zezwól i nie zapisuj w dzienniku** .
7. Jeśli wybierzesz opcję **Blokuj** trybie można zezwolić na podłączanie tylko urządzeń wejściowych Bluetooth (klawiatury, myszy itp.). Aby to zrobić, w sekcji **Wykluczenia** wybierz pole wyboru **Urządzenia wejściowe (myszy i klawiatury)**.
8. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

W jaki sposób skonfigurować reguły dostępu do urządzeń Bluetooth w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.

5. W sekcji **Reguły dostępu do urządzenia** kliknij odnośnik **Urządzenia i sieci Wi-Fi**.

   Tabela zawiera reguły dostępu do wszystkich urządzeń, które są obecne w klasyfikacji komponentu Kontrola urządzeń.

6. Wybierz typ urządzenia **Urządzenia Bluetooth**.

   Spowoduje to otwarcie ustawień dostępu do urządzenia Bluetooth.

7. Skonfiguruj tryb dostępu do urządzenia Bluetooth: **Zezwól**, **Zablokuj**, **Zezwól i nie zapisuj w dzienniku**.

8. Jeśli wybierzesz opcję **Zablokuj** trybie można zezwolić na podłączanie tylko urządzeń wejściowych Bluetooth (klawiatury, myszy itp.). Aby to zrobić, w sekcji **Wykluczenia** wybierz pole wyboru **Urządzenia wejściowe (myszy i klawiatury)**.

9. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

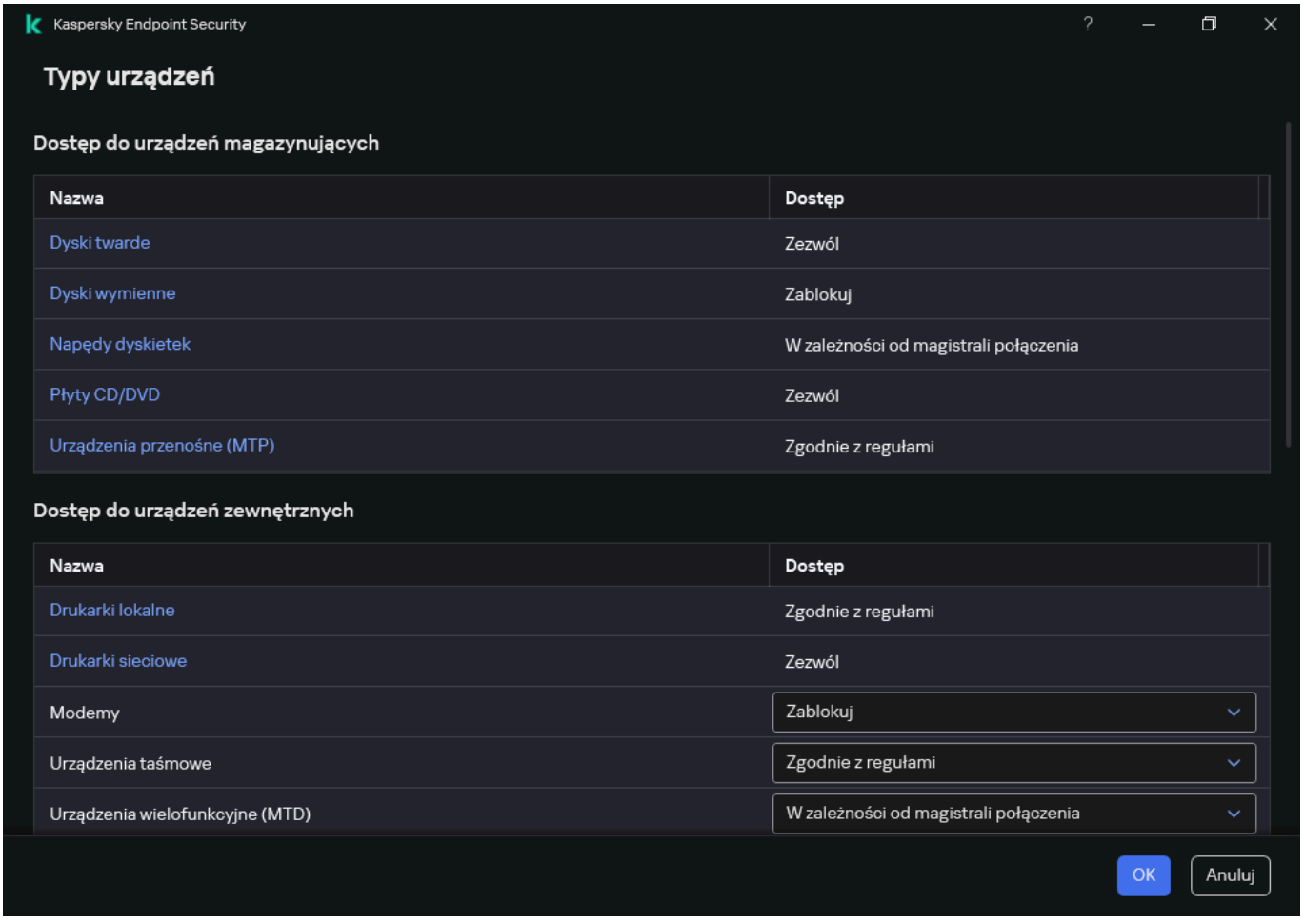
Jak skonfigurować reguły dostępu do urządzeń Bluetooth w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.

3. W sekcji **Ustawienia dostępu** kliknij przycisk **Urządzenia i sieci Wi-Fi**.

   Otwarte okno wyświetla reguły dostępu dla wszystkich urządzeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.



Typy urządzeń w komponencie Kontrola urządzeń

4. W sekcji **Dostęp do urządzeń zewnętrznych** kliknij odnośnik **Bluetooth**.

   Spowoduje to otwarcie ustawień dostępu do urządzenia Bluetooth.

5. W menu **Dostęp**, skonfiguruj tryb dostępu do urządzeń mobilnych: **Zezwól**, **Zablokuj**, **Zezwól i nie zapisuj w dzienniku**.

6. Jeśli wybierzesz opcję **Zablokuj** trybie można zezwolić na podłączanie tylko urządzeń wejściowych Bluetooth (klawiatury, myszy itp.). Aby to zrobić, w sekcji **Wykluczenia** wybierz pole wyboru **Urządzenia wejściowe (myszy i klawiatury)**.

7. Zapisz swoje zmiany.

Kontrola wydruku

Kontrola drukowania nie jest obsługiwana na komputerach opartych na architekturze Arm.

Możesz użyć opcji Kontrola wydruku, aby skonfigurować dostęp użytkowników do drukarek lokalnych i sieciowych.

Kontrola drukarki lokalnej

Kaspersky Endpoint Security umożliwia skonfigurowanie dostępu do drukarek lokalnych na dwóch poziomach: *łączenie* oraz *drukowanie*.

Kaspersky Endpoint Security kontroluje połączenie drukarki lokalnej przez następujące magistrale: USB, Port szeregowy (COM), Port równoległy (LPT).

Kaspersky Endpoint Security kontroluje połączenie drukarek lokalnych z portami COM i LPT tylko na poziomie magistrali. Aby zapobiec połączeniom drukarek przez porty COM i LPT, należy wybrać tryb dostępu W zależności od magistrali połączenia dla drukarek lokalnych i zabronić połączeń do magistrali COM i LPT.

W przypadku drukarek podłączonych do USB aplikacja sprawuje kontrolę na dwóch poziomach: typ urządzenia (drukarki lokalne) oraz magistrala połączenia (USB).

Możesz wybrać jeden z następujących trybów dostępu do lokalnych drukarek za pomocą USB:

- **Zezwól** ✓. Kaspersky Endpoint Security zapewnia pełny dostęp do drukarek lokalnych wszystkim użytkownikom. Użytkownicy mogą podłączać drukarki i drukować dokumenty za pomocą środków dostępnych w systemie operacyjnym.

- **Blokuj** ⊘. Kaspersky Endpoint Security blokuje połączenie drukarek lokalnych. Aplikacja umożliwia podłączenie tylko zaufanych drukarek.

- **W zależności od magistrali połączenia**. Kaspersky Endpoint Security umożliwia łączenie się z drukarkami lokalnymi zgodnie ze stanem połączenia magistrali USB (**Zezwól** lub **Blokuj**).
- **Zgodnie z regułami**. Aby kontrolować drukowanie, musisz dodać *reguły drukowania*. W regułach możesz wybrać użytkowników lub grupy użytkowników, którym chcesz umożliwić lub zablokować dostęp do drukowania dokumentów na drukarkach lokalnych.

Kontrola drukarki sieciowej

Kaspersky Endpoint Security umożliwia skonfigurowanie dostępu do drukowania na drukarkach sieciowych. Możesz wybrać jeden z następujących trybów dostępu do drukarek sieciowych:

- **Zezwól i nie zapisuj w dzienniku**. Kaspersky Endpoint Security nie kontroluje drukowania na drukarkach sieciowych. Aplikacja przyznaje dostęp do drukowania wszystkim użytkownikom i nie zapisuje informacji o wydruku do dziennika zdarzeń.
- **Zezwól**. Kaspersky Endpoint Security zapewnia dostęp do drukowania na drukarkach sieciowych wszystkim użytkownikom.
- **Blokuj**. Kaspersky Endpoint Security ogranicza wszystkim użytkownikom dostęp do drukarek sieciowych. Aplikacja umożliwia dostęp tylko do zaufanych drukarek.
- **Zgodnie z regułami**. Kaspersky Endpoint Security przyznaje dostęp do drukowania zgodnie z regułami drukowania. W regułach możesz wybrać użytkowników lub grupy użytkowników, którzy będą mogli drukować dokumentów na drukarce sieciowej.

Dodawanie reguł drukowania dotyczących drukarek

Jak dodawać reguły drukowania w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
4. W menu **Ustawienia Kontroli urządzeń**, Wybierz zakładkę **Typy urządzeń**.

   Tabela zawiera reguły dostępu do wszystkich urządzeń, które są obecne w klasyfikacji komponentu Kontrola urządzeń.
5. W menu kontekstowym typów urządzeń: **Drukarki lokalne** oraz **Drukarki sieciowe** skonfiguruj tryb dostępu do odpowiednich drukarek: **Zezwól**, **Blokuj**, **Zezwól i nie zapisuj w dzienniku** (tylko w przypadku drukarek sieciowych) lub **W zależności od magistrali połączenia** (tylko w przypadku drukarek lokalnych).
6. Aby skonfigurować reguły drukowania na drukarkach lokalnych i sieciowych, kliknij dwukrotnie listy reguł, aby je otworzyć.
7. Wybierz **Zgodnie z regułami** jako tryb dostępu do drukarki.

8. Wybierz użytkowników lub grupy użytkowników, do których chcesz zastosować regułę drukowania.

   a. Kliknij **Dodaj**.

      Spowoduje to otwarcie okna dodania nowej reguły drukowania.

   b. Przypisz priorytet do wpisu reguły. Wpis reguły zawiera następujące atrybuty: konto użytkownika, czynność (zezwalaj/blokuj) i priorytet.

      Reguła posiada określony priorytet. Jeśli użytkownik został dodany do kilku grup, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o regułę z najwyższym priorytetem. Kaspersky Endpoint Security umożliwia użytkownikowi przypisanie priorytetu od 0 do 10 000. Im większa wartość, tym większy priorytet. Innymi słowy, wpis z wartością 0 posiada najniższy priorytet.

      Na przykład, możesz nadać uprawnienia tylko do odczytu grupie Każdy oraz nadać uprawnienia do odczytu/zapisu grupie administracyjnej. Aby to zrobić, przypisz priorytet 1 dla grupy administratorów oraz przypisz priorytet 0 dla grupy Każdy.

      Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Innymi słowy, jeśli użytkownik został dodany do kilku grup, a priorytet wszystkich reguł jest taki sam, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o dowolną istniejącą regułę blokowania.

   c. W menu **Akcja** skonfiguruj dostęp użytkownika do drukowania na drukarce.

   d. Kliknij **Użytkownicy i grupy** i wybierz użytkowników lub grupy użytkowników, aby ustawić dostęp do drukowania. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

   e. Kliknij **OK**.

9. Zapisz swoje zmiany.

Jak dodać regułę drukowania w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.

5. W sekcji **Reguły dostępu do urządzenia** kliknij odnośnik **Urządzenia i sieci Wi-Fi**.

   Tabela zawiera reguły dostępu do wszystkich urządzeń, które są obecne w klasyfikacji komponentu Kontrola urządzeń.

6. Wybierz rodzaj urządzenia **Drukarki lokalne** lub **Drukarki sieciowe**.

   Spowoduje to otwarcie reguł dostępu do drukarki.

7. Skonfiguruj tryb dostępu do odpowiednich drukarek: **Zezwól**, **Zablokuj**, **Zezwól i nie zapisuj w dzienniku** (tylko w przypadku drukarek sieciowych), **W zależności od magistrali** (tylko w przypadku drukarek lokalnych) lub **Niestandardowe**.

8. Jeśli wybierzesz opcję **Niestandardowe** należy dodać reguły drukowania drukarek lokalnych lub sieciowych. Aby to zrobić, kliknij przycisk **Dodaj** w tabeli zasad drukowania.

   Spowoduje to otwarcie ustawień nowej reguły drukowania.

9. Przypisz priorytet do wpisu reguły. Wpis reguły zawiera następujące atrybuty: konto użytkownika, czynność (zezwalaj/blokuj) i priorytet.

   Reguła posiada określony priorytet. Jeśli użytkownik został dodany do kilku grup, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o regułę z najwyższym priorytetem. Kaspersky Endpoint Security umożliwia użytkownikowi przypisanie priorytetu od 0 do 10 000. Im większa wartość, tym większy priorytet. Innymi słowy, wpis z wartością 0 posiada najniższy priorytet.

   Na przykład, możesz nadać uprawnienia tylko do odczytu grupie Każdy oraz nadać uprawnienia do odczytu/zapisu grupie administracyjnej. Aby to zrobić, przypisz priorytet 1 dla grupy administratorów oraz przypisz priorytet 0 dla grupy Każdy.

   Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Innymi słowy, jeśli użytkownik został dodany do kilku grup, a priorytet wszystkich reguł jest taki sam, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o dowolną istniejącą regułę blokowania.

10. W menu **Akcja** skonfiguruj dostęp użytkownika do drukowania na drukarce.

11. W menu **Użytkownik lub grupa**, wybierz użytkowników lub grupy użytkowników, aby ustawić dostęp do drukowania. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

12. Zapisz swoje zmiany.

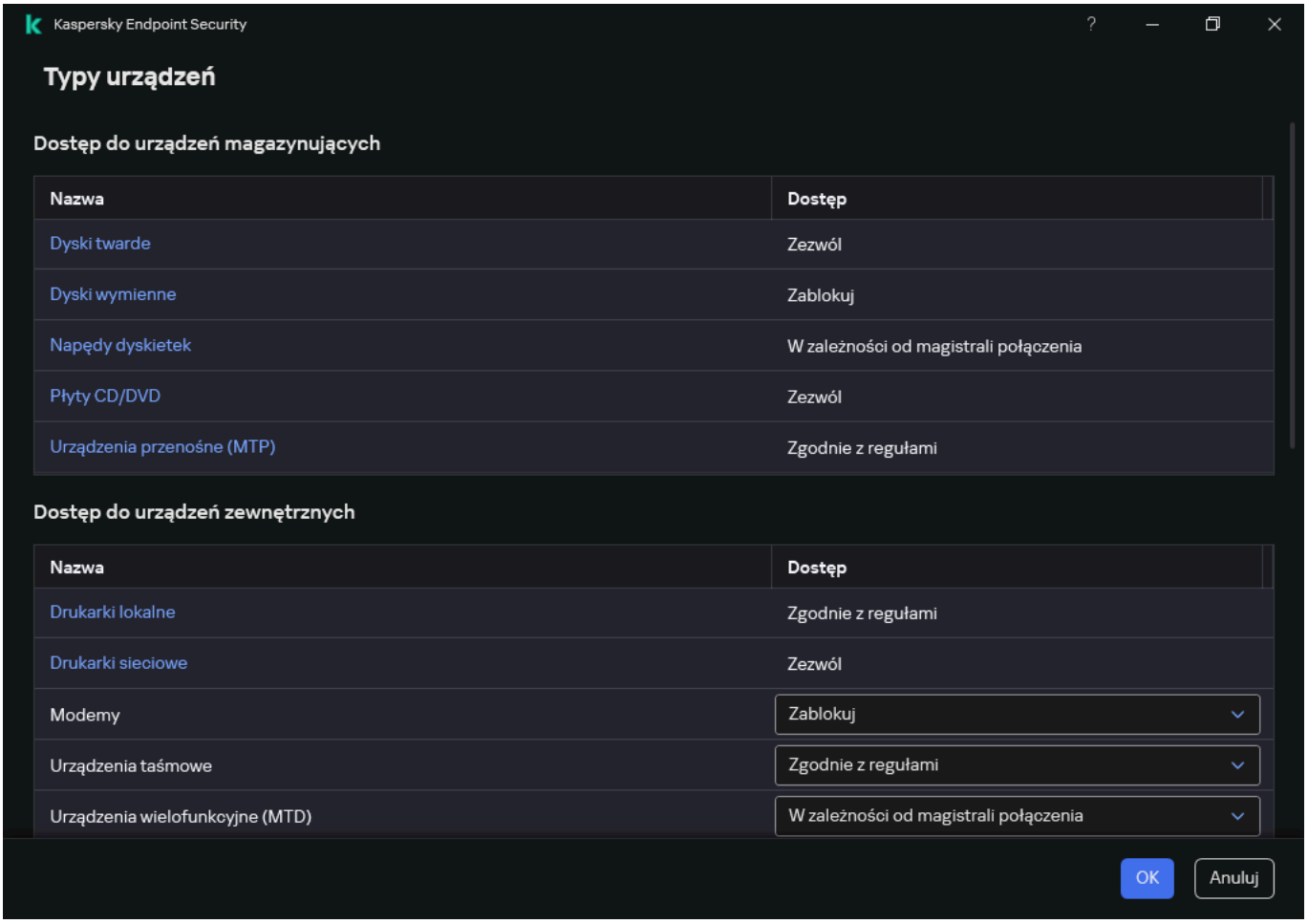
Jak dodać reguły drukowania w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.

3. W sekcji **Ustawienia dostępu** kliknij przycisk **Urządzenia i sieci Wi-Fi**.

Otwarte okno wyświetla reguły dostępu dla wszystkich urządzeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.



Typy urządzeń w komponencie Kontrola urządzeń

4. W menu **Dostęp do urządzeń zewnętrznych**, kliknij **Drukarki lokalne** lub **Drukarki sieciowe**.

   Spowoduje to otwarcie okna z regułami dostępu do drukarki.

5. W **Dostęp do drukarek lokalnych** lub **Dostęp do drukarek sieciowych** skonfiguruj tryb dostępu dla drukarek: **Zezwól**, **Zablokuj**, **Zezwól i nie zapisuj w dzienniku** (tylko dla drukarek sieciowych), **W zależności od magistrali połączenia** (tylko dla drukarek lokalnych) lub **Zgodnie z regułami**.

6. Jeśli wybierzesz opcję **Zgodnie z regułami** należy dodać reguły drukowania na drukarkach. Wybierz użytkowników lub grupy użytkowników, do których chcesz zastosować regułę drukowania.

   a. Kliknij **Dodaj**.

      Spowoduje to otwarcie okna dodania nowej reguły drukowania.

   b. Przypisz priorytet do wpisu reguły. Wpis reguły zawiera następujące atrybuty: konto użytkownika, uprawnienia (zezwól/zablokuj) i priorytet.

      Reguła posiada określony priorytet. Jeśli użytkownik został dodany do kilku grup, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o regułę z najwyższym priorytetem. Kaspersky Endpoint Security umożliwia użytkownikowi przypisanie priorytetu od 0 do 10 000. Im większa wartość, tym większy priorytet. Innymi słowy, wpis z wartością 0 posiada najniższy priorytet.

      Na przykład, możesz nadać uprawnienia tylko do odczytu grupie Każdy oraz nadać uprawnienia do odczytu/zapisu grupie administracyjnej. Aby to zrobić, przypisz priorytet 1 dla grupy administratorów oraz przypisz priorytet 0 dla grupy Każdy.

Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Innymi słowy, jeśli użytkownik został dodany do kilku grup, a priorytet wszystkich reguł jest taki sam, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o dowolną istniejącą regułę blokowania.

c. W menu **Akcja**, skonfiguruj uprawnienia użytkownika w celu uzyskania dostępu do drukowania.

d. W menu **Użytkownicy i grupy**, wybierz użytkowników lub grupy użytkowników, aby ustawić dostęp do drukowania. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

7. Zapisz swoje zmiany.

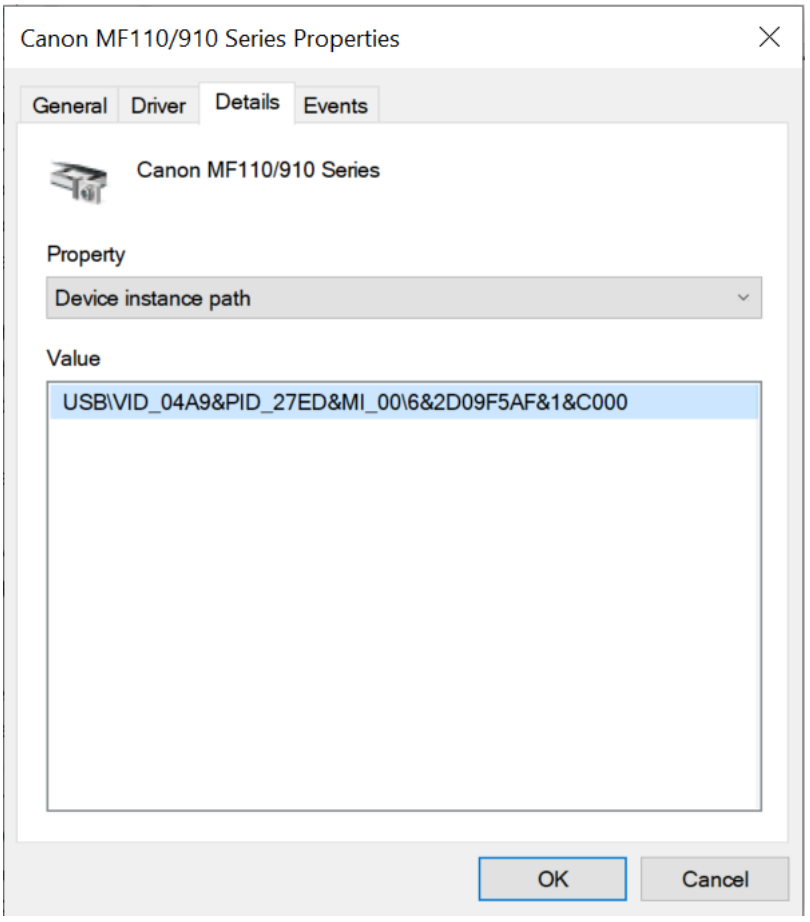
Zaufane drukarki

Zaufane urządzenia są urządzeniami, do których użytkownicy, określeni w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

Procedura dodawania zaufanych drukarek jest dokładnie taka sama, jak w przypadku innych typów zaufanych urządzeń. Możesz dodać drukarki lokalne według identyfikatora lub modelu urządzenia. Drukarki sieciowe można dodawać tylko według identyfikatora urządzenia.

Aby dodać zaufaną lokalną drukarkę za pomocą identyfikatora, będziesz potrzebować jej unikalnego identyfikatora (Hardware ID – HWID). Identyfikator można znaleźć we właściwościach urządzenia za pomocą narzędzi systemu operacyjnego (patrz rysunek poniżej). Można to zrobić w narzędziu Device Manager. Identyfikator lokalnej drukarki może wyglądać następująco: `6&2D09F5AF&1&C000`. Dodawanie urządzeń według identyfikatora jest wygodne, jeśli chcesz dodać kilka określonych urządzeń. Możesz także użyć masek.

Aby dodać zaufaną lokalną drukarkę według modelu urządzenia, będą Ci potrzebne jej Vendor ID (VID) i Product ID (PID). Identyfikatory można znaleźć we właściwościach urządzenia za pomocą narzędzi systemu operacyjnego (patrz rysunek poniżej). Szablon do wprowadzenia VID i PID: `VID_04A9&PID_27FD`. Dodawanie urządzeń według modelu jest wygodne, jeśli w swojej organizacji używasz urządzeń pewnego modelu. W ten sposób możesz dodać wszystkie urządzenia tego modelu.



Identyfikator urządzenia w Menedżerze urządzeń

Aby dodać zaufaną drukarkę sieciową, będziesz potrzebować jej identyfikatora urządzenia. W przypadku drukarek sieciowych identyfikatorem urządzenia może być nazwa sieciowa drukarki (nazwa udostępnionej drukarki), adres IP drukarki lub adres URL drukarki.

Kontrola połączeń Wi-Fi

Kontrola urządzeń umożliwia zarządzanie połączeniem Wi-Fi komputera (laptopa). Publiczne sieci Wi-Fi mogą nie być bezpieczne, a korzystanie z nich może spowodować utratę danych. Kontrola urządzeń pozwala zablokować użytkownikowi możliwość łączenia się z Wi-Fi lub zezwolić na łączenie się tylko z zaufanymi sieciami. Na przykład możesz zezwolić na łączenie się tylko z firmową siecią Wi-Fi, która jest wystarczająco bezpieczna. Kontrola urządzeń zablokuje dostęp do wszystkich sieci Wi-Fi, za wyjątkiem tych określonych na liście zaufanych.

Na komputerach z systemem Windows 11 należy włączyć usługi lokalizacyjne, aby kontrolować połączenia Wi-Fi. Aby to zrobić, musisz włączyć opcję **Usługi lokalizacyjne** przełączyć się w ustawieniach systemu operacyjnego (**Ustawienia → Prywatność & zabezpieczeń → Lokalizacja**). Jeśli usługi lokalizacyjne są wyłączone, Kaspersky Endpoint Security nie kontroluje połączeń z sieciami Wi-Fi.

Jak ograniczyć połączenia Wi-Fi w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
4. W menu **Ustawienia Kontroli urządzeń**, Wybierz zakładkę **Typy urządzeń**.

   Tabela zawiera reguły dostępu do wszystkich urządzeń, które są obecne w klasyfikacji komponentu Kontrola urządzeń.
5. W menu kontekstowym dotyczącym typu urządzenia **Wi-Fi** wybierz akcję Kontrola urządzeń, która jest wykonywana podczas łączenia się z siecią Wi-Fi: **Zezwól** (), **Blokuj** (), lub **Blokuj z wyjątkami** ().
6. Jeśli wybrano opcję **Blokuj z wyjątkami**, utwórz listę zaufanych sieci Wi-Fi:

   a. Kliknij dwukrotnie, aby otworzyć listę zaufanych sieci Wi-Fi.

   b. W sekcji **Zaufane sieci Wi-Fi** kliknij przycisk **Dodaj**.

   c. Spowoduje to otwarcie okna; w tym oknie skonfiguruj zaufaną sieć Wi-Fi (patrz rysunek poniżej):

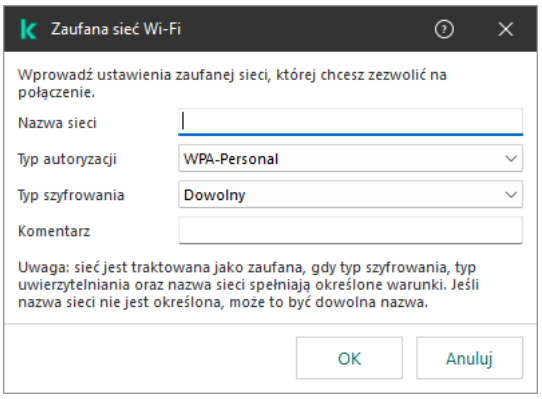
   - **Nazwa sieci**. Nazwa lub SSID (Service Set Identifier) sieci Wi-Fi.
   - **Typ autoryzacji**. Typ autoryzacji używany podczas łączenia z siecią Wi-Fi.

     Począwszy od Kaspersky Endpoint Security for Windows w wersji 12.0, do aplikacji dodano obsługę protokołu WPA3. Jeśli na komputerze zastosowano zasadę Kaspersky Endpoint Security w wersji 12.2, na komputerach z Kaspersky Endpoint Security w wersji 11.11.0 i wcześniejszych zostanie wybrany protokół WPA2; WPA2 / WPA3 jest wybrany dla wersji od 12.0 do 12.1; WPA3 jest wybrany dla wersji 12.2 i nowszych.
   - **Typ szyfrowania**. Typ szyfrowania używany do ochrony ruchu w sieci Wi-Fi.
   - **Komentarz**. Więcej informacji o dodanej sieci Wi-Fi.

   Ustawienia zaufanej sieci Wi-Fi można wyświetlić w ustawieniach routera.

   Sieć Wi-Fi jest uznawana za zaufaną, jeśli jej ustawienia odpowiadają wszystkim ustawieniom określonym w regule.

7. Zapisz swoje zmiany.



Ustawienia zaufanej sieci Wi-Fi

Jak ograniczyć połączenia Wi-Fi w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
5. W menu **Reguły dostępu do urządzenia**, Wybierz zakładkę **Urządzenia i sieci Wi-Fi**.

   Tabela zawiera reguły dostępu do wszystkich urządzeń, które są obecne w klasyfikacji komponentu Kontrola urządzeń.
6. W sekcji **Sieci Wi-Fi** kliknij odnośnik **Wi-Fi**.
7. W oknie, które zostanie otwarte, wybierz czynność Kontrola urządzeń podjętą podczas łączenia z Wi-Fi: **Zezwól**, **Zablokuj** lub **Blokuj z wykluczeniami**.
8. Jeśli wybrano opcję **Blokuj z wykluczeniami**, utwórz listę zaufanych sieci Wi-Fi:

   a. Kliknij dwukrotnie, aby otworzyć listę zaufanych sieci Wi-Fi.

   b. W sekcji **Zaufane sieci Wi-Fi** kliknij przycisk **Dodaj**.

   c. Spowoduje to otwarcie okna; w tym oknie skonfiguruj zaufaną sieć Wi-Fi (patrz rysunek poniżej):

   - **Nazwa**. Nazwa lub SSID (Service Set Identifier) sieci Wi-Fi.
   - **Typ autoryzacji**. Typ autoryzacji używany podczas łączenia z siecią Wi-Fi.

     Począwszy od Kaspersky Endpoint Security for Windows w wersji 12.0, do aplikacji dodano obsługę protokołu WPA3. Jeśli na komputerze zastosowano zasadę Kaspersky Endpoint Security w wersji 12.2, na komputerach z Kaspersky Endpoint Security w wersji 11.11.0 i wcześniejszych zostanie wybrany protokół WPA2; WPA2 / WPA3 jest wybrany dla wersji od 12.0 do 12.1; WPA3 jest wybrany dla wersji 12.2 i nowszych.

- **Typ szyfrowania**. Typ szyfrowania używany do ochrony ruchu w sieci Wi-Fi.
- **Komentarz**. Więcej informacji o dodanej sieci Wi-Fi.

Ustawienia zaufanej sieci Wi-Fi można wyświetlić w ustawieniach routera.

> Sieć Wi-Fi jest uznawana za zaufaną, jeśli jej ustawienia odpowiadają wszystkim ustawieniom określonym w regule.

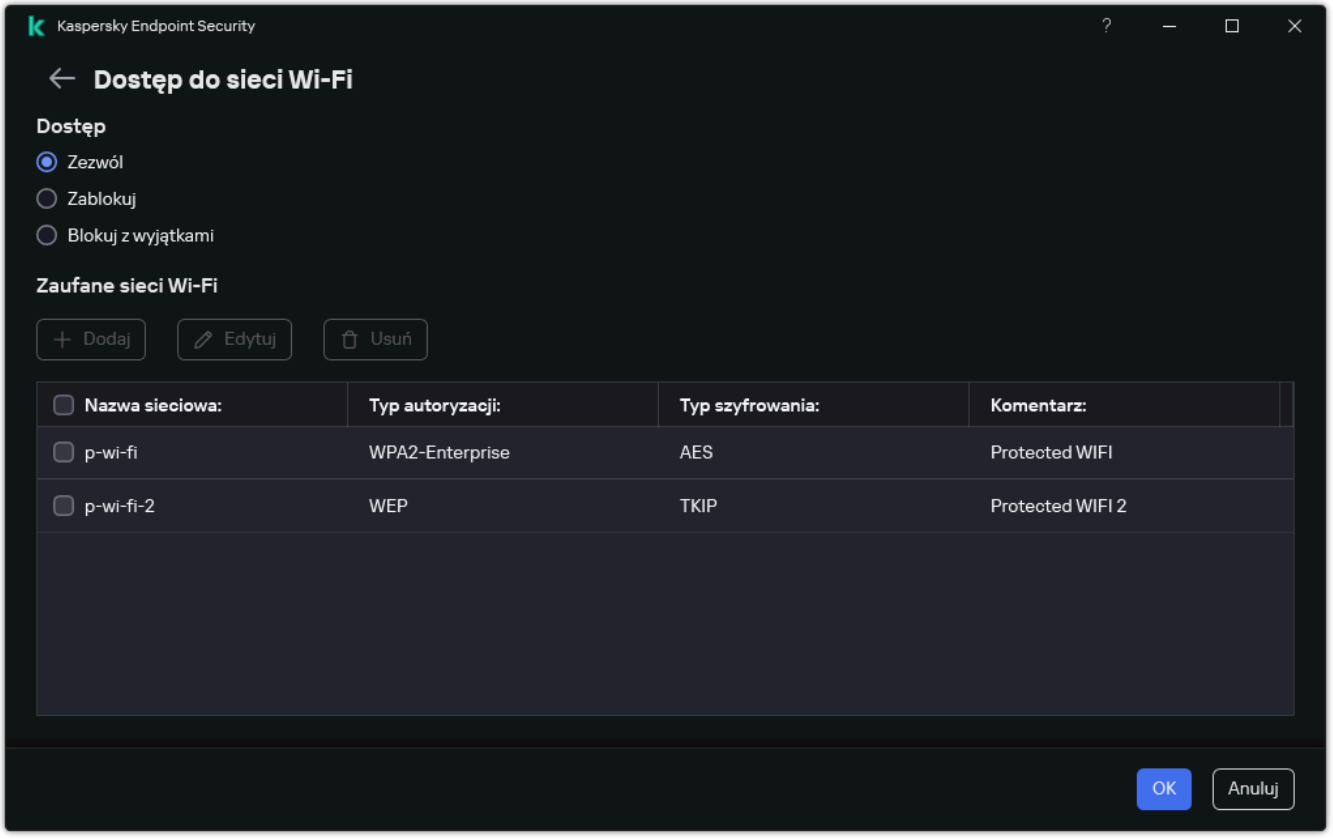
9. Zapisz swoje zmiany.

Jak ograniczyć połączenia Wi-Fi w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń → Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij przycisk **Urządzenia i sieci Wi-Fi**.

   Otwarte okno wyświetla reguły dostępu dla wszystkich urządzeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.
4. W sekcji **Dostęp do sieci Wi-Fi** kliknij odnośnik **Wi-Fi**.

   W otwartym oknie zostaną wyświetlone reguły dostępu do sieci Wi-Fi.



Ustawienia dostępu Wi-Fi

5. W menu **Dostęp**, wybierz czynność Kontrola urządzeń podjętą podczas łączenia z Wi-Fi: **Zezwól**, **Zablokuj**, lub **Blokuj z wyjątkami**.

6. Jeśli wybrano opcję **Blokuj z wyjątkami**, utwórz listę zaufanych sieci Wi-Fi:

   a. W sekcji **Zaufane sieci Wi-Fi** kliknij przycisk **Dodaj**.

   b. Spowoduje to otwarcie okna; w tym oknie skonfiguruj zaufaną sieć Wi-Fi (patrz rysunek poniżej):

   - **Nazwa sieciowa**. Nazwa lub SSID (Service Set Identifier) sieci Wi-Fi.
   - **Typ autoryzacji**. Typ autoryzacji używany podczas łączenia z siecią Wi-Fi.

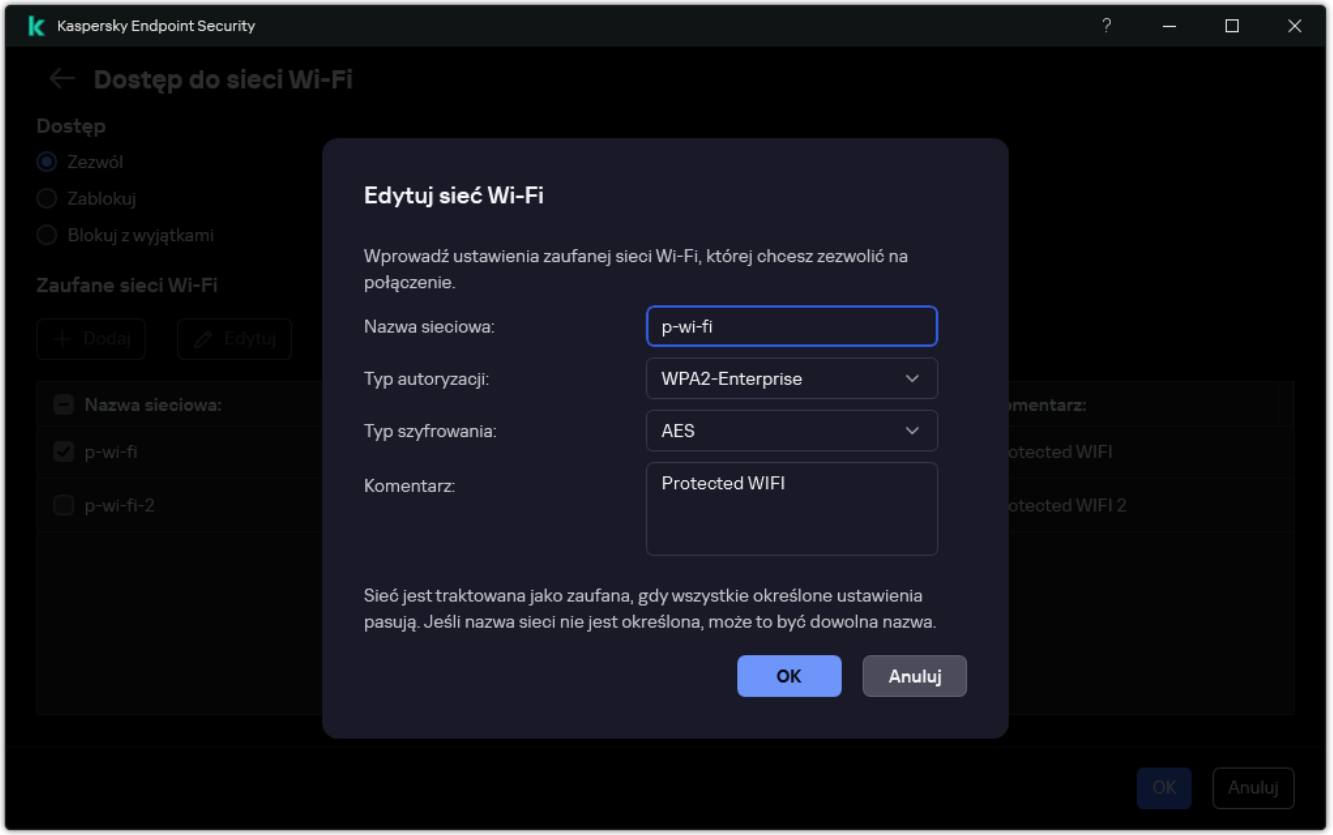
     Począwszy od Kaspersky Endpoint Security for Windows w wersji 12.0, do aplikacji dodano obsługę protokołu WPA3. Jeśli na komputerze zastosowano zasadę Kaspersky Endpoint Security w wersji 12.2, na komputerach z Kaspersky Endpoint Security w wersji 11.11.0 i wcześniejszych zostanie wybrany protokół WPA2; WPA2 / WPA3 jest wybrany dla wersji od 12.0 do 12.1; WPA3 jest wybrany dla wersji 12.2 i nowszych.

   - **Typ szyfrowania**. Typ szyfrowania używany do ochrony ruchu w sieci Wi-Fi.
   - **Komentarz**. Więcej informacji o dodanej sieci Wi-Fi.

   Ustawienia zaufanej sieci Wi-Fi można wyświetlić w ustawieniach routera.

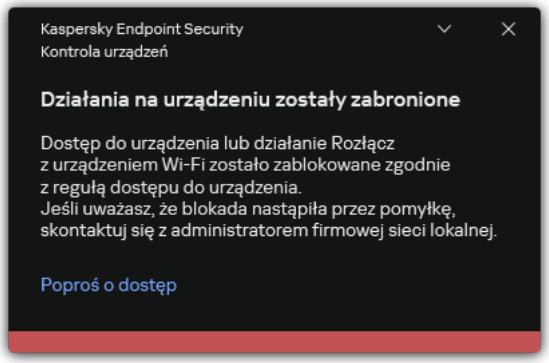
   Sieć Wi-Fi jest uznawana za zaufaną, jeśli jej ustawienia odpowiadają wszystkim ustawieniom określonym w regule.

7. Zapisz swoje zmiany.



Ustawienia zaufanej sieci Wi-Fi

W rezultacie, gdy użytkownik próbuje połączyć się z siecią Wi-Fi, która nie jest wymieniona jako zaufana, aplikacja blokuje połączenie i wyświetla powiadomienie (patrz rysunek poniżej).



Komunikat Kontroli urządzeń

Monitorowanie korzystania z nośników wymiennych

Monitorowanie korzystania z dysków wymiennych obejmuje:

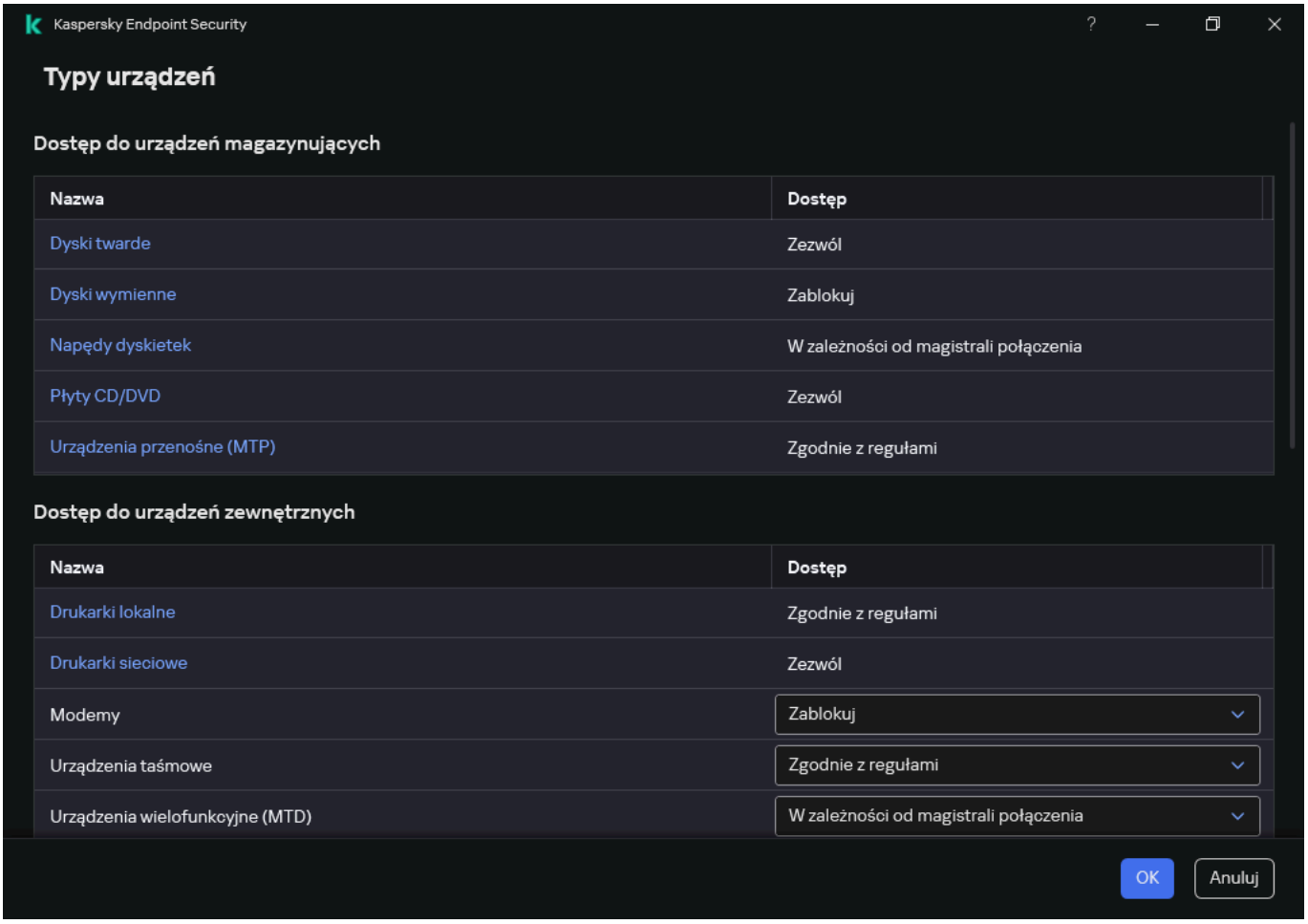
- Monitorowanie działań wykonywanych na plikach na dyskach wymiennych.
- Monitorowanie podłączenia i odłączenia zaufanych dysków wymiennych.

  Kaspersky Endpoint Security umożliwia monitorowanie podłączenia i odłączenia wszystkich zaufanych urządzeń, a nie tylko dysków wymiennych. Możesz włączyć zapisywanie zdarzeń w ustawieniach powiadomień dla komponentu Kontrola urządzeń. Zdarzenia mają priorytet *Wiadomość informacyjna*.

W celu włączenia monitorowania korzystania z nośnika wymiennego:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij przycisk **Urządzenia i sieci Wi-Fi**.

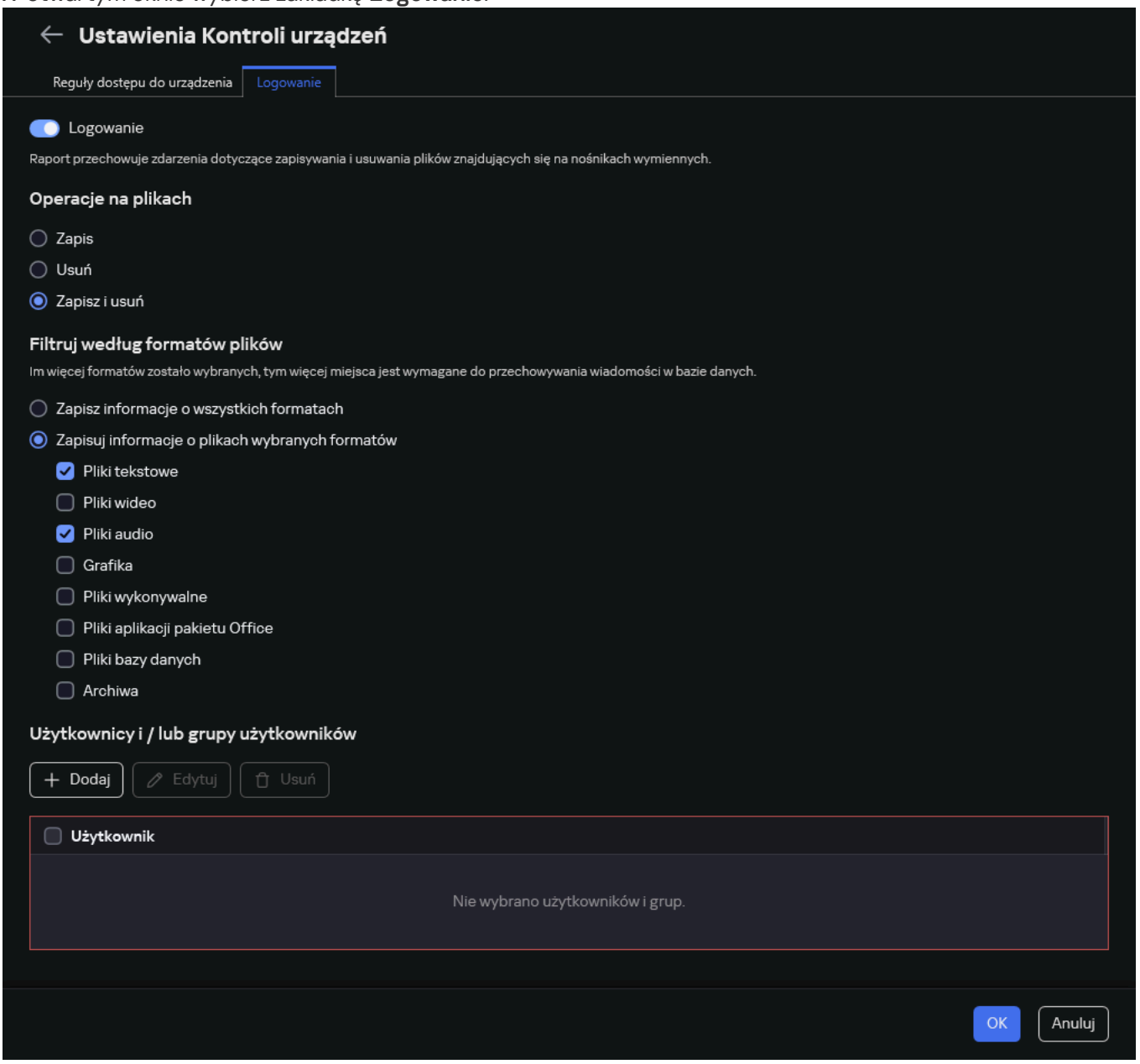
Otwarte okno wyświetla reguły dostępu dla wszystkich urządzeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.



Typy urządzeń w komponencie Kontrola urządzeń

4. W bloku **Dostęp do urządzeń magazynujących** wybierz **Dyski wymienne**.

5. W otwartym oknie wybierz zakładkę **Logowanie**.



Ustawienia monitorowania użycia dysku wymiennego

6. Włącz przełącznik **Logowanie**.

7. W sekcji **Operacje na plikach** wybierz operacje, które chcesz monitorować: **Zapis**, **Usuń**.

8. W sekcji **Filtruj według formatów plików** wybierz formaty plików, których skojarzone operacje powinny zostać zarejestrowane przez Kontrolę urządzeń.

9. Wybierz użytkowników lub grupy użytkowników korzystających z nośników wymiennych, które chcesz monitorować.

10. Zapisz swoje zmiany.

W wyniku tego działania, jeśli użytkownicy zapisują do plików znajdujących się na nośnikach wymiennych lub usuwają pliki z nośników wymiennych, Kaspersky Endpoint Security będzie zapisywał informacje o tych działaniach do raportu zdarzeń i wyśle zdarzenia do Kaspersky Security Center. Możesz wyświetlić zdarzenia skojarzone z plikami na nośnikach wymiennych w Konsoli administracyjnej Kaspersky Security Center, w obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Zdarzenia**. Aby zdarzenia były wyświetlane w lokalnym raporcie zdarzeń Kaspersky Endpoint Security, w ustawieniach powiadomień modułu Kontrola urządzeń należy zaznaczyć pole **Operacja na pliku została wykonana**.

Zmiana czasu trwania buforowania

Komponent Kontrola urządzeń rejestruje zdarzenia dotyczące monitorowanych urządzeń, takie jak podłączanie i odłączanie urządzenia, odczyt pliku z urządzenia, zapis pliku na urządzeniu oraz inne zdarzenia. Następnie Kontrola urządzeń zezwala na lub blokuje działanie zgodnie z ustawieniami Kaspersky Endpoint Security.

Kontrola urządzeń zapisuje informacje o zdarzeniach dla określonego przedziału czasu zwanego *okresem buforowania*. Jeśli informacje dotyczące zdarzenia są buforowane, a to zdarzenie jest powtarzane, wówczas nie ma potrzeby informowania Kaspersky Endpoint Security o tym fakcie ani wyświetlać żadnego monitu o udzielenie dostępu do odpowiedniego działania, takiego jak nawiązanie połączenia z urządzeniem. To umożliwia wygodniejszą pracę z urządzeniem.

Zdarzenie jest uznawane za duplikat urządzenia, jeśli wszystkie następujące ustawienia zdarzenia odpowiadają wpisowi w pamięci podręcznej:

- ID urządzenia
- SID próby dostępu do konta użytkownika
- Kategoria urządzenia
- Działanie podjęte na urządzeniu
- Uprawnienia aplikacji dla tego działania: dozwolone lub zablokowane
- Ścieżka dostępu do procesu użytego do podjęcia działania
- Plik, do którego jest uzyskiwany dostęp

Przed zmianą okresu buforowania wyłącz autoochronę Kaspersky Endpoint Security. Po zmianie okresu buforowania włącz autoochronę.

W celu zmiany okresu buforowania:

1. Otwórz edytor rejestru na komputerze.
2. W edytorze rejestru przejdź do następującej sekcji:
   - Dla 64-bitowych systemów operacyjnych:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]`
   - Dla 32-bitowych systemów operacyjnych:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]`
3. Otwórz `DeviceControlEventsCachePeriod` do edycji.
4. Określ, przez ile minut Kontrola urządzeń musi zapisywać informacje o zdarzeniu zanim te informacje zostaną usunięte.

Działania podejmowane na zaufanych urządzeniach

Zaufane urządzenia są urządzeniami, do których użytkownicy, określeni w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

Aby pracować z zaufanymi urządzeniami, możesz przyznać dostęp do pojedynczego użytkownika, grupy użytkowników lub wszystkich użytkowników organizacji.

Na przykład, jeśli Twoja organizacja nie zezwala na korzystanie z dysków wymiennych, ale administratorzy używają dysków wymiennych w swojej pracy, możesz zezwolić na dyski wymienne tylko dla grupy administratorów. Aby to zrobić, dodaj dyski wymienne do listy zaufanych i skonfiguruj uprawnienia dostępu użytkownika.

Nie jest zalecane dodawanie więcej niż 5000 zaufanych urządzeń, gdyż może to spowodować niestabilność systemu.

Kaspersky Endpoint Security pozwala dodać urządzenie do listy zaufanych w następujący sposób:

- Jeśli Kaspersky Security Center nie jest wdrożony w Twojej organizacji, możesz podłączyć urządzenie do komputera i dodać je do listy zaufanych w ustawieniach aplikacji. Aby rozpowszechnić listę zaufanych urządzeń na wszystkich komputerach w organizacji, możesz włączyć scalanie list zaufanych urządzeń w zasadzie lub skorzystać z procedury eksportu/importu.

- Jeśli Kaspersky Security Center jest wdrożony w Twojej organizacji, możesz zdalnie wykrywać wszystkie podłączone urządzenia i utworzyć listę zaufanych urządzeń w zasadzie. Lista zaufanych urządzeń będzie dostępna na wszystkich komputerach, do których zastosowano zasadę.

Kaspersky Endpoint Security umożliwia kontrolowanie użycia zaufanych urządzeń (połączenie i rozłączenie). Możesz włączyć zapisywanie zdarzeń w ustawieniach powiadomień dla komponentu Kontrola urządzeń. Zdarzenia mają priorytet *Zdarzenia informacyjne*.

Dodawanie urządzenia do listy Zaufane z poziomu interfejsu aplikacji

Domyślnie podczas dodawania urządzenia do listy zaufanych urządzeń dostęp do niego jest dozwolony dla wszystkich użytkowników (grupa użytkowników Wszyscy).

W celu dodania urządzenia do listy Zaufane z poziomu interfejsu aplikacji:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.

3. W sekcji **Ustawienia dostępu** kliknij przycisk **Zaufane urządzenia**.

   Spowoduje to otwarcie listy zaufanych urządzeń.

4. Kliknij **Wybierz**.

   Spowoduje to otwarcie listy podłączonych urządzeń. Lista urządzeń zależy od wartości wybranej z listy rozwijalnej **Wyświetl podłączone urządzenia**.

5. Na liście urządzeń wybierz urządzenie, które chcesz dodać do listy zaufanych.

   Kaspersky Endpoint Security nie obsługuje dodawania urządzeń typu **Napędy dyskietek** na listę zaufanych.

6. W polu **Komentarz** możesz wprowadzić dowolne odpowiednie informacje o zaufanym urządzeniu.

7. Wybierz użytkowników lub grupy użytkowników, którym chcesz zezwolić na dostęp do zaufanych urządzeń.

   Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

8. Zapisz swoje zmiany.

Dodawanie urządzenia do listy Zaufane z poziomu Kaspersky Security Center

Kaspersky Security Center otrzymuje informacje o urządzeniach, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerach i włączona jest Kontrola urządzeń. Nie można dodać urządzenia do listy zaufanych, chyba że informacje o tym urządzeniu są dostępne w Kaspersky Security Center.

Możesz dodać urządzenie do listy zaufanych zgodnie z następującymi danymi:

- **Urządzenia według ID**. Każde urządzenie posiada unikatowy identyfikator (identyfikator sprzętu lub HWID). Możesz sprawdzić identyfikator we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Przykładowy identyfikator urządzenia: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Dodawanie urządzeń według identyfikatora jest wygodne, jeśli chcesz dodać kilka określonych urządzeń.

- **Urządzenia według modelu**. Każde urządzenie posiada identyfikator producenta (VID) oraz identyfikator produktu (PID). Możesz sprawdzić identyfikatory we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Szablon do wprowadzenia VID i PID: `VID_1234&PID_5678`. Dodawanie urządzeń według modelu jest wygodne, jeśli w swojej organizacji używasz urządzeń pewnego modelu. W ten sposób możesz dodać wszystkie urządzenia tego modelu.

- **Urządzenia według maski ID**. Jeśli używasz kilku urządzeń z podobnymi identyfikatorami, możesz dodać urządzenia do listy zaufanych, korzystając z maski. Znak `*` zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku `?` podczas wprowadzania maski. Na przykład, `WDC_C*`.

- **Urządzenia według maski modelu**. Jeśli używasz kilku urządzeń z podobnymi numerami VID lub PID (na przykład, urządzeń od tego samego producenta), możesz dodać urządzenia do listy zaufanych przy użyciu masek. Znak `*` zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku `?` podczas wprowadzania maski. Na przykład, `VID_05AC&PID_*`.

Zmiana listy zaufanych urządzeń może zostać zablokowana przez właściwości zasady nadrzędnej. Aby zmienić listę, musisz zezwolić na zmianę ustawień strefy zaufanej w Web Console (kłódka musi być odblokowana).

Strefy zaufane są grupowane w różny sposób w Konsoli administracyjnej (MMC) i Web Console. Sposoby zapobiegania zmianom parametrów strefy zaufanej również mogą się różnić („kłódki" mogą być inne). Zalecamy korzystanie wyłącznie z Web Console do zarządzania aplikacją. Jeśli skonfigurujesz strefę zaufaną w różnych konsolach, wtyczka zarządzająca może przywrócić „kłódkę" do stanu domyślnego.

W celu dodania urządzeń do listy zaufanych urządzeń:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.

4. W prawej części okna wybierz zakładkę **Zaufane urządzenia**.

5. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę zaufanych urządzeń dla wszystkich komputerów w firmie.

   Listy zaufanych urządzeń w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Zaufane urządzenia z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie zaufanych urządzeń zasady nadrzędnej nie jest możliwe.

6. Kliknij przycisk **Dodaj** i wybierz metodę dodawania urządzenia do listy zaufanych.

7. Aby filtrować urządzenia, wybierz typ urządzenia z listy rozwijanej **Typ urządzenia** (na przykład: **Dyski wymienne**).

   Kaspersky Endpoint Security nie obsługuje dodawania urządzeń typu **Napędy dyskietek** na listę zaufanych.

8. W polu **Nazwa / Model** wprowadź identyfikator urządzenia, model (identyfikator VID i identyfikator PID) lub maskę, w zależności od wybranej metody dodawania.

   Dodawanie urządzeń według maski modelu (VID i PID) działa w następujący sposób: jeśli wprowadzisz maskę modelu, która nie odpowiada żadnemu modelowi, Kaspersky Endpoint Security sprawdza, czy identyfikator urządzenia (HWID) odpowiada masce. Kaspersky Endpoint Security sprawdza tylko część identyfikatora urządzenia, która określa producenta i typ urządzenia (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Jeśli maska modelu odpowiada tej części identyfikatora urządzenia, urządzenia, które odpowiadają masce, zostaną dodane do listy zaufanych urządzeń na komputerze. W tym samym czasie lista urządzeń w Kaspersky Security Center pozostanie pusta po kliknięciu przycisku **Odśwież**. Aby poprawnie wyświetlić listę urządzeń, możesz dodać urządzenia według maski identyfikatora urządzenia.

9. Aby filtrować urządzenia, w polu **Komputer** wprowadź nazwę komputera lub maskę odpowiadającą nazwie komputera, do którego urządzenie jest podłączone.

   Znak `*` zastępuje dowolny zestaw znaków. Znak `?` zastępuje dowolny pojedynczy znak.

10. Kliknij przycisk **Odśwież**.

    Tabela wyświetla listę urządzeń, które spełniają zdefiniowane kryteria filtrowania.

11. Zaznacz pole obok nazw urządzeń, które chcesz dodać do listy zaufanych.

12. W polu **Komentarz** wprowadź opis przyczyny dodania urządzeń do listy zaufanych.

13. Kliknij przycisk **Wybierz** po prawej stronie pola **Zezwól użytkownikom i / lub grupom użytkowników**.

14. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

    Domyślnie dostęp do zaufanych urządzeń jest dozwolony dla grupy Wszyscy.

15. Zapisz swoje zmiany.

Po podłączeniu urządzenia Kaspersky Endpoint Security sprawdza listę zaufanych urządzeń w poszukiwaniu autoryzowanego użytkownika. Jeśli urządzenie jest zaufane, Kaspersky Endpoint Security zezwala na dostęp do urządzenia ze wszystkimi uprawnieniami, nawet jeśli odmówiono dostępu do typu urządzenia lub magistrali połączenia. Jeśli urządzenie jest niezaufane, a dostęp jest zabroniony, możesz poprosić o dostęp do zablokowanego urządzenia.

Eksportowanie i importowanie listy zaufanych urządzeń

Aby rozpowszechnić listę zaufanych urządzeń na wszystkich komputerach w organizacji, możesz skorzystać z procedury eksportu/importu.

Na przykład, jeśli chcesz rozpowszechniać listę zaufanych dysków wymiennych, wykonaj następujące czynności:

1. Podłącz kolejno dyski wymienne do komputera.
2. W ustawieniach Kaspersky Endpoint Security dodaj dyski wymienne do listy zaufanych. W razie potrzeby skonfiguruj uprawnienia dostępu użytkownika. Na przykład, zezwalaj tylko administratorom na dostęp do dysków wymiennych.
3. Wyeksportuj listę zaufanych urządzeń w ustawieniach Kaspersky Endpoint Security (patrz instrukcje poniżej).
4. Prześlij plik listy zaufanych urządzeń na inne komputery w organizacji. Na przykład, umieść plik w folderze udostępnionym.
5. Zaimportuj listę zaufanych urządzeń w ustawieniach Kaspersky Endpoint Security na inne komputery w organizacji (patrz instrukcje poniżej).

W celu zaimportowania lub wyeksportowania listy zaufanych urządzeń:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij przycisk **Zaufane urządzenia**.

   Spowoduje to otwarcie listy zaufanych urządzeń.
4. W celu wyeksportowania listy zaufanych urządzeń:
   a. Wybierz zaufane urządzenia, które chcesz wyeksportować.
   b. Kliknij **Eksportuj**.
   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę zaufanych urządzeń, wybierz folder, w którym chcesz zapisać ten plik.
   d. Zapisz plik.

      Kaspersky Endpoint Security eksportuje całą listę zaufanych urządzeń do pliku XML.
5. W celu zaimportowania listy zaufanych urządzeń:
   a. Z listy rozwijalnej **Importuj** wybierz odpowiednie działanie: **Importuj i dodaj do istniejących** lub **Importuj i zastąp istniejące**.
   b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę zaufanych urządzeń.
   c. Otwórz plik.
6. Zapisz swoje zmiany.

Po podłączeniu urządzenia Kaspersky Endpoint Security sprawdza listę zaufanych urządzeń w poszukiwaniu autoryzowanego użytkownika. Jeśli urządzenie jest zaufane, Kaspersky Endpoint Security zezwala na dostęp do urządzenia ze wszystkimi uprawnieniami, nawet jeśli odmówiono dostępu do typu urządzenia lub magistrali połączenia.

Uzyskiwanie dostępu do zablokowanego urządzenia

Podczas konfigurowania Kontroli urządzeń możesz przez przypadek zablokować dostęp do urządzenia, które jest potrzebne do pracy.

Jeśli Kaspersky Security Center nie jest zainstalowany w Twojej organizacji, możesz udzielić dostępu do urządzenia w ustawieniach Kaspersky Endpoint Security. Na przykład, możesz dodać urządzenie do listy zaufanych lub tymczasowo wyłączyć Kontrolę urządzeń.

Jeśli Kaspersky Security Center jest zainstalowany w Twojej organizacji, a profil został zastosowany do komputerów, możesz zapewnić dostęp do urządzenia w Konsoli administracyjnej.

Tryb online dla zezwalania na dostęp

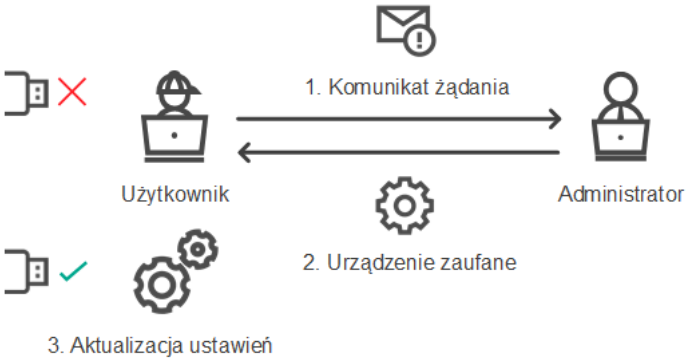
Możesz zezwolić na dostęp do zablokowanego urządzenia w trybie online tylko wtedy, gdy Kaspersky Security Center jest zainstalowany w organizacji, a profil został zastosowany do komputera. Komputer musi mieć możliwość nawiązania połączenia z Serwerem administracyjnym.

Zezwalanie na dostęp w trybie online obejmuje następujące kroki:

1. Użytkownik wysyła do administratora wiadomość zawierającą żądanie dostępu.
2. Administrator otrzymuje wiadomość z żądaniem w konsoli Kaspersky Security Center.

   W konsoli Kaspersky Security Center jest wstępnie ustawiony wybór zdarzeń *Żądania użytkownika* do łatwego śledzenia wiadomości od użytkowników.
3. Administrator dodaje urządzenie do listy zaufanych.

   Możesz dodać zaufane urządzenie w profilu dla grupy administracyjnej lub w lokalnych ustawieniach aplikacji dla pojedynczego komputera.
4. Administrator aktualizuje ustawienia Kaspersky Endpoint Security na komputerze użytkownika.



Schemat zezwalania na dostęp do urządzenia w trybie online

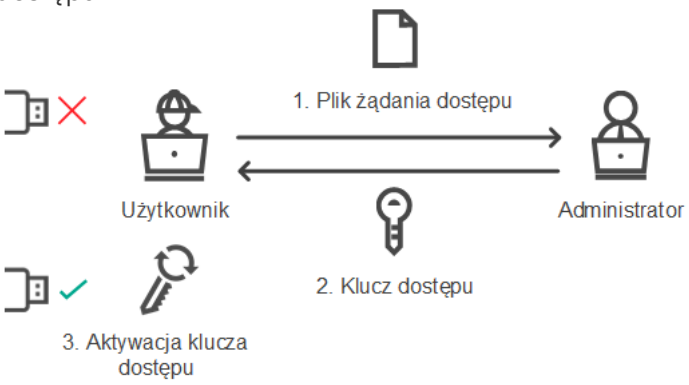
Tryb offline dla zezwalania na dostęp

Możesz zezwolić na dostęp do zablokowanego urządzenia w trybie offline tylko wtedy, gdy Kaspersky Security Center jest zainstalowany w organizacji, a profil został zastosowany do komputera. W ustawieniach profilu, w sekcji **Kontrola urządzeń**, pole **Zezwól na żądania dostępu tymczasowego** musi zostać zaznaczone.

Jeśli konieczne jest zezwolenie na dostęp tymczasowy do zablokowanego urządzenia, ale nie możesz dodać urządzenia do listy zaufanych, możesz zezwolić na dostęp do urządzenia w trybie offline. W ten sposób możesz zezwolić na dostęp do zablokowanego urządzenia nawet wtedy, gdy komputer nie ma dostępu do sieci lub jeśli komputer znajduje się poza siecią firmową.

Zezwalanie na dostęp w trybie offline obejmuje następujące kroki:

1. Użytkownik utworzy plik zawierający żądanie dostępu i wyśle go do administratora.
2. Administrator utworzy klucz dostępu z pliku zawierającego żądanie dostępu i wyśle go do użytkownika.
3. Użytkownik aktywuje klucz dostępu.



Schemat zezwalania na dostęp do urządzenia w trybie offline

Tryb online dla zezwalania na dostęp

Możesz zezwolić na dostęp do zablokowanego urządzenia w trybie online tylko wtedy, gdy Kaspersky Security Center jest zainstalowany w organizacji, a profil został zastosowany do komputera. Komputer musi mieć możliwość nawiązania połączenia z Serwerem administracyjnym.

Użytkownik żąda dostępu do zablokowanego urządzenia w następujący sposób:

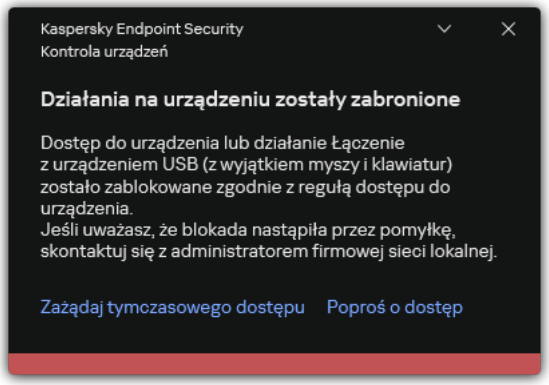
1. Podłącz urządzenie do komputera.

   Kaspersky Endpoint Security wyświetli powiadomienie informujące, że dostęp do urządzenia zostanie zablokowany (patrz rysunek poniżej).

2. Kliknij odnośnik **Poproś o dostęp**.

   To spowoduje otwarcie okna z wiadomością dla administratora. Ta wiadomość zawiera informacje o zablokowanym urządzeniu.

3. Kliknij **Wyślij**.



Komunikat Kontroli urządzeń

Następnie w konsoli Kaspersky Security Center na koncie administratora wyświetlane jest powiadomienie o zdarzeniu *Wiadomość do administratora dotycząca zablokowania dostępu do urządzenia*. Obejmuje ono informacje, takie jak nazwa użytkownika, nazwa komputera, szczegóły urządzenia, do którego użytkownik próbuje uzyskać dostęp, oraz inne informacje. Możesz skonfigurować, w jaki sposób administrator otrzymuje powiadomienia o takich zdarzeniach i, na przykład, wybrać powiadomienia e-mail. W konsoli Kaspersky Security Center jest wstępnie ustawiony wybór zdarzeń *Żądania użytkownika* do łatwego śledzenia wiadomości od użytkowników.

Aby zezwolić na dostęp, musisz dodać urządzenie do listy zaufanych urządzeń. Po zaktualizowaniu ustawień oprogramowania Kaspersky Endpoint Security na komputerze użytkownik może uzyskać dostęp do urządzenia.

Tryb offline dla zezwalania na dostęp

Możesz zezwolić na dostęp do zablokowanego urządzenia w trybie offline tylko wtedy, gdy Kaspersky Security Center jest zainstalowany w organizacji, a profil został zastosowany do komputera. W ustawieniach profilu, w sekcji **Kontrola urządzeń**, pole **Zezwól na żądania dostępu tymczasowego** musi zostać zaznaczone.

Użytkownik żąda dostępu do zablokowanego urządzenia w następujący sposób:

1. Podłącz urządzenie do komputera.

   Kaspersky Endpoint Security wyświetli powiadomienie informujące, że dostęp do urządzenia zostanie zablokowany (patrz rysunek poniżej).

2. Kliknij odnośnik **Zażądaj tymczasowego dostępu**.

   Zostanie otwarte okno zawierające listę podłączonych urządzeń.

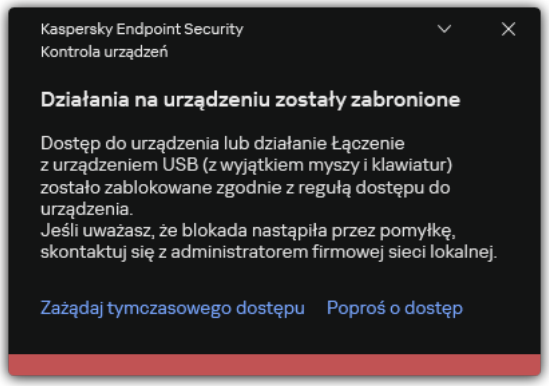
3. Z listy podłączonych urządzeń wybierz urządzenie, do którego chcesz uzyskać dostęp.

4. Kliknij **Uzyskaj plik żądania dostępu**.

5. W polu **Czas dostępu** określ przedział czasu, podczas którego chcesz mieć dostęp do urządzenia.

6. Zapisz plik w pamięci komputera.

   W rezultacie plik z żądaniem dostępu z rozszerzeniem *.akey zostanie pobrany do pamięci komputera. Użyj dowolnej dostępnej metody wysyłania pliku z żądaniem dostępu do urządzenia do administratora korporacyjnej sieci LAN.



Komunikat Kontroli urządzeń

Jak administrator może utworzyć klucz dostępu do zablokowanego urządzenia w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, do której należy wybrany komputer kliencki.

3. W obszarze roboczym wybierz zakładkę **Urządzenia**.

4. Na liście komputerów klienckich wybierz komputer, którego użytkownik ma uzyskać tymczasowy dostęp do zablokowanego urządzenia.

5. Z menu kontekstowego komputera wybierz element **Przydziel dostęp w trybie offline**.

6. Spowoduje to otwarcie okna. Wybierz w nim zakładkę **Kontrola urządzeń**.

7. Kliknij przycisk **Przeglądaj** i pobierz plik zawierający żądanie dostępu, otrzymany od użytkownika.

   Zostaną wyświetlone informacje o zablokowanym urządzeniu, do którego użytkownik zażądał dostępu.

8. Jeśli to konieczne, zmień wartość ustawienia **Czas dostępu**.

   Domyślnie, ustawienie **Czas dostępu** przyjmuje wartość, która została wskazana przez użytkownika podczas tworzenia pliku żądania dostępu.

9. Określ wartość ustawienia **Aktywny przez**.

   Ustawienie to definiuje przedział czasu, podczas którego użytkownik może aktywować dostęp do zablokowanego urządzenia przy pomocy klucza dostępu.

10. Zapisz plik klucza dostępu w pamięci komputera.

Jak administrator może utworzyć klucz dostępu do zablokowanego urządzenia w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Na liście komputerów klienckich wybierz komputer, którego użytkownik ma uzyskać tymczasowy dostęp do zablokowanego urządzenia.
3. Kliknij przycisk wielokropka (...) nad listą komputerów, a następnie przycisk **Udziel dostępu do urządzenia w trybie offline**.
4. W otwartym oknie wybierz sekcję **Kontrola urządzeń**.
5. Kliknij przycisk **Przeglądaj** i pobierz plik zawierający żądanie dostępu, otrzymany od użytkownika.

   Zostaną wyświetlone informacje o zablokowanym urządzeniu, do którego użytkownik zażądał dostępu.
6. Jeśli to konieczne, zmień wartość ustawienia **Czas dostępu (godziny)**.

   Domyślnie, ustawienie **Czas dostępu (godziny)** przyjmuje wartość, która została wskazana przez użytkownika podczas tworzenia pliku żądania dostępu.
7. Ustaw okres czasu, w którym klucz dostępu może być aktywowany na urządzeniu.

   Ustawienie to definiuje przedział czasu, podczas którego użytkownik może aktywować dostęp do zablokowanego urządzenia przy pomocy klucza dostępu.
8. Zapisz plik klucza dostępu w pamięci komputera.

W rezultacie zablokowany klucz dostępu do urządzenia zostanie pobrany do pamięci komputera. Plik klucza dostępu posiada rozszerzenie *.acode. Użyj dowolnej dostępnej metody, aby wysłać klucz dostępu do zablokowanego urządzenia do użytkownika.

Użytkownik aktywuje klucz dostępu w następujący sposób:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Żądanie dostępu** kliknij przycisk **Żądanie dostępu do urządzenia**.
4. W otwartym oknie kliknij przycisk **Aktywuj klucz dostępu**.
5. W otwartym oknie wybierz plik z kluczem dostępu do urządzenia, otrzymany od administratora korporacyjnej sieci LAN.

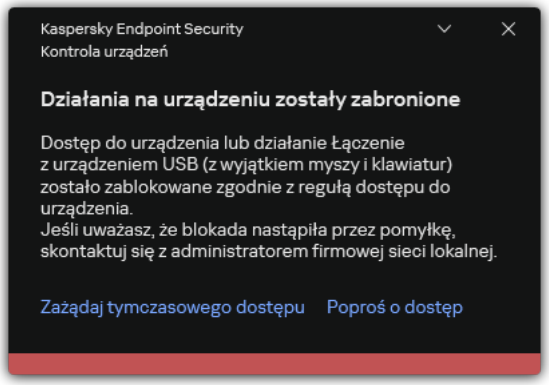
   Spowoduje to otwarcie okna zawierającego informacje o zapewnieniu dostępu.
6. Kliknij **OK**.

W rezultacie użytkownik uzyska dostęp do urządzenia na czas określony przez administratora. Użytkownik otrzyma pełny zestaw uprawnień dostępu do urządzenia (odczyt i zapis). Po wygaśnięciu klucza, dostęp do urządzenia zostanie zablokowany. Jeśli użytkownik żąda tymczasowego dostępu do urządzenia, dodaj urządzenie do listy zaufanych.

Modyfikowanie szablonów wiadomości Kontroli urządzeń

Kiedy użytkownik próbuje uzyskać dostęp do zablokowanego urządzenia, Kaspersky Endpoint Security wyświetla wiadomość informującą, że dostęp do urządzenia jest zablokowany lub operacja na zawartości urządzenia jest zabroniona. Eksperci Kaspersky udostępniają użytkownikowi szablon wiadomości opisującej powody zablokowania dostępu do urządzenia (zobacz poniższy rysunek).

Do zarządzania szablonami wiadomości dostępne są zmienne specjalne (na przykład `%USER_NAME%`). Zmienne umożliwiają stosowanie tego samego szablonu wiadomości na różnych komputerach. Podczas generowania wiadomości program Kaspersky Endpoint Security pobiera wartość zmiennej z ustawień systemu operacyjnego i wstawia ją do wiadomości odpowiedniej dla danego komputera, użytkownika i zdarzenia.



Komunikat Kontroli urządzeń

Jeśli użytkownik uważa, że dostęp do urządzenia został zablokowany lub operacja na zawartości urządzenia jest zabroniona przez pomyłkę, może wysłać wiadomość do administratora lokalnej sieci firmowej poprzez kliknięcie odnośnika w wyświetlonej wiadomości. Aby to zrobić, użytkownik musi kliknąć przycisk **Poproś o dostęp** lub **Zażądaj tymczasowego dostępu** i wysłać wiadomość do administratora opisując sytuację. Możesz również przygotować szablon wiadomości do administratora, uzupełniając go danymi, które mogą pomóc Ci podjąć decyzję o umożliwieniu lub zablokowaniu dostępu do urządzenia. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania dostępu do urządzenia**. Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkownika**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

Jak zmienić szablon wiadomości dotyczącej kontroli urządzeń w konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
4. W sekcji **Ustawienia szablonu wiadomości** kliknij przycisk **Szablony**.

5. Spowoduje to otwarcie okna; w tym oknie należy skonfigurować szablony kontroli aplikacji:

   - **Wiadomość dotycząca blokowania**. Szablon wiadomości, która pojawia się, gdy użytkownik próbuje uzyskać dostęp do zablokowanego urządzenia. Ta wiadomość pojawia się, gdy użytkownik próbuje wykonać działanie na zawartości urządzenia, które zostało zablokowane dla tego użytkownika.

   - **Wiadomość do administratora**. Szablon wiadomości, która jest wysyłana do administratora sieci LAN, gdy użytkownik uważa, że dostęp do urządzenia lub wykonywanie działań na zawartości urządzenia zostały zablokowane przez przypadek.

   Aby dodać zmienną do tekstu szablonu, umieść kursor w odpowiednim miejscu, kliknij przycisk **Zmienna** i wybierz wymaganą zmienną z listy dostępnych opcji.

   Możesz również przywrócić domyślny tekst szablonu.

6. Zapisz swoje zmiany.

Jak zmienić szablon wiadomości dotyczącej kontroli urządzeń w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.

5. W sekcji **Szablony wiadomości** skonfiguruj szablony dla wiadomości Kontroli aplikacji:

   - **Wiadomość do użytkownika**. Szablon wiadomości, która pojawia się, gdy użytkownik próbuje uzyskać dostęp do zablokowanego urządzenia. Ta wiadomość pojawia się, gdy użytkownik próbuje wykonać działanie na zawartości urządzenia, które zostało zablokowane dla tego użytkownika.

   - **Wiadomość do administratora**. Szablon wiadomości, która jest wysyłana do administratora sieci LAN, gdy użytkownik uważa, że dostęp do urządzenia lub wykonywanie działań na zawartości urządzenia zostały zablokowane przez przypadek.

   Aby dodać zmienną do tekstu szablonu, umieść kursor w odpowiednim miejscu, kliknij przycisk **Dodaj zmienną** i wybierz wymaganą zmienną z listy dostępnych opcji.

   Możesz również przywrócić domyślny tekst szablonu.

6. Zapisz swoje zmiany.

Jak zmienić szablon wiadomości dotyczącej kontroli urządzeń w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

3. W sekcji **Szablony wiadomości** skonfiguruj szablony dla wiadomości Kontroli aplikacji:

   - **Wiadomość dotycząca blokowania**. Szablon wiadomości, która pojawia się, gdy użytkownik próbuje uzyskać dostęp do zablokowanego urządzenia. Ta wiadomość pojawia się, gdy użytkownik próbuje wykonać działanie na zawartości urządzenia, które zostało zablokowane dla tego użytkownika.

   - **Wiadomość do administratora**. Szablon wiadomości, która jest wysyłana do administratora sieci LAN, gdy użytkownik uważa, że dostęp do urządzenia lub wykonywanie działań na zawartości urządzenia zostały zablokowane przez przypadek.

   Aby dodać zmienną do tekstu szablonu, umieść kursor w odpowiednim miejscu, kliknij przycisk **Dodaj zmienną** i wybierz wymaganą zmienną z listy dostępnych opcji.

   Możesz również przywrócić domyślny tekst szablonu.

4. Zapisz swoje zmiany.

Anti-Bridging

Anti-Bridging zapobiega tworzeniu mostków sieciowych poprzez uniemożliwienie jednoczesnego nawiązania kilku połączeń sieciowych dla komputera. To umożliwia ochronę sieci firmowej przed atakami na niechronione, nieautoryzowane sieci.

Anti-Bridging reguluje nawiązywanie połączeń sieciowych przy użyciu *reguł połączenia*.

Reguły połączenia są tworzone dla następujących predefiniowanych typów urządzeń:

- Karty sieciowe;
- Karty Wi-Fi;
- Modemy.

Jeśli reguła połączenia jest używana, Kaspersky Endpoint Security:

- Blokuje aktywne połączenie podczas nawiązywania nowego połączenia, jeśli typ urządzenia, określony w regule, jest używany dla obu połączeń;
- Blokuje nawiązane połączenia przy użyciu typów urządzeń, dla których używane są reguły o niższym priorytecie.

Włączanie modułu Anti-Bridging

Domyślnie moduł Anti-Bridging jest wyłączony.

W celu włączenia modułu Anti-Bridging:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij przycisk **Anti-Bridging**.

4. Użyj przełącznika **Włącz moduł Anti-Bridging**, aby włączyć lub wyłączyć tę funkcję.
5. Zapisz swoje zmiany.

Po włączeniu modułu Anti-Bridging, Kaspersky Endpoint Security blokuje już nawiązane połączenia zgodnie z regułami połączeń.

Zmiana stanu reguły połączenia

W celu zmiany stanu reguły połączenia:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij przycisk **Anti-Bridging**.
4. W sekcji **Reguły dla urządzeń** wybierz regułę, której stan chcesz zmienić.
5. Użyj przełączników w kolumnie **Kontrola**, aby włączyć lub wyłączyć regułę.
6. Zapisz swoje zmiany.

Zmiana priorytetu reguły połączenia

W celu zmiany priorytetu reguły połączenia:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij przycisk **Anti-Bridging**.
4. W sekcji **Reguły dla urządzeń** wybierz regułę, której priorytet chcesz zmienić.
5. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły połączenia.

   Im wyżej reguła znajduje się w tabeli reguł, tym wyższy priorytet posiada. Anti-Bridging blokuje wszystkie połączenia za wyjątkiem jednego połączenia nawiązanego przy użyciu typu urządzenia, dla którego używana jest reguła najwyższego poziomu.
6. Zapisz swoje zmiany.

Adaptacyjna kontrola anomalii

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Komponent Adaptacyjna kontrola anomalii monitoruje i blokuje działania, które nie są typowe dla komputerów w sieci firmowej. Adaptacyjna kontrola anomalii wykorzystuje zestaw reguł do śledzenia nietypowych zachowań (na przykład reguła *Uruchomienie procesora poleceń Microsoft Office z aplikacji biurowej*). Reguły są tworzone przez specjalistów z Kaspersky w oparciu o typowe scenariusze złośliwej aktywności. Można skonfigurować, w jaki sposób Adaptacyjna kontrola aplikacji obsługuje każdą regułę i, na przykład, zezwolić na wykonywanie skryptów PowerShell, które automatyzują określone zadania przepływu pracy. Kaspersky Endpoint Security aktualizuje zestaw reguł wraz z bazami danych aplikacji. Aktualizacje zestawów reguł muszą być potwierdzone ręcznie.

Ustawienia komponentu Adaptacyjna kontrola anomalii

Konfiguracja Adaptacyjnej kontroli anomalii składa się z następujących kroków:

1. Uczenie modułu Adaptacyjna kontrola anomalii.

   Po włączeniu Adaptacyjnej kontroli anomalii, jej reguły działają w *trybie uczenia*. Podczas uczenia moduł Adaptacyjna kontrola anomalii monitoruje wyzwalanie reguł i wysyła zdarzenia wyzwalające do Kaspersky Security Center. Każda reguła ma swój czas trwania trybu uczenia. Czas trwania trybu uczenia jest ustawiany przez ekspertów z Kaspersky. Zazwyczaj tryb uczenia jest aktywny przez dwa tygodnie.

   Jeśli podczas treningu reguła nie została w ogóle uruchomiona, Adaptacyjna kontrola anomalii uzna działania związane z tą regułą za nietypowe. Kaspersky Endpoint Security zablokuje wszystkie działania związane z tą regułą.

   Jeśli reguła została wyzwolona podczas treningu, Kaspersky Endpoint Security rejestruje zdarzenia w raporcie wyzwalającym regułę oraz w repozytorium **Wyzwalacze reguł w Trybie inteligentnego uczenia**.

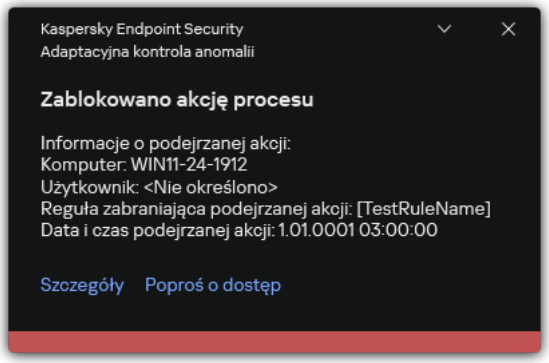
2. Analizowanie raportu dotyczącego wyzwalania reguły.

   Administrator analizuje raport wyzwalania reguł lub zawartość repozytorium **Wyzwalacze reguł w Trybie inteligentnego uczenia**. Następnie administrator może wybrać zachowanie Adaptacyjnej kontroli anomalii, gdy reguła jest wyzwalana: albo zablokować, albo zezwolić. Administrator może również kontynuować monitorowanie działania reguły i wydłużyć czas trwania trybu uczenia. Jeśli administrator nie podejmie żadnych działań, aplikacja będzie również kontynuować pracę w trybie uczenia. Czas trwania trybu uczenia zostanie zrestartowany.

Adaptacyjna kontrola anomalii jest konfigurowana w czasie rzeczywistym poprzez następujące kanały:

- Adaptacyjna kontrola anomalii automatycznie rozpoczyna blokowanie działań związanych z regułami, które nigdy nie zostały wyzwolone w trybie uczenia.
- Kaspersky Endpoint Security dodaje nowe reguły lub usuwa przestarzałe.
- Administrator konfiguruje działanie Adaptacyjnej kontroli anomalii po przejrzeniu raportu dotyczącego wyzwalania reguły i zawartości repozytorium **Wyzwalacze reguł w Trybie inteligentnego uczenia**. Zalecamy sprawdzenie raportu o wyzwalaniu reguł i zawartości magazynu **Wyzwalacze reguł w Trybie inteligentnego uczenia**.

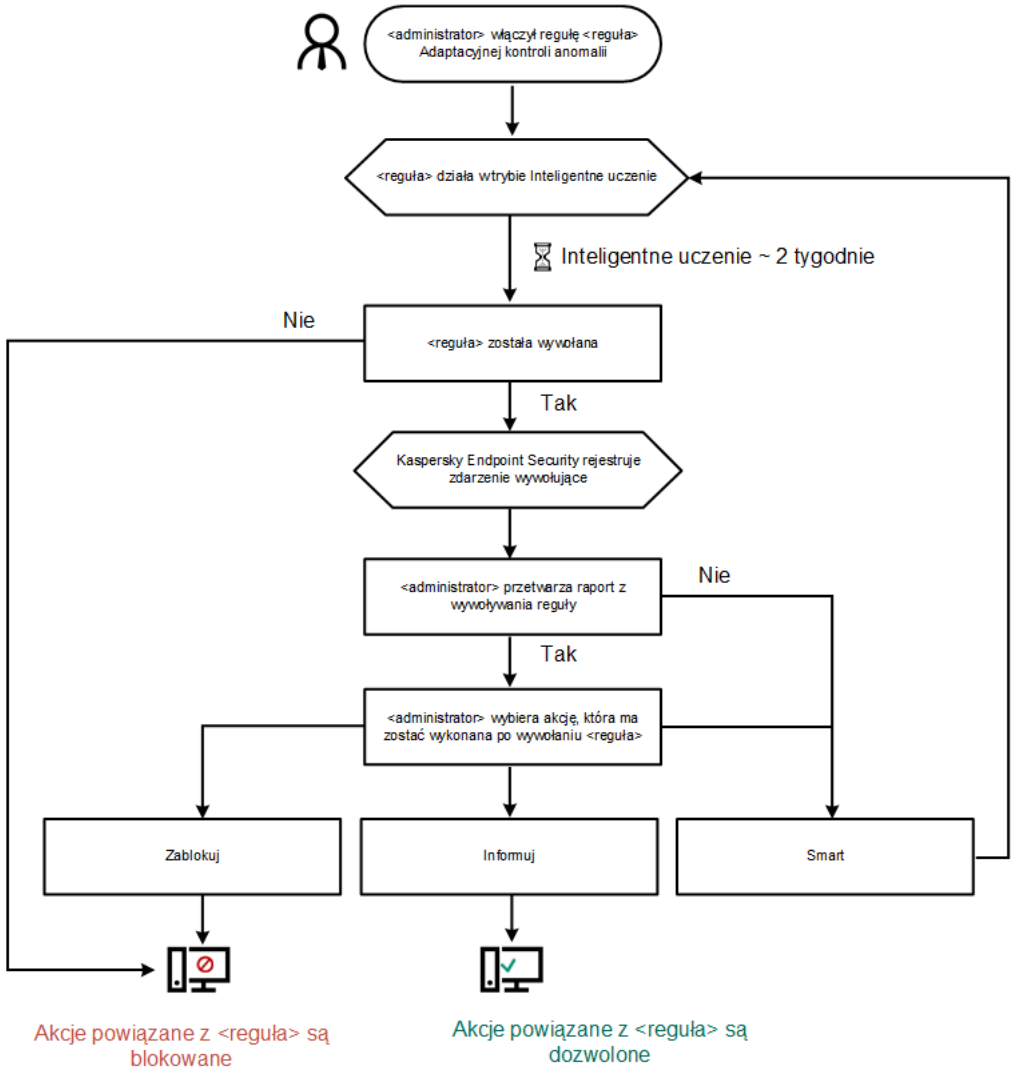
Jeśli złośliwa aplikacja spróbuje wykonać akcję, Kaspersky Endpoint Security zablokuje tę akcję i wyświetli powiadomienie (patrz rysunek poniżej).



Powiadomienie Adaptacyjnej kontroli anomalii

Algorytm działania Adaptacyjnej kontoli anomalii

Kaspersky Endpoint Security decyduje, czy zezwolić na lub zablokować działanie skojarzone z regułą opartą o następujący algorytm (patrz rysunek poniżej).



Algorytm działania Adaptacyjnej kontoli anomalii

Uczenie modułu Adaptacyjna kontrola anomalii

Adaptacyjna kontrola anomalii obejmuje zestaw reguł (wzorców zachowań). Po włączeniu Adaptacyjnej kontroli anomalii, jej reguły działają w *trybie uczenia*. Podczas uczenia moduł Adaptacyjna kontrola anomalii monitoruje wyzwalanie reguł i wysyła zdarzenia wyzwalające do Kaspersky Security Center. Adaptacyjna kontrola anomalii nie blokuje działania aplikacji na komputerze, a jedynie informuje administratora. Możesz również ręcznie wybrać akcję, która zostanie wykonana po uruchomieniu reguły Adaptacyjnej kontroli anomalii.

Jak wyświetlić listę reguł Adaptacyjnej kontroli anomalii w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Kontrola zabezpieczeń → Adaptacyjna kontrola anomalii**.
5. Zaznacz pole **Adaptacyjna kontrola anomalii**.
6. Pod **Ustawienia reguł Adaptacyjnej kontroli anomalii**, przejrzyj listę zasad.

   Domyślnie wszystkie reguły działają w trybie **Inteligentny**.
7. W razie potrzeby potwierdź aktualizację reguły Adaptacyjnej kontroli anomalii.
8. W razie potrzeby wybierz akcję, która zostanie wykonana po uruchomieniu reguły Adaptacyjnej kontroli anomalii:

   - **Zablokuj**. Jeśli to działanie jest wybrane, reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zablokuje aktywność objętą regułą i zarejestruje wpis zawierający informacje o aktywności.
   - **Poinformuj**. Jeśli to działanie jest wybrane, reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zezwoli na aktywność objętą regułą i zarejestruje wpis zawierający informacje o aktywności.
9. W razie potrzeby wyłącz reguły, których nie chcesz używać.
10. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak przeglądać reguły Adaptacyjnej kontroli anomalii w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń → Adaptacyjna kontrola anomalii**.
5. Włącz przełącznik **Adaptacyjna kontrola anomalii WŁĄCZONA**.

6. Pod **Reguły**, przejrzyj listę zasad.

   Domyślnie wszystkie reguły działają w trybie **Inteligentny**.

7. W razie potrzeby potwierdź aktualizację reguły Adaptacyjnej kontroli anomalii.

8. W razie potrzeby wybierz akcję, która zostanie wykonana po uruchomieniu reguły Adaptacyjnej kontroli anomalii:

   - **Zablokuj**. Jeśli to działanie jest wybrane, reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zablokuje aktywność objętą regułą i zarejestruje wpis zawierający informacje o aktywności.

   - **Powiadom**. Jeśli to działanie jest wybrane, reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zezwoli na aktywność objętą regułą i zarejestruje wpis zawierający informacje o aktywności.

9. W razie potrzeby wyłącz reguły, których nie chcesz używać.

10. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak wyświetlić listę reguł Adaptacyjnej kontroli anomalii w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.

3. Włącz przełącznik **Adaptacyjna kontrola anomalii**.

4. W sekcji **Reguły** kliknij odnośnik **Edytuj reguły**.

   Zostanie otwarta lista Reguła Adaptacyjnej kontroli anomalii. Domyślnie wszystkie reguły działają w trybie **Inteligentny**.

5. W razie potrzeby potwierdź aktualizację reguły Adaptacyjnej kontroli anomalii.

6. W razie potrzeby wybierz akcję, która zostanie wykonana po uruchomieniu reguły Adaptacyjnej kontroli anomalii:

   - **Zablokuj**. Jeśli to działanie jest wybrane, reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zablokuje aktywność objętą regułą i zarejestruje wpis zawierający informacje o aktywności.

   - **Poinformuj**. Jeśli to działanie jest wybrane, reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zezwoli na aktywność objętą regułą i zarejestruje wpis zawierający informacje o aktywności.

7. W razie potrzeby wyłącz reguły, których nie chcesz używać.

8. Zapisz swoje zmiany.

Każda reguła ma swój czas trwania trybu uczenia. Czas trwania trybu uczenia jest ustawiany przez ekspertów z Kaspersky. Zazwyczaj tryb uczenia jest aktywny przez dwa tygodnie.

Jeżeli podczas trybu uczenia reguła nigdy nie została wyzwolona, Adaptacyjna kontrola anomalii uznaje takie zachowanie za nietypowe i zmienia status reguły na **Inteligentne blokowanie**. Następnie aplikacja blokuje każdą aktywność zgodną z tą regułą.

Jeśli w trakcie trybu uczenia zostanie wyzwolona reguła, należy ręcznie skonfigurować akcję, którą aplikacja zastosuje do wykrytej aktywności zgodnej z tą regułą. Jeśli nie wybierzesz akcji po wyzwoleniu reguły, Adaptacyjna kontrola anomalii będzie kontynuować działanie w trybie uczenia się.

Włączanie i wyłączanie reguły Adaptacyjnej kontroli anomalii

W celu włączenia lub wyłączenia reguły Adaptacyjnej kontroli anomalii:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. W sekcji **Reguły** kliknij przycisk **Edytuj reguły**.
   Zostanie otwarta lista Reguła Adaptacyjnej kontroli anomalii.
4. W tabeli wybierz zestaw reguł (na przykład: *Aktywność aplikacji biurowych*) i rozwiń zestaw.
5. Wybierz regułę (na przykład: *Uruchomienie procesora poleceń Microsoft Office z aplikacji biurowej*).
6. Użyj przełącznika w kolumnie **Stan**, aby włączyć lub wyłączyć regułę Adaptacyjnej kontroli anomalii.
7. Zapisz swoje zmiany.

Modyfikowanie akcji podejmowanej w momencie wyzwolenia reguły Adaptacyjnej kontroli anomalii

W celu zmodyfikowania akcji podejmowanej w momencie wyzwolenia reguły Adaptacyjnej kontroli anomalii:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. W sekcji **Reguły** kliknij przycisk **Edytuj reguły**.
   Zostanie otwarta lista Reguła Adaptacyjnej kontroli anomalii.
4. Wybierz regułę w tabeli.
5. Kliknij **Edytuj**.
   Zostanie otwarte okno właściwości reguły Adaptacyjnej kontroli anomalii.

6. W sekcji **Akcja** wybierz jedną z następujących opcji:

   - **Inteligentny**. Jeśli ta opcja jest zaznaczona, reguły Adaptacyjnej kontroli anomalii działa w trybie Inteligentne uczenie się przez czas zdefiniowany przez ekspertów z Kaspersky. W tym trybie, gdy reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zezwoli na aktywność objętą regułą i zarejestruje wpis w magazynie **Wyzwalacze reguł w Trybie inteligentnego uczenia** Serwera administracyjnego Kaspersky Security Center. Jeśli przedział czasu ustawiony dla trybu Inteligentne uczenie się zostanie zakończony, Kaspersky Endpoint Security zablokuje aktywność objęta regułą Adaptacyjna kontrola anomalii i zarejestruje wpis zawierający informacje o aktywności.

   - **Zablokuj**. Jeśli to działanie jest wybrane, reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zablokuje aktywność objętą regułą i zarejestruje wpis zawierający informacje o aktywności.

   - **Poinformuj**. Jeśli to działanie jest wybrane, reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zezwoli na aktywność objętą regułą i zarejestruje wpis zawierający informacje o aktywności.

7. Zapisz swoje zmiany.

Tworzenie wykluczeń dla reguły Adaptacyjnej kontroli anomalii

Nie możesz utworzyć więcej niż 1 000 wykluczeń dla reguł Adaptacyjnej kontroli anomalii. Nie jest zalecane tworzenie więcej niż 200 wykluczeń. Aby zmniejszyć liczbę używanych wykluczeń, zalecane jest używanie masek w ustawieniach wykluczeń.

Wykluczenie dla reguły Adaptacyjnej kontroli anomalii zawiera opis obiektów źródłowych i docelowych. *Obiekt źródłowy* to obiekt wykonujący działania. *Obiekt docelowy* to obiekt, na którym wykonywane są działania. Na przykład, otworzyłeś plik o nazwie `file.xlsx`. W rezultacie plik biblioteki z rozszerzeniem DLL jest załadowywany do pamięci komputera. Ta biblioteka jest używana przez przeglądarkę (plik wykonywalny o nazwie `browser.exe`). W tym przykładzie `file.xlsx` to obiekt źródłowy, Excel to proces źródłowy, `browser.exe` to obiekt docelowy, a Browser to proces docelowy.

W celu utworzenia wykluczenia dla reguły Adaptacyjnej kontroli anomalii:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.

3. W sekcji **Reguły** kliknij przycisk **Edytuj reguły**.

   Zostanie otwarta lista Reguła Adaptacyjnej kontroli anomalii.

4. Wybierz regułę w tabeli.

5. Kliknij **Edytuj**.

   Zostanie otwarte okno właściwości reguły Adaptacyjnej kontroli anomalii.

6. W sekcji **Wykluczenia** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno właściwości wykluczenia.

7. Wybierz użytkownika, dla którego chcesz skonfigurować wykluczenie.

Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

> Adaptacyjna kontrola anomalii nie obsługuje wykluczeń dla grup użytkowników. Jeśli wybierzesz grupę użytkowników, Kaspersky Endpoint Security nie stosuje wykluczenia.

8. W polu **Opis** wprowadź opis wykluczenia.

9. Zdefiniuj ustawienia obiektu źródłowego lub procesu źródłowego uruchomionego przez obiekt:

   - **Proces źródłowy**. Ścieżka lub maska ścieżki do pliku lub folderu zawierającego pliki (na przykład: `C:\Dir\File.exe` lub `Dir\*.exe`).
   - **Suma kontrolna procesu źródłowego**. suma kontrolna SHA256 pliku
   - **Obiekt źródłowy**. Ścieżka lub maska ścieżki do pliku lub folderu zawierającego pliki (na przykład: `C:\Dir\File.exe` lub `Dir\*.exe`). Na przykład, ścieżka do pliku `document.docm`, która wykorzystuje skrypt lub makro do uruchamiania procesów docelowych.

     Możesz także określić inne obiekty, które powinny zostać wykluczone, takie jak adres internetowy, makra, polecenie w wierszu polecenia, ścieżka do rejestru lub inne. Określ obiekt zgodnie z następującym szablonem: `object://<object>` gdzie `<object>` odnosi się do nazwy obiektu, na przykład, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Można też użyć masek, na przykład, `object://*C:\Windows\temp\*`.
   - **Suma kontrolna obiektu źródłowego**. suma kontrolna SHA256 pliku

   Reguła Adaptacyjnej kontroli anomalii nie jest stosowana do działań wykonywanych przez obiekt lub do procesów uruchomionych przez obiekt.

10. Określ ustawienia obiektu docelowego lub procesów docelowych uruchomionych na obiekcie.

    - **Proces docelowy**. Ścieżka lub maska ścieżki do pliku lub folderu zawierającego pliki (na przykład: `C:\Dir\File.exe` lub `Dir\*.exe`).
    - **Suma kontrolna procesu docelowego**. suma kontrolna SHA256 pliku
    - **Obiekt docelowy**. Polecenie uruchamiające proces docelowy. Określ polecenie, używając następującego wzoru `object://<command>`, na przykład: `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Można też użyć masek, na przykład, `object://*C:\Windows\temp\*`.
    - **Suma kontrolna obiektu docelowego**. suma kontrolna SHA256 pliku

    Reguła Adaptacyjnej kontroli anomalii nie jest stosowana do działań podejmowanych na obiekcie lub do procesów uruchomionych na obiekcie.

11. Zapisz swoje zmiany.

Eksportowanie i importowanie wykluczeń dla reguł Adaptacyjnej kontroli anomalii

W celu wyeksportowania lub zaimportowania listy wykluczeń dla wybranych reguł:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. W sekcji **Reguły** kliknij przycisk **Edytuj reguły**.

   Zostanie otwarta lista Reguła Adaptacyjnej kontroli anomalii.
4. W celu wyeksportowania listy reguł:
   a. Wybierz reguły, których wyjątki chcesz wyeksportować.
   b. Kliknij **Eksportuj**.
   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.
   d. Potwierdź chęć wyeksportowania tylko wybranych wykluczeń lub wyeksportuj całą listę wykluczeń.
   e. Zapisz plik.
5. W celu zaimportowania listy wykluczeń:
   a. Kliknij **Importuj**.
   b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.
   c. Otwórz plik.

      Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
6. Zapisz swoje zmiany.

Stosowanie aktualizacji dla reguł Adaptacyjnej kontroli anomalii

Nowe reguły Adaptacyjnej kontroli anomalii mogą zostać dodane do tabeli reguł, a istniejące reguły Adaptacyjnej kontroli anomalii mogą zostać usunięte z tabeli reguł po zaktualizowaniu antywirusowych baz danych. Kaspersky Endpoint Security rozróżnia reguły Adaptacyjnej kontroli anomalii, które mają zostać usunięte lub dodane do tabeli, jeśli aktualizacja dla tych reguł nie została zastosowana.

Dopóki aktualizacja nie zostanie zastosowana, Kaspersky Endpoint Security wyświetli reguły Adaptacyjnej kontroli anomalii ustawione do usunięcia przez aktualizację w tabeli reguł i przypisze do nich stan *Wyłączono*. Nie jest możliwa zmiana ustawień tych reguł.

W celu zastosowania aktualizacji dla reguł Adaptacyjnej kontroli anomalii:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. W sekcji **Reguły** kliknij przycisk **Edytuj reguły**.

   Zostanie otwarta lista Reguła Adaptacyjnej kontroli anomalii.
4. W otwartym oknie kliknij przycisk **Zatwierdź aktualizacje**.

   Przycisk **Zatwierdź aktualizacje** jest dostępny, jeśli aktualizacja dla reguł Adaptacyjnej kontroli anomalii jest dostępna.
5. Zapisz swoje zmiany.

Modyfikowanie szablonów wiadomości Adaptacyjnej kontroli anomalii

Jeśli użytkownik spróbuje wykonać działanie zablokowane przez Adaptacyjną kontrolę anomalii, Kaspersky Endpoint Security wyświetli komunikat o zablokowaniu potencjalnie szkodliwych działań. Jeżeli użytkownik ma pewność, że działanie zostało zablokowane przez pomyłkę, powinien użyć odnośnika dostępnego w wiadomości w celu przesłania zgłoszenia do administratora lokalnej sieci firmowej.

Dostępne są specjalne szablony wiadomości wysyłanych do administratora na temat blokowania potencjalnie szkodliwych działań. Do zarządzania szablonami wiadomości dostępne są zmienne specjalne (na przykład `%USER_NAME%`). Zmienne umożliwiają stosowanie tego samego szablonu wiadomości na różnych komputerach. Podczas generowania wiadomości program Kaspersky Endpoint Security pobiera wartość zmiennej z ustawień systemu operacyjnego i wstawia ją do wiadomości odpowiedniej dla danego komputera, użytkownika i zdarzenia.

W celu zmodyfikowania szablonu wiadomości:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. W sekcji **Szablony** skonfiguruj szablony dla wiadomości Adaptacyjnej kontroli anomalii:

   - **Wiadomość dotycząca blokowania**. Szablon komunikatu, który jest wyświetlany użytkownikowi po wyzwoleniu reguły komponentu Adaptacyjna kontrola anomalii, która blokuje nietypowe działanie.
   - **Wiadomość do administratora**. Szablon wiadomości dla użytkownika, która może zostać wysłana do lokalnego administratora sieci korporacyjnej, jeśli użytkownik uzna, że zablokowanie jest pomyłką. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania aktywności aplikacji**. Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkownika**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

   Aby dodać zmienną do tekstu szablonu, umieść kursor w odpowiednim miejscu, kliknij przycisk **Dodaj zmienną** i wybierz wymaganą zmienną z listy dostępnych opcji.

Możesz również przywrócić domyślny tekst szablonu za pomocą przycisku **Resetuj**.

4. Zapisz swoje zmiany.

Monitorowanie działania Adaptacyjnej kontroli anomalii

Adaptacyjna kontrola anomalii obejmuje kilka narzędzi monitorujących. Głównym celem monitorowania Adaptacyjnej kontroli anomalii jest konfiguracja komponentu podczas szkolenia.

Raporty komponentu Adaptacyjna kontrola anomalii

Adaptacyjna kontrola anomalii korzysta z następujących raportów:

- **Raport o stanie reguł Adaptacyjnej kontroli anomalii**. Raport zawiera informacje o statusie reguł Adaptacyjnej kontroli anomalii (*Wyłączone*, *Inteligentne uczenie*, *Inteligentne blokowanie*, *Powiadom*, *Zablokuj*). Raport ten umożliwia analizę poziomu szkolenia Adaptacyjnej kontroli anomalii i ocenę liczby reguł, które zostały przełączone z trybu *Inteligentne uczenie* do normalnego trybu pracy (na przykład *Inteligentne blokowanie*).

- **Raport o wywołanych regułach Adaptacyjnej kontroli anomalii**. Raport zawiera informacje o wyzwalaczach reguł. Raport pokazuje również tryb wyzwalania reguły: *Zablokuj* (w tym *Inteligentne blokowanie*) lub *Powiadom*. Raport ten umożliwia ocenę aktywności Adaptacyjnej kontroli anomalii na komputerach użytkowników.

Jak przeglądać raporty Adaptacyjnej kontroli anomalii w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Kontrola zabezpieczeń → Adaptacyjna kontrola anomalii**.

4. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz wyświetlić raport na temat stanu reguł Adaptacyjnej kontroli anomalii, kliknij link **Raport o stanie reguł Adaptacyjnej kontroli anomalii**.

   - Jeśli chcesz wyświetlić raport na temat uruchomionych reguł Adaptacyjnej kontroli anomalii, kliknij link **Raport o wywołanych regułach Adaptacyjnej kontroli anomalii**.

5. Zostanie rozpoczęty proces tworzenia raportu.

   Raport zostanie wyświetlony w nowym oknie.

Jak przeglądać raporty Adaptacyjnej kontroli anomalii w Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Kontrola zabezpieczeń → Adaptacyjna kontrola anomalii**.

5. W sekcji **Reguły** wykonaj jedną z następujących czynności:

   - Jeśli chcesz wyświetlić raport na temat stanu reguł Adaptacyjnej kontroli anomalii, wybierz opcje **Pokaż raport → Stan reguł**.

   - Jeśli chcesz wyświetlić raport na temat wyzwolonych reguł Adaptacyjnej kontroli anomalii, kliknij **Pokaż raport → Wykrycia**.

6. Zostanie rozpoczęty proces tworzenia raportu.

   Raport zostanie wyświetlony w nowym oknie.

Aby generować raporty w konsoli Kaspersky Security Center, należy włączyć przesyłanie danych do Serwera administracyjnego. Przesyłanie danych jest domyślnie włączone.

Jak włączyć przesyłanie danych Adaptacyjnej kontroli anomalii w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Ustawienia ogólne → Raporty i Kopia zapasowa**.

4. W sekcji **Przesyłanie danych do Serwera administracyjnego** kliknij przycisk **Ustawienia**.

5. Zaznacz następujące pola:

   - **Raport o stanie reguł Adaptacyjnej kontroli anomalii**.

   - **Raport o wywołanych regułach Adaptacyjnej kontroli anomalii**.

6. Zapisz swoje zmiany.

Jak włączyć przesyłanie danych Adaptacyjnej kontroli anomalii w Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne → Integracja KSC**.

5. W sekcji **Przesyłanie danych do Serwera administracyjnego** zaznacz następujące pola wyboru:

   - **Raport o stanie reguł Adaptacyjnej kontroli anomalii**.

   - **Raport o wywołanych regułach Adaptacyjnej kontroli anomalii**.

6. Zapisz swoje zmiany.

magazyn Wyzwalacze reguł w Trybie inteligentnego uczenia

W trybie szkolenia Adaptacyjna kontrola anomalii wysyła informacje o wyzwolonych regułach do oddzielnego magazynu - **Wyzwalacze reguł w Trybie inteligentnego uczenia**. Informacje o wyzwolonych regułach są przedstawiane w magazynie w postaci listy zdarzeń. Aby dostosować Adaptacyjną kontrolę anomalii, możesz potwierdzić nietypowe zachowanie na komputerze lub dodać wykluczenie z reguły.

Zdarzenia komponentu Adaptacyjna kontrola anomalii

Adaptacyjna kontrola anomalii rejestruje zdarzenia wyzwalające reguły w trybach *Zablokuj* (w tym *Inteligentne blokowanie*) i *Powiadom*. W tym celu przewidziano następujące zdarzenia:

Zablokowano akcję procesu

Pominięto akcję procesu

Zdarzenia zawierają informacje o podejrzanej aktywności, w tym o sumach kontrolnych plików, zaangażowanych użytkownikach, czasie wyzwolenia reguły i nazwie komputera. Po przeanalizowaniu zdarzenia możesz natychmiast dodać wykluczenia z reguły, jeśli uznasz, że działanie jest poprawne.

Kontrola aplikacji

Kontrola aplikacji zarządza uruchamianiem aplikacji na komputerach użytkowników. Pozwala to na wdrożenie polityki bezpieczeństwa firmy podczas korzystania z aplikacji. Kontrola aplikacji zmniejsza także ryzyko infekcji komputera poprzez ograniczenie dostępu do aplikacji.

Konfiguracja Kontroli aplikacji obejmuje następujące kroki:

1. Tworzenia kategorii aplikacji.

   Administrator tworzy kategorie aplikacji, którymi chce zarządzać. Kategorie aplikacji są przeznaczone dla wszystkich komputerów w sieci firmowej, niezależnie od grup administracyjnych. Aby utworzyć kategorię, możesz użyć następujących kryteriów: kategoria KL (na przykład: *Przeglądarki*), skrót pliku, dostawca aplikacji i inne kryteria.

2. Tworzenie reguł Kontroli aplikacji.

   Administrator tworzy reguły Kontroli aplikacji w zasadzie dla grupy administracyjnej. Reguła obejmuje kategorie aplikacji i stan uruchamiania aplikacji z tych kategorii: zablokowane lub dozwolone. Administrator może utworzyć wiele reguł. Jeden wniosek może spełniać kryteria wielu zasad. Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Kaspersky Endpoint Security sprawdza, czy aplikacja pasuje do reguły przy każdym uruchomieniu. Kaspersky Endpoint Security sekwencyjnie porównuje aplikację ze wszystkimi regułami Kontroli aplikacji.

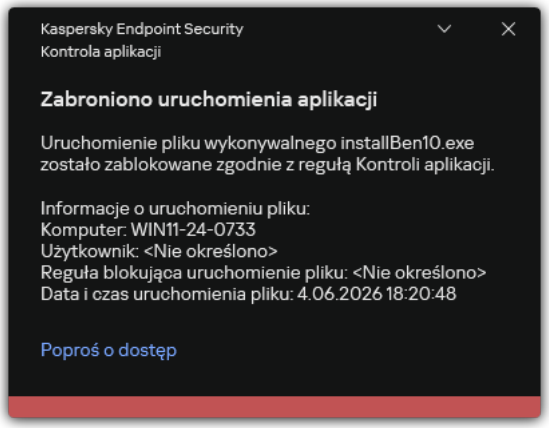
3. Wybieranie trybu Kontroli aplikacji.

   Administrator wybiera tryb pracy z aplikacjami, które nie są uwzględnione w żadnej z reguł (lista zablokowanych i lista zezwolonych).

Jeśli użytkownik spróbuje uruchomić niedozwoloną aplikację, Kaspersky Endpoint Security zablokuje uruchomienie aplikacji i wyświetli powiadomienie (patrz rysunek poniżej).

Tryb testowy służy do sprawdzania konfiguracji Kontroli aplikacji. W tym trybie Kaspersky Endpoint Security wykonuje następujące czynności:

- Umożliwia uruchamianie aplikacji, w tym zabronionych.
- Wyświetla powiadomienie o uruchomieniu zabronionej aplikacji i dodaje informacje do raportu na komputerze użytkownika.
- Wysyła dane o uruchomieniu zabronionych aplikacji do Kaspersky Security Center.



Powiadomienie Kontroli aplikacji

Tryby działania Kontroli aplikacji

Komponent Kontrola aplikacji działa w dwóch trybach:

- **Lista zablokowanych**. W tym trybie Kontrola aplikacji umożliwia użytkownikom uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji zabronionych w regułach Kontroli aplikacji.

  Ten tryb jest włączony domyślnie.

- **Lista zezwolonych**. W tym trybie Kontrola aplikacji blokuje użytkownikom możliwość uruchamiania dowolnych aplikacji, za wyjątkiem aplikacji, które są dozwolone i nie są zabronione w regułach Kontroli aplikacji.

  Jeżeli reguły zezwalające Kontroli aplikacji zostaną w pełni skonfigurowane, moduł zablokuje uruchamianie wszystkich nowych aplikacji, które nie zostały zweryfikowane przez administratora sieci LAN, natomiast zezwoli na działanie systemu operacyjnego i zaufanych aplikacji potrzebnych użytkownikom w ich pracy.

  Możesz przeczytać zalecenia odnośnie konfiguracji reguł Kontroli aplikacji w trybie listy zezwolonych.

Moduł Kontrola aplikacji można skonfigurować do pracy w tych trybach, korzystając z lokalnego interfejsu Kaspersky Endpoint Security oraz programu Kaspersky Security Center.

Jednakże Kaspersky Security Center oferuje narzędzia, które nie są dostępne w lokalnym interfejsie Kaspersky Endpoint Security, a które są potrzebne do:

- Tworzenia kategorii aplikacji.

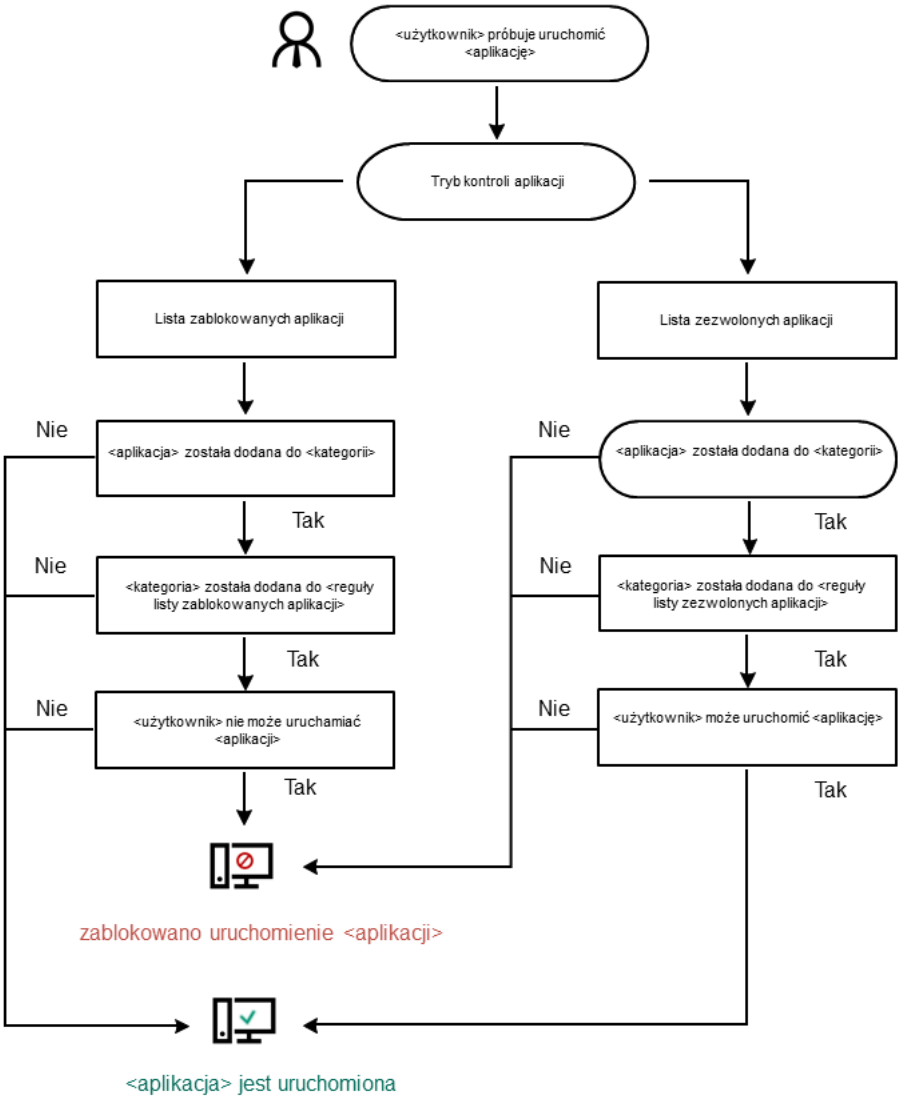
  Reguły Kontroli aplikacji utworzone w Konsoli administracyjnej Kaspersky Security Center są oparte o niestandardowe kategorie aplikacji, a nie o warunki włączenia i wykluczenia, jak ma to miejsce w przypadku lokalnego interfejsu Kaspersky Endpoint Security.

- Otrzymywania informacji o aplikacjach zainstalowanych na komputerach w korporacyjnej sieci LAN.

Dlatego zalecane jest korzystanie z Kaspersky Security Center podczas konfigurowania działania modułu Kontrola aplikacji.

Algorytm działania Kontroli aplikacji

Kaspersky Endpoint Security wykorzystuje algorytm do podjęcia decyzji o uruchomieniu aplikacji (patrz rysunek poniżej).



Algorytm działania Kontroli aplikacji

Ograniczenia funkcjonalności Kontroli aplikacji

Działanie komponentu Kontrola aplikacji jest ograniczone w następujących przypadkach:

- Jeśli wersja aplikacji zostanie zaktualizowana, importowanie ustawień komponentu Kontrola aplikacji nie będzie obsługiwane.
- Jeśli nie ma połączenia z serwerami KSN, Kaspersky Endpoint Security pobiera informacje o reputacji aplikacji i ich modułach z lokalnych baz danych.

  Lista aplikacji, które Kaspersky Endpoint Security wskazuje jako kategorię KL **Inne oprogramowanie\Aplikacje zaufane zgodnie z reputacją w KSN**, może różnić się w zależności od tego, czy połączenie z serwerami KSN jest dostępne.

- Baza danych Kaspersky Security Center może przechowywać do 150 000 wpisów o przetworzonych plikach. Po osiągnięciu tej liczby wpisów, nowe pliki nie będą przetwarzane. Aby wznowić te działania, należy usunąć pliki, które były wcześniej przechowywane w bazie danych Kaspersky Security Center, z komputera, na którym jest zainstalowany program Kaspersky Endpoint Security.
- Komponent nie kontroluje uruchamiania skryptów, dopóki skrypt jest wysyłany do interpretera za pośrednictwem wiersza poleceń.

  Jeśli uruchamianie interpretera jest dozwolone w regułach Kontroli aplikacji, komponent nie zablokuje uruchomienia skrypt z tego interpretera.

  Jeśli uruchomienie przynajmniej jednego ze skryptów określonych w wierszu poleceń interpretera zostanie zablokowane przez reguły Kontroli aplikacji, komponent zablokuje wszystkie skrypty, określone w wierszu poleceń interpretera.

- Komponent nie kontroluje uruchamiania skryptów z interpreterów, które nie są obsługiwane przez Kaspersky Endpoint Security.

  Kaspersky Endpoint Security obsługuje następujące interpretery:

  - Java
  - PowerShell

  Obsługiwane są następujące typy interpreterów:

  - %ComSpec%
  - %SystemRoot%\system32\regedit.exe
  - %SystemRoot%\regedit.exe
  - %SystemRoot%\system32\regedt32.exe
  - %SystemRoot%\system32\cscript.exe

- %SystemRoot%\system32\wscript.exe
- %SystemRoot%\system32\msiexec.exe
- %SystemRoot%\system32\mshta.exe
- %SystemRoot%\system32\rundll32.exe
- %SystemRoot%\system32\wwahost.exe
- %SystemRoot%\syswow64\cmd.exe
- %SystemRoot%\syswow64\regedit.exe
- %SystemRoot%\syswow64\regedt32.exe
- %SystemRoot%\syswow64\cscript.exe
- %SystemRoot%\syswow64\wscript.exe
- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

Otrzymywanie informacji o aplikacjach zainstalowanych na komputerach użytkowników

Aby utworzyć optymalne reguły Kontroli aplikacji, najpierw należy zastanowić się, które aplikacje są używane na komputerach w korporacyjnej sieci LAN. W tym celu można wykorzystać następujące informacje o:

- Producentach, wersjach i lokalizacjach aplikacji używanych w firmowej sieci LAN.
- Częstotliwości aktualizacji aplikacji.
- Zasadach korzystania z aplikacji (mogą to być zasady zabezpieczeń lub zasady administracyjne).
- Lokalizacji magazynu pakietów dystrybucyjnych aplikacji.

Przeglądanie informacji o aplikacji

Informacje o zainstalowanych aplikacjach są dostarczane przez Agenta sieciowego Kaspersky Security Center. Informacje o zainstalowanych aplikacjach są dostępne w folderze **Rejestr aplikacji** konsoli Kaspersky Security Center. Agent sieciowy aktualizuje informacje przy każdej synchronizacji z konsolą Kaspersky Security Center. Więcej informacji na temat danych wysłanych przez Agenta sieciowego można znaleźć w pomocy do Kaspersky Security Center.

W celu otwarcia okna właściwości aplikacji w folderze Rejestr aplikacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz opcje **Zaawansowane** → **Zarządzanie aplikacjami** → **Rejestr aplikacji**.
3. Wybierz aplikację.
4. Z menu kontekstowego aplikacji wybierz **Właściwości**.

Wyświetlanie informacji o plikach wykonywalnych

Można zmniejszyć obciążenie bazy danych podczas wyszukiwania informacji o plikach wykonywalnych. W tym celu zalecamy uruchomienie zadania *Inwentaryzacja* na kilku komputerach porównawczych, na których zainstalowano standardowy zestaw oprogramowania.

Listę plików wykonywalnych można uzyskać za pomocą zadania *Inwentaryzacja* programu Kaspersky Endpoint Security. W folderze **Pliki wykonywalne** można sprawdzić listę plików wykonywalnych Kaspersky Security Center.

Przed uruchomieniem zadania *Inwentaryzacja* upewnij się, że baza danych spełnia zalecenia Kaspersky Security Center. Szczegółowe informacje na temat ograniczeń bazy danych znajdują się w pomocy do Kaspersky Security Center.

Jak uruchomić zadanie Inwentaryzacja w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Inwentaryzacja**.

Krok 2. Obszar inwentaryzacji

Utwórz listę folderów, w których program Kaspersky Endpoint Security ma szukać plików wykonywalnych. Skonfiguruj ustawienia inwentaryzacji (patrz tabela poniżej).

Krok 3. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 4. Wybieranie konta do uruchomienia zadania

Wybierz konto, aby uruchomić zadanie *Inwentaryzacja*. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika. Jeśli obszar inwentaryzacji obejmuje dyski sieciowe lub inne obiekty z ograniczonym dostępem, wybierz konto użytkownika z wystarczającymi uprawnieniami dostępu.

Krok 5. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz zadania, na przykład ręcznie.

Krok 6. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład *Podstawowa inwentaryzacja*.

Krok 7. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania. Dzięki temu na komputerach użytkowników przeprowadzane jest wyszukiwanie plików wykonywalnych zgodnie ze skonfigurowanym harmonogramem.

Jak w konsoli Web Console i Cloud Console uruchomić zadanie Inwentaryzacja

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Inwentaryzacja**.

   c. W polu **Nazwa zadania** wprowadź krótki opis, na przykład, *Podstawowa inwentaryzacja*.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.

5. Wybierz konto do uruchomienia zadania. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika.

6. Zakończ działanie Kreatora.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Aby skonfigurować zadanie, przejdź do właściwości zadania (patrz poniższa tabela).

8. Zaznacz pole obok zadania.

9. Kliknij **Uruchom**.

   Możesz monitorować stan zadania oraz liczbę urządzeń, na których to zadanie zostało wykonane pomyślnie lub zakończyło się błędem. W wyniku tego działania wyszukiwanie plików wykonywalnych zostanie wykonane na komputerach użytkowników zgodnie z określonym harmonogramem.

Ustawienia inwentaryzacji

Parametr	Opis
Zakres inwentaryzacji	Lista obiektów, które będą stanowić obszar inwentaryzacji.
Inwentaryzacja modułów DLL	Kaspersky Endpoint Security wyszukuje moduły DLL w obszarze inwentaryzacji i wysyła informacje do Kaspersky Security Center. Włączenie inwentaryzacji modułów DLL znacznie wydłuża czas wykonywania zadania inwentaryzacji i zwiększa rozmiar bazy danych.
Inwentaryzacja plików skryptu	Kaspersky Endpoint Security wyszukuje skrypty w obszarze inwentaryzacji i wysyła informacje do Kaspersky Security Center. Włączenie inwentaryzacji skryptów znacznie wydłuża czas wykonywania zadania inwentaryzacji i zwiększa rozmiar bazy danych.
Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności	Odroczono uruchomienie zadania, gdy zasoby komputera są zajęte. Kaspersky Endpoint Security uruchamia zadanie skanowania, jeśli komputer jest zablokowany lub wygaszacz ekranu jest włączony. Jeśli przerwałeś wykonywanie zadania, na przykład, poprzez odblokowanie komputera, Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane. Ta opcja terminarza umożliwia zaoszczędzenie zasobów komputera w trakcie korzystania z komputera.
Skanuj tylko nowe i zmienione pliki	Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.
Pomiń plik skanowany dłużej niż (sek.) N sek	Ograniczenie czasu wykonywania zadania. Po określonym czasie Kaspersky Endpoint Security zatrzyma zadanie. Zadanie nie zostanie oznaczone jako zakończone. Następnym razem, gdy Kaspersky Endpoint Security uruchomi zadanie, zostanie ono uruchomione od początku i zgodnie z terminarzem.
Skanuj archiwa	Skanowanie ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE i innych archiwów. Aplikacja skanuje archiwa nie tylko według rozszerzenia, ale także według formatu. Podczas sprawdzania archiwów aplikacja przeprowadzi cykliczne rozpakowywanie. Pozwala to na wykrywanie zagrożeń w archiwach wielopoziomowych (archiwach wewnątrz archiwów).

Parametr	Opis
Skanuj pakiety dystrybucyjne	Skanowanie pakietów dystrybucyjnych aplikacji firm trzecich.
Nie rozpakowuj dużych plików złożonych	Jeżeli to pole jest zaznaczone, aplikacja nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość. Jeśli pole nie jest zaznaczone, aplikacja skanuje pliki złożone o wszystkich rozmiarach. Aplikacja skanuje pliki o dużych rozmiarach, które zostają wypakowane z archiwów niezależnie od tego, czy pole jest zaznaczone.

W celu otwarcia okna właściwości dla pliku wykonywalnego w folderze Pliki wykonywalne:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz opcje **Zaawansowane → Zarządzanie aplikacjami → Pliki wykonywalne**.
3. Wybierz plik wykonywalny.
4. Z otwartego menu kontekstowego pliku wykonywalnego wybierz **Właściwości**.

Aby przejrzeć ogólne informacje o aplikacji i jej plikach wykonywalnych oraz listę komputerów, na których jest zainstalowana aplikacja, otwórz okno właściwości aplikacji wybranej w folderze **Rejestr aplikacji** lub w folderze **Pliki wykonywalne**.

Aktualizowanie informacji o zainstalowanych aplikacjach i plikach wykonywalnych

Począwszy od Kaspersky Endpoint Security 12.3 for Windows, działanie komponentu Kontrola aplikacji z bazą danych plików wykonywalnych jest zoptymalizowane. Kaspersky Endpoint Security 12.3 for Windows automatycznie aktualizuje bazę danych po usunięciu pliku z komputera. Umożliwia to aktualizowanie bazy danych i oszczędzanie zasobów Kaspersky Security Center.

Aby baza danych zainstalowanych aplikacji była aktualna, musi być włączone wysyłanie informacji o aplikacji do Serwera administracyjnego (domyślnie włączone).

Włączanie przesyłania informacji o aplikacji w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne → Raporty i Kopia zapasowa**.
4. W sekcji **Przesyłanie danych do Serwera administracyjnego** kliknij przycisk **Ustawienia**.
5. Zaznacz pole **Uruchomione aplikacje**.
6. Zapisz swoje zmiany.

Aktywacja aplikacji w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Integracja KSC**.
5. W sekcji **Przesyłanie danych do Serwera administracyjnego** kliknij przycisk **Ustawienia zaawansowane**.
6. W otwartym oknie zaznacz pole **O uruchomionych aplikacjach**.
7. Zapisz swoje zmiany.

Jak włączyć tryb zablokowanych aplikacji?

Tryb *Blokowane aplikacje* to tryb, w którym Kontrola aplikacji umożliwia użytkownikom uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji zabronionych w regułach Kontroli aplikacji. Oznacza to, że jeśli nie istnieje żadna reguła odmowy, Kontrola aplikacji zezwala na uruchomienie aplikacji. Ten tryb jest włączony domyślnie.

Przed włączeniem trybu *Blokowane aplikacje* zalecamy przetestowanie reguł Kontroli aplikacji. W tym celu możesz włączyć tryb testowy.

Jak wybrać tryb zablokowanych aplikacji w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
5. Zaznacz pole **Kontrola aplikacji**.
6. W sekcji **Ustawienia Kontroli aplikacji** użyj listy rozwijalnej **Tryb kontroli**, aby wybrać **Lista zablokowanych**.
7. Z listy rozwijalnej **Akcja** wybierz akcję dla Kontroli aplikacji:

   - **Przetestuj reguły**. Kontrola aplikacji nie blokuje aplikacji, których uruchomienie jest zabronione przez reguły, ale generuje zdarzenia dotyczące uruchomienia aplikacji, które w innym przypadku zostałyby zablokowane.
   - **Zastosuj reguły**. Kontrola aplikacji blokuje zablokowane aplikacje i generuje odpowiednie zdarzenia.

8. Wybierz status reguł Kontroli aplikacji:

   - **Włączona**. Ten stan oznacza, że przy włączonym komponencie Kontrola aplikacji reguła ta jest wykorzystywana.
   - **Wyłączona**. Ten stan oznacza, że reguła jest ignorowana, gdy działa komponent Kontrola aplikacji.
   - **Sprawdź**. Ten stan oznacza, że Kaspersky Endpoint Security zawsze zezwala na uruchamianie aplikacji, do których reguła jest stosowana, ale zapisuje informacje o uruchamianiu takich aplikacji w raporcie.

   Jeśli to konieczne, dodaj nowe reguły Kontroli aplikacji.

9. Skonfiguruj ustawienia zaawansowane Kontroli aplikacji:

   - **Monitoruj ładowanie modułów DLL (znacznie zwiększa obciążenie systemu)**. Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security kontroluje wczytywanie modułów DLL, gdy użytkownicy próbują uruchomić aplikacje. Informacja na temat modułu DLL i aplikacji, która załadowała ten moduł DLL, jest zapisywana w raporcie.

     Po włączeniu funkcji kontrolowania wczytywania modułów DLL i sterowników, upewnij się, że w ustawieniach Kontroli aplikacji włączona jest jedna z następujących reguł: domyślna reguła **Obraz systemu** lub inna reguła, która zawiera kategorię KL „**Obraz systemu\Zaufane certyfikaty**” i zapewnia, że moduły DLL i sterowniki są ładowane przed uruchomieniem Kaspersky Endpoint Security. Włączanie kontroli ładowania modułów DLL i sterowników, gdy reguła **Obraz systemu** jest wyłączona, może spowodować niestabilność systemu operacyjnego.

     Kaspersky Endpoint Security monitoruje tylko moduły DLL i sterowniki ładowane po zaznaczeniu pola. Po zaznaczeniu pola zalecane jest ponowne uruchomienie komputera w celu zapewnienia, że aplikacja monitoruje wszystkie sterowniki i moduły DLL, w tym te załadowane przed uruchomieniem Kaspersky Endpoint Security.

   - **Używaj ścisłej weryfikacji podpisem cyfrowym**. Można wybrać certyfikat jako warunek wyzwalający regułę kontroli aplikacji. Jeśli to pole wyboru jest zaznaczone, Kaspersky Endpoint Security stosuje reguły do aplikacji podpisanych certyfikatami wyłącznie z zaufanych systemowych magazynów certyfikatów. Aplikacje podpisane takim certyfikatem są także uznawane za zaufane przez komponenty ochrony, na przykład zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Jeśli jednak w regule kontroli aplikacji określisz certyfikat z innego magazynu, Kaspersky Endpoint Security nie zastosuje takiej reguły.

     Jeśli pole wyboru nie jest zaznaczone, Kaspersky Endpoint Security stosuje reguły do aplikacji podpisanych certyfikatem z Trusted Root Certificate Store systemu Windows. Takie aplikacje nie należą do strefy zaufanej. Komponenty ochrony monitorują aktywność takich aplikacji.

   - **Wiadomość dotycząca blokowania**. Szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła Kontroli aplikacji, która blokuje uruchamianie aplikacji.
   - **Wiadomość do administratora**. Szablon wiadomości, którą użytkownik może wysłać do administratora korporacyjnej sieci LAN, jeśli uważa, że aplikacja została przypadkowo zablokowana.

10. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć tryb zablokowanych aplikacji w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
5. Włącz przełącznik **Kontrola aplikacji WŁĄCZONA**.
6. W bloku **Tryb działania** wybierz **Blokuj wszystko poza listą reguł**.
7. W sekcji **Akcja** wybierz akcję dla Kontroli aplikacji:
   - **Poinformuj**. Kontrola aplikacji nie blokuje aplikacji, których uruchomienie jest zabronione przez reguły, ale generuje zdarzenia dotyczące uruchomienia aplikacji, które w innym przypadku zostałyby zablokowane.
   - **Zastosuj reguły**. Kontrola aplikacji blokuje zablokowane aplikacje i generuje odpowiednie zdarzenia.
8. Wybierz status reguł Kontroli aplikacji:
   - **Włączono**. Ten stan oznacza, że przy włączonym komponencie Kontrola aplikacji reguła ta jest wykorzystywana.
   - **Wyłączono**. Ten stan oznacza, że reguła jest ignorowana, gdy działa komponent Kontrola aplikacji.
   - **Tryb testowy**. Ten stan oznacza, że Kaspersky Endpoint Security zawsze zezwala na uruchamianie aplikacji, do których reguła jest stosowana, ale zapisuje informacje o uruchamianiu takich aplikacji w raporcie.

   Jeśli to konieczne, dodaj nowe reguły Kontroli aplikacji.
9. Skonfiguruj ustawienia zaawansowane Kontroli aplikacji:
   - **Monitoruj ładowanie modułów DLL**. Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security kontroluje wczytywanie modułów DLL, gdy użytkownicy próbują uruchomić aplikacje. Informacja na temat modułu DLL i aplikacji, która załadowała ten moduł DLL, jest zapisywana w raporcie.

     Po włączeniu funkcji kontrolowania wczytywania modułów DLL i sterowników, upewnij się, że w ustawieniach Kontroli aplikacji włączona jest jedna z następujących reguł: domyślna reguła **Obraz systemu** lub inna reguła, która zawiera kategorię KL „**Obraz systemu\Zaufane certyfikaty**” i zapewnia, że moduły DLL i sterowniki są ładowane przed uruchomieniem Kaspersky Endpoint Security. Włączanie kontroli ładowania modułów DLL i sterowników, gdy reguła **Obraz systemu** jest wyłączona, może spowodować niestabilność systemu operacyjnego.

     Kaspersky Endpoint Security monitoruje tylko moduły DLL i sterowniki ładowane po zaznaczeniu pola. Po zaznaczeniu pola zalecane jest ponowne uruchomienie komputera w celu zapewnienia, że aplikacja monitoruje wszystkie sterowniki i moduły DLL, w tym te załadowane przed uruchomieniem Kaspersky Endpoint Security.

- **Używaj ścisłej weryfikacji podpisem cyfrowym**. Można wybrać certyfikat jako warunek wyzwalający regułę kontroli aplikacji. Jeśli to pole wyboru jest zaznaczone, Kaspersky Endpoint Security stosuje reguły do aplikacji podpisanych certyfikatami wyłącznie z zaufanych systemowych magazynów certyfikatów. Aplikacje podpisane takim certyfikatem są także uznawane za zaufane przez komponenty ochrony, na przykład zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Jeśli jednak w regule kontroli aplikacji określisz certyfikat z innego magazynu, Kaspersky Endpoint Security nie zastosuje takiej reguły.

  Jeśli pole wyboru nie jest zaznaczone, Kaspersky Endpoint Security stosuje reguły do aplikacji podpisanych certyfikatem z Trusted Root Certificate Store systemu Windows. Takie aplikacje nie należą do strefy zaufanej. Komponenty ochrony monitorują aktywność takich aplikacji.

- **Wiadomość do użytkownika**. Szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła Kontroli aplikacji, która blokuje uruchamianie aplikacji.

- **Wiadomość do administratora**. Szablon wiadomości, którą użytkownik może wysłać do administratora korporacyjnej sieci LAN, jeśli uważa, że aplikacja została przypadkowo zablokowana.

10. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć tryb zablokowanych aplikacji w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

3. Włącz przełącznik **Kontrola aplikacji**.

4. W bloku **Tryb Kontroli uruchamiania aplikacji** wybierz **Lista zablokowanych. Dozwolone są wszystkie aplikacja za wyjątkiem tych znajdujących się na liście reguł**.

5. W sekcji **Akcja wykonywana podczas uruchamiania aplikacji zablokowanych przez reguły** wybierz akcję dla Kontroli aplikacji:

   - **Informuj (tryb testowy) i rejestruj zdarzenia w raport**. Kontrola aplikacji nie blokuje aplikacji, których uruchomienie jest zabronione przez reguły, ale generuje zdarzenia dotyczące uruchomienia aplikacji, które w przeciwnym razie zostałyby zablokowane.

   - **Zablokuj**. Kontrola aplikacji blokuje zablokowane aplikacje i generuje odpowiednie zdarzenia.

6. Wybierz status reguł Kontroli aplikacji:

   - **Włączone**. Ten stan oznacza, że przy włączonym komponencie Kontrola aplikacji reguła ta jest wykorzystywana.

   - **Wyłączone**. Ten stan oznacza, że reguła jest ignorowana, gdy działa komponent Kontrola aplikacji.

   - **Tryb testowy**. Ten stan oznacza, że Kaspersky Endpoint Security zawsze zezwala na uruchamianie aplikacji, do których reguła jest stosowana, ale zapisuje informacje o uruchamianiu takich aplikacji w raporcie.

   Jeśli to konieczne, dodaj nowe reguły Kontroli aplikacji.

7. Skonfiguruj ustawienia zaawansowane Kontroli aplikacji:

   - **Monitoruj ładowanie modułów DLL**. Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security kontroluje wczytywanie modułów DLL, gdy użytkownicy próbują uruchomić aplikacje. Informacja na temat modułu DLL i aplikacji, która załadowała ten moduł DLL, jest zapisywana w raporcie.

Po włączeniu funkcji kontrolowania wczytywania modułów DLL i sterowników, upewnij się, że w ustawieniach Kontroli aplikacji włączona jest jedna z następujących reguł: domyślna reguła **Obraz systemu** lub inna reguła, która zawiera kategorię KL „**Obraz systemu\Zaufane certyfikaty**" i zapewnia, że moduły DLL i sterowniki są ładowane przed uruchomieniem Kaspersky Endpoint Security. Włączanie kontroli ładowania modułów DLL i sterowników, gdy reguła **Obraz systemu** jest wyłączona, może spowodować niestabilność systemu operacyjnego.

Kaspersky Endpoint Security monitoruje tylko moduły DLL i sterowniki ładowane po zaznaczeniu pola. Po zaznaczeniu pola zalecane jest ponowne uruchomienie komputera w celu zapewnienia, że aplikacja monitoruje wszystkie sterowniki i moduły DLL, w tym te załadowane przed uruchomieniem Kaspersky Endpoint Security.

- **Używaj ścisłej weryfikacji podpisem cyfrowym**. Można wybrać certyfikat jako warunek wyzwalający regułę kontroli aplikacji. Jeśli to pole wyboru jest zaznaczone, Kaspersky Endpoint Security stosuje reguły do aplikacji podpisanych certyfikatami wyłącznie z zaufanych systemowych magazynów certyfikatów. Aplikacje podpisane takim certyfikatem są także uznawane za zaufane przez komponenty ochrony, na przykład zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Jeśli jednak w regule kontroli aplikacji określisz certyfikat z innego magazynu, Kaspersky Endpoint Security nie zastosuje takiej reguły.

  Jeśli pole wyboru nie jest zaznaczone, Kaspersky Endpoint Security stosuje reguły do aplikacji podpisanych certyfikatem z Trusted Root Certificate Store systemu Windows. Takie aplikacje nie należą do strefy zaufanej. Komponenty ochrony monitorują aktywność takich aplikacji.

- **Szablony wiadomości o blokowaniu aplikacji**. Szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła Kontroli aplikacji, która blokuje uruchamianie aplikacji.

- **Tekst szablonu wiadomości, który jest wyświetlany w momencie zablokowania uruchomienia aplikacji**. Szablon wiadomości, którą użytkownik może wysłać do administratora korporacyjnej sieci LAN, jeśli uważa, że aplikacja została przypadkowo zablokowana.

8. Zapisz swoje zmiany.

W wyniku tego działania Kontrola aplikacji blokuje zablokowane aplikacje. Kaspersky Endpoint Security tworzy także zdarzenia *Zabroniono uruchomienia aplikacji*. Możesz użyć tych zdarzeń, aby wygenerować raport *Raport o zabronionych aplikacjach* w konsoli Kaspersky Security Center. Podsumowanie raportu zawiera listę aplikacji i komputerów, na których została wyzwolona reguła Kontroli aplikacji.

Kontrola aplikacji na podstawie komputera bazowego

Możesz użyć komputera bazowego do utworzenia obrazu z zestawem potrzebnych Ci aplikacji. Następnie możesz użyć tego obrazu, aby wdrożyć system operacyjny i aplikacje na innych komputerach. Aktualizacja obrazu nie zawsze jest możliwa. Komponent Kontrola aplikacji umożliwia prowadzenie listy dozwolonych aplikacji na podstawie komputera bazowego. Kontrola aplikacji automatycznie ustala, które aplikacje są zainstalowane na komputerze bazowym, i aktualizuje kategorię. W ten sposób komputery otrzymują aktualną listę dozwolonych aplikacji.

Konfigurowanie Kontroli aplikacji na podstawie komputera bazowego obejmuje następujące kroki:

1. Tworzenie automatycznie aktualizowanej kategorii. Podczas tworzenia nowej kategorii wybierz kategorię **Kategoria obejmująca pliki wykonywalne z określonego folderu** oraz wybierz komputer bazowy.

Jak utworzyć automatycznie aktualizowaną kategorię w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz opcje **Zaawansowane** → **Zarządzanie aplikacjami** → **Kategorie aplikacji**.
3. W obszarze roboczym kliknij **Nowa kategoria**.

   Spowoduje to uruchomienie Kreatora tworzenia kategorii aplikacji.
4. Postępuj zgodnie z instrukcjami Kreatora tworzenia kategorii aplikacji.

Krok 1. Wybieranie typu kategorii

Wybierz **Kategoria obejmująca pliki wykonywalne z wybranych urządzeń** jako typ kategorii.

Krok 2. Wprowadzanie nazwy kategorii użytkownika

W tym kroku określ nazwę kategorii aplikacji.

Krok 3. Ustawienia

> Ten krok jest dostępny, jeśli wybrałeś typ kategorii **Kategoria zawierająca pliki wykonywalne z wybranych urządzeń**.

W tym kroku kliknij przycisk **Dodaj** i określ komputery, których pliki wykonywalne zostaną dodane do kategorii aplikacji przez Kaspersky Security Center. Wszystkie pliki wykonywalne z określonych komputerów, znajdujące się w folderze **Pliki wykonywalne**, zostaną dodane do kategorii aplikacji przez Kaspersky Security Center.

W tym kroku możesz skonfigurować następujące ustawienia:

- Algorytm obliczania funkcji skrótu. W celu wybrania algorytmu musisz zaznaczyć przynajmniej jedną z następujących opcji:
  - **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)**.
- Pole **Synchronizuj dane z repozytorium Serwera administracyjnego**. Zaznacz to pole, jeśli chcesz, żeby Kaspersky Security Center okresowo czyścił kategorię aplikacji i dodawał do niej wszystkie pliki wykonywalne z określonych komputerów, znajdujących się w folderze **Pliki wykonywalne**.

  Jeśli pole **Synchronizuj dane z repozytorium Serwera administracyjnego** jest odznaczone, Kaspersky Security Center nie wprowadzi żadnych modyfikacji do kategorii aplikacji po jej utworzeniu.

Krok 4. Filtr

W tym kroku skonfiguruj filtr plików.

Możesz określić typ pliku, którego chcesz użyć do utworzenia kategorii aplikacji.

- **Wszystkie pliki**. Kategoria będzie obejmować wszystkie pliki. Ta opcja jest wybrana domyślnie.
- **Tylko pliki spoza kategorii aplikacji**. Kategoria będzie obejmować tylko pliki spoza kategorii aplikacji.

Możesz określić foldery wybranych komputerów zawierające pliki, których chcesz użyć do utworzenia kategorii aplikacji.

- **Wszystkie foldery**. Kategoria będzie obejmować wszystkie foldery. Ta opcja jest wybrana domyślnie.
- **Określony folder**. Kategoria będzie obejmować tylko wskazany folder. Jeśli wybierzesz tę opcję, musisz określić ścieżkę do folderu.

Krok 5. Tworzenie kategorii niestandardowej

Zakończ działanie Kreatora.

Jak utworzyć kategorię z zawartością dodaną automatycznie w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Operacje** → **Aplikacje innych firm** → **Kategorie aplikacji**.

   Spowoduje to otwarcie listy kategorii aplikacji.

2. Kliknij **Dodaj**.

   Spowoduje to uruchomienie Kreatora tworzenia kategorii aplikacji.

3. Skonfiguruj ustawienia ogólne kategorii aplikacji:

   - Nazwa kategorii.
   - Metoda tworzenia kategorii. Wybierz **Kategoria obejmująca pliki wykonywalne z wybranych urządzeń** jako typ kategorii.

   Przejdź do następnego kroku.

4. Skonfiguruj ustawienia zaawansowane kategorii aplikacji:

   - Określ komputery, z których Kaspersky Security Center będzie dodawać pliki wykonywalne do kategorii aplikacji. Wszystkie pliki wykonywalne z określonych komputerów, znajdujące się w folderze **Pliki wykonywalne**, zostaną dodane do kategorii aplikacji przez Kaspersky Security Center.
   - Wybierz algorytm obliczania funkcji skrótu.

- Skonfiguruj interwał synchronizacji danych z pamięcią masową Serwera administracyjnego.
- Skonfiguruj filtr dla plików.

5. Zakończ działanie Kreatora.

Podczas tworzenia automatycznie aktualizowanej kategorii wygodne może okazać się podzielenie plików na wiele kategorii. Na przykład pliki systemu operacyjnego i pliki z folderu Program Files. Aby to zrobić, możesz skorzystać z filtra w ustawieniach kategorii i wybrać poszczególne foldery.

2. Wybieranie trybu Kontroli aplikacji. Musisz uniemożliwić wykonywanie wszystkich aplikacji, którym nie udzielono wyraźnego zezwolenia. W tym celu wybierz tryb *Blokowane aplikacje*.

3. Tworzenie reguły Kontroli aplikacji. W ustawieniach reguły wybierz kategorię, do której należą pliki wykonywalne z komputera bazowego.

Jak skonfigurować Kontrolę aplikacji na podstawie komputera bazowego w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
5. Zaznacz pole **Kontrola aplikacji**.
6. W sekcji **Ustawienia Kontroli aplikacji** użyj listy rozwijalnej **Tryb kontroli**, aby wybrać **Lista zablokowanych**.
7. Z listy rozwijalnej **Akcja** wybierz akcję dla Kontroli aplikacji:
   - **Przetestuj reguły**. Kontrola aplikacji nie blokuje aplikacji, których uruchomienie jest zabronione przez reguły, ale generuje zdarzenia dotyczące uruchomienia aplikacji, które w innym przypadku zostałyby zablokowane.
   - **Zastosuj reguły**. Kontrola aplikacji blokuje zablokowane aplikacje i generuje odpowiednie zdarzenia.
8. Na liście reguł Kontroli aplikacji kliknij przycisk **Dodaj**.

   To spowoduje uruchomienie Kreatora dodawania reguły Kontroli aplikacji.
9. Z listy rozwijanej **Kategoria** wybierz automatycznie aktualizowaną kategorię na podstawie komputera bazowego.
10. Wybierz użytkowników lub grupy użytkowników, do których chcesz zastosować regułę Kontroli aplikacji.

11. Skonfiguruj ustawienia zaawansowane reguły Kontroli aplikacji:

    - **Zabroń innym użytkownikom**. Aplikacja zapobiega uruchamianiu aplikacji należących do wybranej kategorii wszystkim użytkownikom, którzy nie znajdują się na liście.

    - **Zaufane programy aktualizujące**. Kaspersky Endpoint Security uważa aplikacje znajdujące się w wybranej kategorii za zaufane programy aktualizujące mogące tworzyć inne pliki wykonywalne, których uruchomienie będzie dozwolone.

12. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak skonfigurować Kontrolę aplikacji na podstawie komputera bazowego w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

5. Włącz przełącznik **Kontrola aplikacji WŁĄCZONA**.

6. W bloku **Tryb działania** wybierz **Blokuj wszystko poza listą reguł**.

7. W sekcji **Akcja** wybierz akcję dla Kontroli aplikacji:

    - **Poinformuj**. Kontrola aplikacji nie blokuje aplikacji, których uruchomienie jest zabronione przez reguły, ale generuje zdarzenia dotyczące uruchomienia aplikacji, które w innym przypadku zostałyby zablokowane.

    - **Zastosuj reguły**. Kontrola aplikacji blokuje zablokowane aplikacje i generuje odpowiednie zdarzenia.

8. Na liście reguł Kontroli aplikacji kliknij przycisk **Dodaj**.

   To spowoduje uruchomienie Kreatora dodawania reguły Kontroli aplikacji.

9. Pod **Kategorie/Aplikacje** wybierz automatycznie aktualizowaną kategorię na podstawie komputera bazowego.

10. Wybierz użytkowników lub grupy użytkowników, do których chcesz zastosować regułę Kontroli aplikacji.

11. Skonfiguruj ustawienia zaawansowane reguły Kontroli aplikacji:

    - **Użytkownicy**. Aplikacja zapobiega uruchamianiu aplikacji należących do wybranej kategorii wszystkim użytkownikom, którzy nie znajdują się na liście.

    - **Zaufane programy aktualizujące**. Kaspersky Endpoint Security uważa aplikacje znajdujące się w wybranej kategorii za zaufane programy aktualizujące mogące tworzyć inne pliki wykonywalne, których uruchomienie będzie dozwolone.

12. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak skonfigurować Kontrolę aplikacji na podstawie komputera bazowego w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
3. Włącz przełącznik **Kontrola aplikacji**.
4. W bloku **Tryb Kontroli uruchamiania aplikacji** wybierz **Lista zablokowanych. Dozwolone są wszystkie aplikacja za wyjątkiem tych znajdujących się na liście reguł**.
5. W sekcji **Akcja wykonywana podczas uruchamiania aplikacji zablokowanych przez reguły** wybierz akcję dla Kontroli aplikacji:
   - **Informuj (tryb testowy) i rejestruj zdarzenia w raport**. Kontrola aplikacji nie blokuje aplikacji, których uruchomienie jest zabronione przez reguły, ale generuje zdarzenia dotyczące uruchomienia aplikacji, które w przeciwnym razie zostałyby zablokowane.
   - **Zablokuj**. Kontrola aplikacji blokuje zablokowane aplikacje i generuje odpowiednie zdarzenia.
6. Na liście reguł Kontroli aplikacji kliknij przycisk **Dodaj**.

   To spowoduje uruchomienie Kreatora dodawania reguły Kontroli aplikacji.
7. Pod **Kategoria** wybierz automatycznie aktualizowaną kategorię na podstawie komputera bazowego.
8. Wybierz użytkowników lub grupy użytkowników, do których chcesz zastosować regułę Kontroli aplikacji.
9. Skonfiguruj ustawienia zaawansowane reguły Kontroli aplikacji:
   - **Zabroń innym użytkownikom**. Aplikacja zapobiega uruchamianiu aplikacji należących do wybranej kategorii wszystkim użytkownikom, którzy nie znajdują się na liście.
   - **Zaufane programy aktualizujące**. Kaspersky Endpoint Security uważa aplikacje znajdujące się w wybranej kategorii za zaufane programy aktualizujące mogące tworzyć inne pliki wykonywalne, których uruchomienie będzie dozwolone.
10. Zapisz swoje zmiany.

Zarządzanie regułami Kontroli aplikacji

Kaspersky Endpoint Security kontroluje uruchamianie aplikacji przez użytkownika przy użyciu reguł. Reguła Kontroli aplikacji określa warunki wyzwalania oraz działania wykonywane przez Kontrolę aplikacji, gdy reguła zostaje wyzwolona (zezwalanie lub blokowanie uruchamiania aplikacji przez użytkowników).

Warunki wyzwalające regułę

Warunek wyzwalający regułę przedstawia następującą zależność: „typ warunku - kryterium warunku - wartość warunku". W oparciu o warunki wyzwalające regułę, Kaspersky Endpoint Security stosuje (lub nie stosuje) regułę do aplikacji.

W regułach używane są następujące typy warunków:

- *Warunki włączenia*. Kaspersky Endpoint Security stosuje regułę do aplikacji, jeśli aplikacja odpowiada przynajmniej jednemu warunkowi włączenia.

- *Warunki wykluczenia*. Kaspersky Endpoint Security nie stosuje reguły do aplikacji, jeśli aplikacja odpowiada przynajmniej jednemu warunkowi wykluczenia i nie odpowiada żadnemu warunkowi włączenia.

Warunki wyzwalające regułę są tworzone przy użyciu kryteriów. Do tworzenia reguł w Kaspersky Endpoint Security używane są następujące kryteria:

- Ścieżka do folderu zawierającego plik wykonywalny aplikacji lub ścieżka dostępu do pliku wykonywalnego aplikacji.

- Metadane: nazwa pliku wykonywalnego aplikacji, wersja pliku wykonywalnego aplikacji, nazwa aplikacji, wersja aplikacji, producent aplikacji.

- Suma kontrolna pliku wykonywalnego aplikacji.

- Certyfikat: wydawca, temat, odcisk palca.

- Włączenie aplikacji do kategorii KL.

- Lokalizacja pliku wykonywalnego aplikacji na nośniku wymiennym.

Wartość kryterium musi być określona dla każdego kryterium używanego w warunku. Jeśli parametry uruchamianej aplikacji odpowiadają wartościom kryteriów określonym w warunkach włączenia, reguła zostanie wyzwolona. W tym przypadku Kontrola aplikacji wykona akcję określoną w regule. Jeśli parametry aplikacji odpowiadają wartościom kryteriów określonych w warunku wykluczenia, Kontrola aplikacji nie kontroluje uruchamiania aplikacji.

Jeśli jako warunek wyzwalający regułę wybrałeś certyfikat, musisz być pewny, że ten certyfikat jest dodawany do zaufanego magazynu systemu na komputerze oraz sprawdzić ustawienia korzystania z zaufanego magazynu systemu w aplikacji.

Decyzja podjęta przez komponent Kontrola aplikacji w momencie wyzwolenia reguły

Jeśli reguła zostanie wyzwolona, Kontrola aplikacji zezwala użytkownikom (lub grupom użytkowników) na uruchamianie aplikacji lub blokuje uruchomienie zgodnie z regułą. Możesz wybrać pojedynczych użytkownika lub grupę użytkowników, którzy mogą (lub nie mogą) uruchamiać aplikacje wyzwalające regułę.

Jeśli reguła nie określa tych użytkowników mogących uruchamiać aplikacje odpowiadające regule, reguła ta jest zwana regułą *blokującą*.

Jeśli reguła, która nie określa żadnych użytkowników, którzy nie mogą uruchamiać aplikacji odpowiadających regule, reguła ta jest zwana regułą *zezwalającą*.

Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Na przykład, jeśli reguła zezwalająca Kontroli aplikacji została określona dla grupy użytkowników, a dla użytkownika w tej grupie użytkowników określono regułę blokującą, nie będzie on mógł uruchamiać aplikacji.

Stan działania reguły

Reguły Kontroli aplikacji mogą posiadać jeden z następujących stanów działania:

- **Włączone**. Ten stan oznacza, że przy włączonym komponencie Kontrola aplikacji reguła ta jest wykorzystywana.
- **Wyłączone**. Ten stan oznacza, że reguła jest ignorowana, gdy działa komponent Kontrola aplikacji.
- **Tryb testowy**. Ten stan oznacza, że Kaspersky Endpoint Security zezwala na uruchamianie aplikacji, do których reguły są stosowane, ale rejestrują informacje o uruchamianiu takich aplikacji w raporcie.

Dodawanie warunku wyzwalającego dla reguły Kontroli aplikacji

Aby tworzenie reguł Kontroli aplikacji było wygodniejsze, możesz utworzyć kategorie aplikacji.

Zalecane jest utworzenie kategorii „Aplikacje do pracy", do której będzie należeć standardowy zestaw aplikacji używanych w firmie. Jeżeli różne grupy użytkowników używają w swojej pracy różnych zestawów aplikacji, dla każdej grupy użytkowników można utworzyć oddzielną kategorię aplikacji.

Aby utworzyć kategorię aplikacji w Konsoli Administracyjnej:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz opcje **Zaawansowane → Zarządzanie aplikacjami → Kategorie aplikacji**.
3. W obszarze roboczym kliknij **Nowa kategoria**.

   Zostanie uruchomiony Kreator tworzenia kategorii użytkownika.
4. Postępuj zgodnie z instrukcjami Kreatora tworzenia kategorii użytkownika.

Krok 1. Wybieranie typu kategorii

W tym kroku wybierz jeden z następujących typów kategorii aplikacji:

- Kategoria z zawartością dodaną ręcznie. Dane plików wykonywalnych są dodawane do tej kategorii ręcznie Jeżeli wybrano ten typ kategorii, w kroku *Konfiguracja warunków włączania aplikacji do kategorii* i *Konfiguracja warunków wykluczania aplikacji z kategorii* będzie można określić kryteria uwzględnienia plików wykonywalnych w kategorii.

- Kategoria zawierająca pliki wykonywalne znajdujące się na wybranych urządzeniach. Takie pliki wykonywalne są przetwarzane automatycznie, a ich metryki są dodawane do kategorii Jeśli wybrano ten typ kategorii, w kroku *Ustawienia* będzie można określić komputer, którego pliki wykonywalne zostaną automatycznie uwzględnione w kategorii.

- 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 Jeśli wybrano ten typ kategorii, w kroku *Folder repozytorium* będzie można określić folder, z którego pliki wykonywalne zostaną automatycznie uwzględnione w kategorii.

Podczas tworzenia kategorii z zawartością dodaną automatycznie, Kaspersky Security Center przeprowadza inwentaryzację plików w następujących formatach: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX i SCR.

Krok 2. Wprowadzanie nazwy kategorii użytkownika

W tym kroku określ nazwę kategorii aplikacji.

Krok 3. Konfigurowanie warunków uwzględniania aplikacji w kategorii

Dodanie do reguł kontroli aplikacji dużej liczby warunków (na przykład skrótów plików) powoduje zwiększenie zużycia zasobów komputera. Gdy łączna liczba warunków osiągnie 50 000, mogą wystąpić problemy z wydajnością. Aby zoptymalizować wydajność, zaleca się sprawdzenie warunków i zmniejszenie ich liczby.

Ten krok jest dostępny, jeśli wybrałeś typ kategorii **Kategoria z zawartością dodaną ręcznie**.

W tym kroku, z listy rozwijalnej **Dodaj** wybierz warunki uwzględnienia aplikacji w kategorii:

- **Z listy plików wykonywalnych**. Dodaj aplikacje z listy plików wykonywalnych na urządzeniu klienckim do kategorii niestandardowej.

- **Z właściwości pliku**. Określ szczegółowe dane plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.

- **Metadane z plików w folderze**. Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne. Kaspersky Security Center wskaże metadane tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.

- **Sumy kontrolne plików znajdujących się w folderze**. Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne. Kaspersky Security Center wskaże sumy kontrolne tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.

- **Certyfikaty dla plików z folderu**. Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne podpisane certyfikatami. Kaspersky Security Center wskaże certyfikaty tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.

  Nie jest zalecane używanie warunków, których właściwości nie posiadają określonego parametru **Odcisk palca certyfikatu**.

- **Metadane plików instalatora MSI**. Wybierz pakiet MSI. Kaspersky Security Center wskaże metadane plików wykonywalnych spakowanych w pakiecie MSI jako warunek dodania aplikacji do kategorii niestandardowej.

- **Sumy kontrolne plików z instalatora MSI aplikacji**. Wybierz pakiet MSI. Kaspersky Security Center wskaże sumy kontrolne plików wykonywalnych spakowanych w pakiecie MSI jako warunek dodania aplikacji do kategorii niestandardowej.

- **Z kategorii KL**. Określ kategorię KL jako warunek dodania aplikacji do kategorii niestandardowej. *Kategoria KL* to lista aplikacji, które mają podobne atrybuty. Lista jest utrzymywana przez specjalistów z Kaspersky. Na przykład, kategoria KL o nazwie *Aplikacje biurowe* zawiera aplikacje pakietu Microsoft Office, Adobe Acrobat i wiele innych.

  Możesz wybrać wszystkie kategorie KL do wygenerowania rozszerzonej listy zaufanych aplikacji.

- **Określ ścieżkę do aplikacji (maski są obsługiwane)**. Wybierz folder na urządzeniu klienckim. Kaspersky Security Center doda pliki wykonywalne z tego folderu do kategorii niestandardowej.

- **Wybierz certyfikat z repozytorium**. Wybierz certyfikaty, które zostały użyte do podpisania plików wykonywalnych, jako warunek dodania aplikacji do kategorii niestandardowej.

  Nie jest zalecane używanie warunków, których właściwości nie posiadają określonego parametru **Odcisk palca certyfikatu**.

  Możesz wybrać magazyn certyfikatów. Domyślnie Kontrola aplikacji stosuje reguły wyłącznie do aplikacji podpisanych certyfikatem pochodzącym z zaufanego systemowego magazynu certyfikatów. Umożliwia to pole wyboru **Używaj ścisłej weryfikacji podpisem cyfrowym**.

- **Typ dysku**. Określ typ urządzenia magazynującego (wszystkie dyski twarde i dyski wymienne lub tylko dyski wymienne) jako warunek dodania aplikacji do kategorii niestandardowej.

Krok 4. Konfigurowanie warunków wykluczenia aplikacji z kategorii

Ten krok jest dostępny, jeśli wybrałeś typ kategorii **Kategoria z zawartością dodaną ręcznie**.

Aplikacje określone w tym kroku zostaną wykluczone z kategorii nawet wtedy, gdy te aplikacje zostały określone w kroku „Konfigurowanie warunków uwzględniania aplikacji w kategorii".

W tym kroku, z listy rozwijalnej **Dodaj** wybierz warunki wykluczania aplikacji z kategorii:

- **Z listy plików wykonywalnych**. Dodaj aplikacje z listy plików wykonywalnych na urządzeniu klienckim do kategorii niestandardowej.
- **Z właściwości pliku**. Określ szczegółowe dane plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.
- **Metadane z plików w folderze**. Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne. Kaspersky Security Center wskaże metadane tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.
- **Sumy kontrolne plików znajdujących się w folderze**. Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne. Kaspersky Security Center wskaże sumy kontrolne tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.
- **Certyfikaty dla plików z folderu**. Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne podpisane certyfikatami. Kaspersky Security Center wskaże certyfikaty tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.
- **Metadane plików instalatora MSI**. Wybierz pakiet MSI. Kaspersky Security Center wskaże metadane plików wykonywalnych spakowanych w pakiecie MSI jako warunek dodania aplikacji do kategorii niestandardowej.
- **Sumy kontrolne plików z instalatora MSI aplikacji**. Wybierz pakiet MSI. Kaspersky Security Center wskaże sumy kontrolne plików wykonywalnych spakowanych w pakiecie MSI jako warunek dodania aplikacji do kategorii niestandardowej.
- **Z kategorii KL**. Określ kategorię KL jako warunek dodania aplikacji do kategorii niestandardowej. *Kategoria KL* to lista aplikacji, które mają podobne atrybuty. Lista jest utrzymywana przez specjalistów z Kaspersky. Na przykład, kategoria KL o nazwie *Aplikacje biurowe* zawiera aplikacje pakietu Microsoft Office, Adobe Acrobat i wiele innych.

  Możesz wybrać wszystkie kategorie KL do wygenerowania rozszerzonej listy zaufanych aplikacji.
- **Określ ścieżkę do aplikacji (maski są obsługiwane)**. Wybierz folder na urządzeniu klienckim. Kaspersky Security Center doda pliki wykonywalne z tego folderu do kategorii niestandardowej.
- **Wybierz certyfikat z repozytorium**. Wybierz certyfikaty, które zostały użyte do podpisania plików wykonywalnych, jako warunek dodania aplikacji do kategorii niestandardowej.
- **Typ dysku**. Określ typ urządzenia magazynującego (wszystkie dyski twarde i dyski wymienne lub tylko dyski wymienne) jako warunek dodania aplikacji do kategorii niestandardowej.

Krok 5. Ustawienia

Ten krok jest dostępny, jeśli wybrałeś typ kategorii **Kategoria zawierająca pliki wykonywalne z wybranych urządzeń**.

W tym kroku kliknij przycisk **Dodaj** i określ komputery, których pliki wykonywalne zostaną dodane do kategorii aplikacji przez Kaspersky Security Center. Wszystkie pliki wykonywalne z określonych komputerów, znajdujące się w folderze **Pliki wykonywalne**, zostaną dodane do kategorii aplikacji przez Kaspersky Security Center.

W tym kroku możesz skonfigurować następujące ustawienia:

- Algorytm obliczania funkcji skrótu. W celu wybrania algorytmu musisz zaznaczyć przynajmniej jedną z następujących opcji:
  - **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)**.
- Pole **Synchronizuj dane z repozytorium Serwera administracyjnego**. Zaznacz to pole, jeśli chcesz, żeby Kaspersky Security Center okresowo czyścił kategorię aplikacji i dodawał do niej wszystkie pliki wykonywalne z określonych komputerów, znajdujących się w folderze **Pliki wykonywalne**.

  Jeśli pole **Synchronizuj dane z repozytorium Serwera administracyjnego** jest odznaczone, Kaspersky Security Center nie wprowadzi żadnych modyfikacji do kategorii aplikacji po jej utworzeniu.

Krok 6. Folder Repozytorium

Ten krok jest dostępny, jeśli wybrałeś typ kategorii **Kategoria zawierająca pliki wykonywalne z określonego folderu**.

W tym kroku określ folder, w którym Kaspersky Security Center wyszuka pliki wykonywalne do automatycznego dodania aplikacji do kategorii aplikacji.

W tym kroku możesz skonfigurować następujące ustawienia:

- Pole **Uwzględnij w tej kategorii biblioteki dołączane dynamicznie (DLL)**. Zaznacz to pole, jeśli chcesz, aby biblioteki dołączane dynamicznie (pliki DLL) były uwzględnione w kategorii aplikacji.

  Uwzględnienie plików DLL w kategorii aplikacji może zmniejszyć wydajność Kaspersky Security Center.

- Pole **Uwzględnij w tej kategorii dane skryptów**. Zaznacz to pole, jeśli chcesz, aby skrypty były uwzględniane w kategorii aplikacji.

  Uwzględnienie skryptów w kategorii aplikacji może zmniejszyć wydajność Kaspersky Security Center.

- Algorytm obliczania funkcji skrótu. W celu wybrania algorytmu musisz zaznaczyć przynajmniej jedną z następujących opcji:

  - **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)**.

- Pole **Wymuś skanowanie folderu pod kątem zmian**. Zaznacz to pole, jeśli chcesz, żeby Kaspersky Security Center okresowo wyszukiwał pliki wykonywalne w folderze używanym do automatycznego dodawania do kategorii aplikacji.

  Jeśli pole **Wymuś skanowanie folderu pod kątem zmian** jest odznaczone, Kaspersky Security Center wyszukuje pliki wykonywalne w folderze używanym do automatycznego dodawania do kategorii aplikacji tylko wtedy, gdy w folderze zostały wprowadzone zmiany, pliki zostały dodane do niego lub zostały usunięte z niego.

- Pole **Zakres skanowania (1—168 godzin)**. W tym polu możesz określić przedział czasu (w godzinach), po jakim Kaspersky Security Center rozpocznie wyszukiwanie plików wykonywalnych w folderze używanym do automatycznego dodawania do kategorii aplikacji.

  Pole to jest dostępne, jeśli zaznaczone jest pole wyboru **Wymuś skanowanie folderu pod kątem zmian**.

Krok 7. Tworzenie kategorii niestandardowej

Zakończ działanie Kreatora.

W celu dodania nowego warunku wyzwalającego dla reguły Kontroli aplikacji w interfejsie aplikacji:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

3. Kliknij przycisk **Blokowane aplikacje** lub **Dozwolone aplikacje**.

   Spowoduje to otwarcie listy reguł Kontroli aplikacji.

4. Wybierz regułę, dla której chcesz skonfigurować warunek wyzwalający.

   Zostanie otwarte okno właściwości reguły Kontroli aplikacji.

5. Wybierz zakładkę **Warunki: N** lub zakładkę **Wykluczenia: N** i kliknij przycisk **Dodaj**.

6. Wybierz warunki wyzwalające dla reguły Kontroli aplikacji:

   - **Warunki z właściwości uruchomionych aplikacji**. Na liście uruchomionych aplikacji możesz wybrać aplikacje, do których zostanie zastosowana reguła Kontroli aplikacji. Kaspersky Endpoint Security wyświetla także aplikacje, które były wcześniej uruchomione na komputerze. Możesz także wybrać kryteria, których chcesz użyć do utworzenia jednego lub kilku warunków wyzwalających regułę: **Suma kontrolna pliku**, **Certyfikat**, **Kategoria KL**, **Metadane** lub **Ścieżka do pliku lub folderu**.

   - **Warunki „Kategorii KL”**. *Kategoria KL* to lista aplikacji, które mają podobne atrybuty. Lista jest utrzymywana przez specjalistów z Kaspersky. Na przykład, kategoria KL „Aplikacje biurowe” zawiera aplikacje pakietu Microsoft Office, Adobe® Acrobat® i wiele innych.

- **Warunek niestandardowy**. Możesz wybrać plik aplikacji oraz jeden z warunków wyzwalających regułę: **Suma kontrolna pliku**, **Certyfikat**, **Metadane** lub **Ścieżka do pliku lub folderu**.

- **Warunek według nośnika plików (dysk wymienny)**. Reguła Kontroli aplikacji jest stosowana tylko do plików, które są uruchamiane na nośniku wymiennym.

- **Warunki z właściwości plików w określonym folderze**. Reguła Kontroli aplikacji jest stosowana tylko do plików w obrębie określonego folderu. Możesz także włączyć lub wykluczyć pliki z podfolderów. Możesz także wybrać kryteria, których chcesz użyć do utworzenia jednego lub kilku warunków wyzwalających regułę: **Suma kontrolna pliku**, **Certyfikat**, **Kategoria KL**, **Metadane** lub **Ścieżka do pliku lub folderu**.

7. Zapisz swoje zmiany.

Podczas dodawania warunków należy uwzględnić następujące specjalne właściwości Kontroli aplikacji:

- Kaspersky Endpoint Security obsługuje znaki `*` i `?` przy wprowadzaniu maski w metadanych: **Nazwa pliku**, **Nazwa aplikacji**, **Dostawca**.

- Kaspersky Endpoint Security nie obsługuje sumy kontrolnej pliku MD5 i nie kontroluje uruchamiania aplikacji w oparciu o sumę kontrolną MD5. Jako warunek wyzwalający regułę używana jest suma kontrolna SHA256.

- Nie jest zalecane używanie tylko elementów **Wydawca** i **Podmiot certyfikatu** jako warunków wyzwalających regułę. Użycie tych kryteriów jest niemiarodajne.

- Jeśli używasz dowiązania symbolicznego, w polu **Ścieżka do pliku lub folderu** zalecane jest rozwiązanie dowiązania symbolicznego w celu poprawnego działania reguły Kontroli aplikacji. W tym celu kliknij przycisk **Rozwiąż dowiązanie symboliczne**.

Dodawanie plików wykonywalnych z folderu Pliki wykonywalne do kategorii aplikacji

W folderze **Pliki wykonywalne** zostanie wyświetlona lista plików wykonywalnych wykrytych na komputerach. Kaspersky Endpoint Security wygeneruje listę plików wykonywalnych po wykonaniu zadania inwentaryzacji.

W celu dodania plików wykonywalnych z folderu Pliki wykonywalne do kategorii aplikacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W drzewie Konsoli administracyjnej wybierz opcje **Zaawansowane** → **Zarządzanie aplikacjami** → **Pliki wykonywalne**.

3. W obszarze roboczym wybierz pliki wykonywalne, które chcesz dodać do kategorii aplikacji.

4. Kliknij wybrany plik wykonywalny prawym klawiszem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Dodaj do kategorii**.

5. W otwartym oknie wykonaj następujące czynności:

   - W górnej części okna wybierz jedną z poniższych opcji:

     - **Dodaj do nowej kategorii aplikacji**. Wybierz tę opcję, jeśli chcesz utworzyć nową kategorię aplikacji i dodać do niej pliki wykonywalne.

     - **Dodaj do istniejącej kategorii aplikacji**. Wybierz tę opcję, jeśli chcesz wybrać istniejącą kategorię aplikacji i dodać do niej pliki wykonywalne.

   - W sekcji **Typ reguły** wybierz jedną z następujących opcji:

     - **Reguły dodawania do włączeń**. Wybierz tę opcję, jeśli chcesz utworzyć warunek, który dodaje pliki wykonywalne do kategorii aplikacji.

     - **Reguły dodawania do wykluczeń**. Wybierz tę opcję, jeśli chcesz utworzyć warunek, który wyklucza pliki wykonywalne z kategorii aplikacji.

   - W sekcji **Parametr użyty jako warunek** wybierz jedną z następujących opcji:

     - **Szczegóły certyfikatu (lub sumy kontrolne SHA256 dla plików bez certyfikatu)**.

     - **Szczegóły certyfikatu (pliki bez certyfikatu zostaną pominięte)**.

     - **Tylko SHA256 (pliki bez sumy kontrolnej zostaną pominięte)**.

     - **Tylko MD5 (tryb wycofany, wyłącznie dla wersji Kaspersky Endpoint Security 10 Service Pack 1)**.

6. Zapisz swoje zmiany.

Dodawanie plików wykonywalnych związanych ze zdarzeniami do kategorii aplikacji

W celu dodania plików wykonywalnych związanych ze zdarzeniami Kontroli aplikacji do kategorii aplikacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Zdarzenia**.

3. Wybierz wybór zdarzeń związanych z działaniem komponentu Kontrola aplikacji (Przeglądanie zdarzeń z działania modułu Kontrola aplikacji, Przeglądanie zdarzeń z działania testowego komponentu Kontrola aplikacji) z listy rozwijalnej **Wybory zdarzeń**.

4. Kliknij przycisk **Uruchom wybrane**.

5. Wybierz zdarzenia, których skojarzone pliki wykonywalne chcesz dodać do kategorii aplikacji.

6. Kliknij wybrane zdarzenia prawym klawiszem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Dodaj do kategorii**.

7. W otwartym oknie skonfiguruj ustawienia kategorii aplikacji:

   - W górnej części okna wybierz jedną z poniższych opcji:

     - **Dodaj do nowej kategorii aplikacji**. Wybierz tę opcję, jeśli chcesz utworzyć nową kategorię aplikacji i dodać do niej pliki wykonywalne.

     - **Dodaj do istniejącej kategorii aplikacji**. Wybierz tę opcję, jeśli chcesz wybrać istniejącą kategorię aplikacji i dodać do niej pliki wykonywalne.

   - W sekcji **Typ reguły** wybierz jedną z następujących opcji:

     - **Reguły dodawania do włączeń**. Wybierz tę opcję, jeśli chcesz utworzyć warunek, który dodaje pliki wykonywalne do kategorii aplikacji.

     - **Reguły dodawania do wykluczeń**. Wybierz tę opcję, jeśli chcesz utworzyć warunek, który wyklucza pliki wykonywalne z kategorii aplikacji.

   - W sekcji **Parametr użyty jako warunek** wybierz jedną z następujących opcji:

     - **Szczegóły certyfikatu (lub sumy kontrolne SHA-256 dla plików bez certyfikatu)**.

     - **Szczegóły certyfikatu (pliki bez certyfikatu zostaną pominięte)**.

     - **Tylko SHA-256 (pliki bez sumy kontrolnej zostaną pominięte)**.

     - **Tylko MD5 (tryb wycofany, wyłącznie dla Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Zapisz swoje zmiany.

Dodawanie reguły Kontroli aplikacji

W celu dodania reguły Kontroli aplikacji przy użyciu Kaspersky Security Center:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Kontrola zabezpieczeń → Kontrola aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola aplikacji.

4. Kliknij **Dodaj**.

   Zostanie otwarte okno **Reguła kontroli aplikacji**.

5. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz utworzyć nową kategorię:

     a. Kliknij **Utwórz kategorię**.

     Zostanie uruchomiony Kreator tworzenia kategorii użytkownika.

b. Postępuj zgodnie z instrukcjami Kreatora tworzenia kategorii użytkownika.

c. Z listy rozwijalnej **Kategoria** wybierz utworzoną kategorię aplikacji.

- Jeśli chcesz edytować istniejącą kategorię:

a. Z listy rozwijalnej **Kategoria** wybierz utworzoną kategorię aplikacji, którą chcesz edytować.

b. Kliknij **Właściwości**.

c. Zmodyfikuj ustawienia wybranej kategorii aplikacji.

d. Zapisz swoje zmiany.

e. Z listy rozwijalnej **Kategoria** wybierz utworzoną kategorię aplikacji, w oparciu o którą chcesz utworzyć regułę.

6. W tabeli **Użytkownicy i ich uprawnienia** kliknij przycisk **Dodaj**.

   Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

7. W tabeli **Użytkownicy i ich uprawnienia**:

   - Jeśli chcesz zezwolić użytkownikom i/lub grupom użytkowników na uruchamianie aplikacji, które należą do wybranej kategorii, zaznacz pola **Zezwól** obok odpowiednich wierszy.

   - Jeśli chcesz zablokować użytkownikom i/lub grupom użytkowników możliwość uruchamiania aplikacji, które należą do wybranej kategorii, zaznacz pola **Zablokuj** obok odpowiednich wierszy.

8. Wybierz pole **Zabroń innym użytkownikom**, jeśli chcesz, aby dla wszystkich użytkowników, którzy nie pojawiają się w kolumnie **Użytkownik lub grupa** i nie są częścią grupy użytkowników określonej w kolumnie **Użytkownik lub grupa**, została zablokowana możliwość uruchamiania aplikacji, które należą do wybranej kategorii.

9. Jeżeli chcesz, aby Kaspersky Endpoint Security uważał aplikacje znajdujące się w wybranej kategorii aplikacji za zaufane programy aktualizujące mogące tworzyć inne pliki wykonywalne, których uruchomienie będzie dozwolone, zaznacz pole **Zaufane programy aktualizujące**.

   Jeśli przenosisz ustawienia Kaspersky Endpoint Security, lista plików wykonywalnych utworzonych przez zaufane programy aktualizujące także zostanie przeniesiona.

10. Zapisz swoje zmiany.

W celu dodania reguły Kontroli aplikacji:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

3. Kliknij przycisk **Blokowane aplikacje** lub **Dozwolone aplikacje**.

   Spowoduje to otwarcie listy reguł Kontroli aplikacji.

4. Kliknij **Dodaj**.

   To spowoduje otwarcie okna ustawień reguły Kontroli aplikacji.

5. Na zakładce **Ustawienia ogólne** zdefiniuj główne ustawienia reguły:

   a. W polu **Nazwa reguły** wprowadź nazwę reguły.

   b. W polu **Opis** wprowadź opis reguły.

   c. W tabeli **Użytkownicy i ich uprawnienia** kliknij przycisk **Dodaj**.

   Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.

   Reguła jest domyślnie stosowana do wszystkich użytkowników.

   > Jeśli w tabeli nie ma określonego użytkownika, reguła nie może zostać zapisana.

   d. W tabeli **Użytkownicy i ich uprawnienia** użyj przełącznika do zdefiniowania uprawnienia użytkowników do uruchamiania aplikacji.

   e. Zaznacz pole **Zabroń innym użytkownikom**, jeśli chcesz, żeby aplikacja uniemożliwiła aplikacjom, które spełniają warunki wyzwolenia reguły, uruchamianie dla wszystkich użytkowników, którzy nie znajdują się w tabeli **Użytkownicy i ich uprawnienia** i nie są członkami grup użytkowników w tabeli **Użytkownicy i ich uprawnienia**.

   > Jeśli pole **Zabroń innym użytkownikom** jest odznaczone, Kaspersky Endpoint Security nie kontroluje uruchamiania aplikacji przez użytkowników, którzy nie są określeni w tabeli **Użytkownicy i ich uprawnienia** i nie należą do grup użytkowników określonych w tabeli **Użytkownicy i ich uprawnienia**.

   f. Zaznacz pole **Zaufane programy aktualizujące**, jeśli chcesz, żeby program Kaspersky Endpoint Security uznawał aplikacje odpowiadające warunkom wyzwolenia reguły za zaufane programy aktualizujące. *Zaufane programy aktualizujące* to aplikacje, które mogą tworzyć inne pliki wykonywalne, które będą mogły potem działać.

   Jeśli aplikacja wyzwoli kilka reguł, Kaspersky Endpoint Security ustawi flagę *Zaufane programy aktualizujące*, jeśli spełnione są następujące warunki:

   - Wszystkie reguły pozwalają aplikacji na uruchomienie.
   - Przynajmniej obok jednej reguły jest zaznaczone pole **Zaufane programy aktualizujące**.

6. Na zakładce **Warunki: N** utwórz lub edytuj listę warunków włączenia wyzwalających regułę.

7. Na zakładce **Wykluczenia: N** utwórz lub edytuj listę warunków wykluczenia wyzwalających regułę.

   Jeśli przenosisz ustawienia Kaspersky Endpoint Security, lista plików wykonywalnych utworzonych przez zaufane programy aktualizujące także zostanie przeniesiona.

8. Zapisz swoje zmiany.

Zmienianie stanu reguły Kontroli aplikacji przy użyciu Kaspersky Security Center

W celu zmiany stanu reguły Kontroli aplikacji w Konsoli Administracyjnej:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola aplikacji.
4. W kolumnie **Stan** kliknij lewym klawiszem myszy, aby wyświetlić menu kontekstowe, z którego wybierz jeden z następujących elementów:
   - **Włączona**. Ten stan oznacza, że przy włączonym komponencie Kontrola aplikacji reguła ta jest wykorzystywana.
   - **Wyłączona**. Ten stan oznacza, że reguła jest ignorowana, gdy działa komponent Kontrola aplikacji.
   - **Sprawdź**. Ten stan oznacza, że Kaspersky Endpoint Security zawsze zezwala na uruchamianie aplikacji, do których reguła jest stosowana, ale zapisuje informacje o uruchamianiu takich aplikacji w raporcie.
5. Zapisz swoje zmiany.

W celu zmiany stanu reguły Kontroli aplikacji w interfejsie aplikacj:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
3. Kliknij przycisk **Blokowane aplikacje** lub **Dozwolone aplikacje**.

   Spowoduje to otwarcie listy reguł Kontroli aplikacji.
4. W kolumnie **Stan** otwórz menu kontekstowe i wybierz jeden z następujących elementów:
   - **Włączone**. Ten stan oznacza, że przy włączonym komponencie Kontrola aplikacji reguła ta jest wykorzystywana.
   - **Wyłączone**. Ten stan oznacza, że reguła jest ignorowana, gdy działa komponent Kontrola aplikacji.
   - **Tryb testowy**. Ten stan oznacza, że Kaspersky Endpoint Security zawsze zezwala na uruchamianie aplikacji, do których ta reguła jest stosowana, ale zapisuje informacje o uruchamianiu takich aplikacji w raporcie.
5. Zapisz swoje zmiany.

Eksportowanie i importowanie reguł Kontroli aplikacji

Możesz wyeksportować listę reguł Kontroli aplikacji do pliku XML. Możesz użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy reguł Kontroli aplikacji lub przeniesienia listy na inny serwer.

Podczas eksportowania i importowania reguł Kontroli aplikacji należy mieć na uwadze następujące kwestie specjalne:

- Kaspersky Endpoint Security eksportuje listę reguł tylko dla aktywnego trybu Kontroli aplikacji. Innymi słowy, jeśli Kontrola aplikacji działa w trybie listy zabronionych, Kaspersky Endpoint Security eksportuje reguły tylko dla tego trybu. Aby wyeksportować listę reguł dla trybu listy zezwolonych, należy przełączyć tryb i uruchomić eksportowanie ponownie.

- Kaspersky Endpoint Security używa kategorii aplikacji dla działania reguł Kontroli aplikacji. Podczas przenoszenia listy reguł Kontroli aplikacji na inny serwer, musisz także przenieść listę kategorii aplikacji. Więcej informacji dotyczących eksportowania lub importowania kategorii aplikacji można znaleźć w pomocy do Kaspersky Security Center.

Eksportowanie i importowanie listy reguł Kontroli aplikacji w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
4. W celu wyeksportowania listy reguł Kontroli aplikacji:
   a. Wybierz reguły, które chcesz zmienić. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
      Jeśli nie wybrałeś żadnej reguły, Kaspersky Endpoint Security wyeksportuje wszystkie reguły.
   b. Kliknij odnośnik **Eksportuj**.
   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę reguł, i wybierz folder, w którym chcesz zapisać ten plik.
   d. Zapisz plik.
      Kaspersky Endpoint Security eksportuje listę reguł do pliku XML.
5. W celu wyeksportowania reguł Kontroli aplikacji:
   a. Kliknij odnośnik **Importuj**.
      W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.
   b. Otwórz plik.
      Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
6. Zapisz swoje zmiany.

Eksportowanie i importowanie listy reguł Kontroli aplikacji w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

5. W obszarze **Tryb działania** wybierz listę reguł: lista zablokowanych i lista zezwolonych aplikacji.

6. W celu wyeksportowania listy reguł:

   a. Wybierz reguły, które chcesz zmienić.

   b. Kliknij przycisk → **Eksportuj**.

      Kaspersky Endpoint Security eksportuje listę reguł do pliku JSON w domyślnym folderze do pobrania.

7. W celu zaimportowania listy reguł:

   a. Kliknij przycisk → **Importuj**.

      W oknie, które zostanie otwarte, wybierz plik JSON, z którego chcesz zaimportować listę reguł.

   b. Otwórz plik.

      Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku JSON.

8. Zapisz swoje zmiany.

Przeglądanie zdarzeń z działania modułu Kontrola aplikacji

W celu przejrzenia zdarzeń wynikających z działania komponentu Kontrola aplikacji, otrzymanych przez Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Zdarzenia**.

3. Kliknij przycisk **Utwórz wybór**.

4. W otwartym oknie przejdź do sekcji **Zdarzenia**.

5. Kliknij przycisk **Wyczyść wszystkie**.

6. W tabeli **Zdarzenia** zaznacz pole **Zabroniono uruchomienia aplikacji**.

7. Zapisz swoje zmiany.

8. Z listy rozwijalnej **Wybory zdarzeń** wybierz utworzony wybór.

9. Kliknij przycisk **Uruchom wybrane**.

Przeglądanie raportu dotyczącego zablokowanych aplikacji

W celu wyświetlenia raportu dotyczącego zablokowanych aplikacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Raporty**.
3. Kliknij **Nowy szablon raportu**.

   Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu.
4. Postępuj zgodnie z instrukcjami Kreatora szablonu raportu. Na kroku **Wybieranie typu szablonu raportu** wybierz **Inne** → **Raport o zabronionych aplikacjach**.

   Po zakończeniu pracy Kreatora tworzenia nowego szablonu raportu, nowy szablon raportu pojawi się w tabeli, na zakładce **Raporty**.
5. Otwórz raport, klikając go dwukrotnie.

Zostanie rozpoczęty proces tworzenia raportu. Raport zostanie wyświetlony w nowym oknie.

Testowanie działania reguł Kontroli aplikacji

Aby upewnić się, że reguły Kontroli aplikacji nie będą blokowały aplikacji niezbędnych do pracy, po utworzeniu nowych reguł zalecane jest włączenie testowania reguł Kontroli aplikacji i sprawdzenie ich działania. Jeśli testowanie reguł Kontroli aplikacji jest włączone, Kaspersky Endpoint Security nie zablokuje aplikacji, których uruchamianie jest zabronione przez Kontrolę aplikacji, ale zamiast tego wyśle informacje o ich uruchomieniu do Serwera administracyjnego.

Analiza działania reguł Kontroli aplikacji obejmuje przejrzenie zdarzeń Kontroli aplikacji zgłoszonych do Kaspersky Security Center. Jeśli wyniki trybu testowego wykazały zdarzenia, w których nie zostały zablokowane uruchomienia wszystkich aplikacji wymaganych do pracy użytkownika komputera, oznacza to, że zostały utworzone poprawne reguły. W innej sytuacji zalecane jest zaktualizowanie ustawień utworzonych reguł, utworzenie dodatkowych reguł oraz usunięcie istniejących reguł.

Domyślnie Kaspersky Endpoint Security pozwala na uruchomienie wszystkich aplikacji, za wyjątkiem aplikacji zabronionych przez reguły.

Włączanie i wyłączanie testowania reguł modułu Kontrola Aplikacji

W celu włączenia lub wyłączenia testowania reguł Kontroli aplikacji w Kaspersky Security Center:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

   W prawej części okna wyświetlone są ustawienia modułu Kontrola aplikacji.

4. Z listy rozwijalnej **Tryb kontroli** wybierz jeden z następujących elementów:

   - **Lista zablokowanych**. Jeśli ta opcja jest zaznaczona, Kontrola aplikacji zezwala wszystkim użytkownikom na uruchomienie dowolnej aplikacji, za wyjątkiem przypadków, gdy aplikacje spełniają warunki reguł blokowania Kontroli aplikacji.

   - **Lista zezwolonych**. Jeśli ta opcja jest zaznaczona, Kontrola aplikacji blokuje wszystkim użytkownikom możliwość uruchomienia jakiejkolwiek aplikacji, za wyjątkiem przypadków, gdy aplikacje spełniają warunki reguł zezwalających Kontroli aplikacji.

5. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz włączyć testowanie reguł Kontroli aplikacji, z listy rozwijalnej **Akcja** wybierz opcję **Przetestuj reguły**.

   - Jeśli chcesz włączyć Kontrolę aplikacji do zarządzania uruchamianiem aplikacji na komputerach użytkowników, z listy rozwijalnej wybierz **Zastosuj reguły**.

6. Zapisz swoje zmiany.

W celu włączenia testowania reguł Kontroli aplikacji lub wybrania akcji blokowania dla Kontroli aplikacji:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

3. Kliknij przycisk **Blokowane aplikacje** lub **Dozwolone aplikacje**.

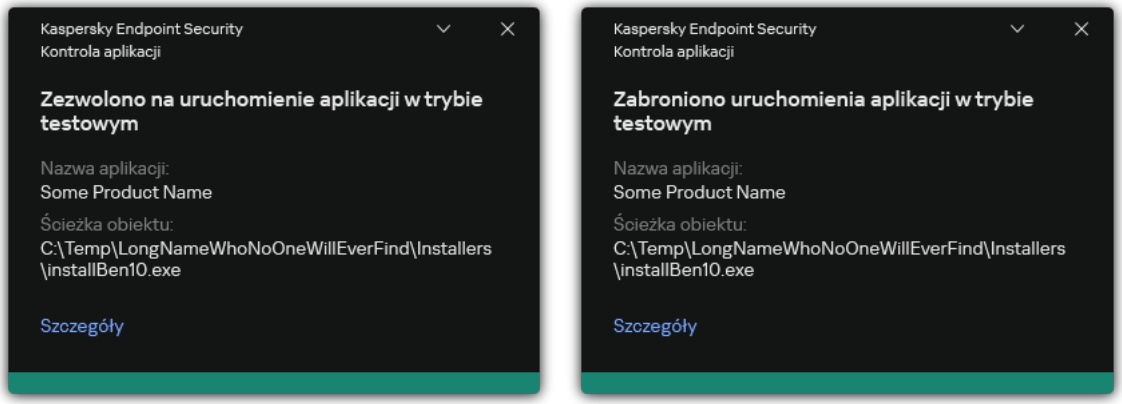
   Spowoduje to otwarcie listy reguł Kontroli aplikacji.

4. W kolumnie **Stan** wybierz **Tryb testowy**.

   Ten stan oznacza, że Kaspersky Endpoint Security zawsze zezwala na uruchamianie aplikacji, do których ta reguła jest stosowana, ale zapisuje informacje o uruchamianiu takich aplikacji w raporcie.

5. Zapisz swoje zmiany.

Kaspersky Endpoint Security nie zablokuje aplikacji, których uruchamianie jest zabronione przez komponent Kontroli aplikacji, ale wyśle informacje o ich uruchomieniu do Serwera administracyjnego. Możesz także skonfigurować wyświetlanie powiadomień o testowaniu reguł na komputerze użytkownika (patrz rysunek poniżej).



Powiadomienia Kontroli aplikacji w trybie testowym

Przeglądanie raportu dotyczącego zablokowanych aplikacji w trybie testowym

W celu wyświetlenia raportu dotyczącego zablokowanych aplikacji w trybie testowym:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Raporty**.
3. Kliknij **Nowy szablon raportu**.

   Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu.
4. Postępuj zgodnie z instrukcjami Kreatora szablonu raportu. W kroku **Wybieranie typu szablonu raportu** wybierz **Inne → Raport o zabronionych aplikacjach w trybie testowym**.

   Po zakończeniu pracy Kreatora tworzenia nowego szablonu raportu, nowy szablon raportu pojawi się w tabeli, na zakładce **Raporty**.
5. Otwórz raport, klikając go dwukrotnie.

Zostanie rozpoczęty proces tworzenia raportu. Raport zostanie wyświetlony w nowym oknie.

Przeglądanie zdarzeń z działania testowego komponentu Kontrola aplikacji

W celu przejrzenia zdarzeń testowych Kontroli aplikacji otrzymanych przez Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Zdarzenia**.
3. Kliknij przycisk **Utwórz wybór**.
4. W otwartym oknie przejdź do sekcji **Zdarzenia**.
5. Kliknij przycisk **Wyczyść wszystkie**.
6. W tabeli **Zdarzenia** zaznacz pola **Zabroniono uruchomienia aplikacji w trybie testowym** i **Zezwolono na uruchomienie aplikacji w trybie testowym**.
7. Zapisz swoje zmiany.
8. Z listy rozwijalnej **Wybory zdarzeń** wybierz utworzony wybór.
9. Kliknij przycisk **Uruchom wybrane**.

Monitor aktywności aplikacji

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Monitor aktywności aplikacji to narzędzie służące do wyświetlania informacji o aktywności aplikacji na komputerze użytkownika w czasie rzeczywistym.

Używanie Monitora aktywności aplikacji wymaga zainstalowania komponentów Kontrola aplikacji i Ochrona przed włamaniami. Jeśli te komponenty nie są zainstalowane, sekcja Monitor aktywności aplikacji w oknie głównym aplikacji jest ukryta.

W celu uruchomienia Monitora aktywności aplikacji:

W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Monitor aktywności aplikacji**.

W tym oknie informacje o aktywności aplikacji na komputerze użytkownika są przedstawione na trzech zakładkach:

- Zakładka **Wszystkie aplikacje** wyświetla informacje o wszystkich aplikacjach zainstalowanych na komputerze.
- Zakładka **Uruchomione** wyświetla informacje o zużyciu zasobów komputera według każdej aplikacji w czasie rzeczywistym. Z poziomu tej zakładki może także przejść do konfigurowania uprawnień dla pojedynczej aplikacji.
- Zakładka **Uruchomione przy starcie** wyświetla listę aplikacji, które są uruchamiane podczas uruchamiania systemu operacyjnego.

Jeśli chcesz ukryć informacje o aktywności aplikacji na komputerze użytkownika, możesz ograniczyć dostęp użytkownika do narzędzia Monitor aktywności aplikacji.

Jak w interfejsie aplikacji ukryć Monitor aktywności aplikacji, korzystając z Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Interfejs**.
4. Użyj pola **Ukryj sekcję Monitor aktywności aplikacji**, aby nadać lub wycofać dostęp do narzędzia.
5. Zapisz swoje zmiany.

Jak w interfejsie aplikacji ukryć Monitor aktywności aplikacji, korzystając z Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne** → **Interakcja użytkownika**.

5. Użyj pola **Ukryj sekcję Monitor aktywności aplikacji**, aby nadać lub wycofać dostęp do narzędzia.

6. Zapisz swoje zmiany.

Reguły tworzenia masek nazw dla plików i folderów

Maska nazwy pliku lub folderu to reprezentacja nazwy folderu lub nazwy i rozszerzenia pliku przy użyciu ogólnych znaków.

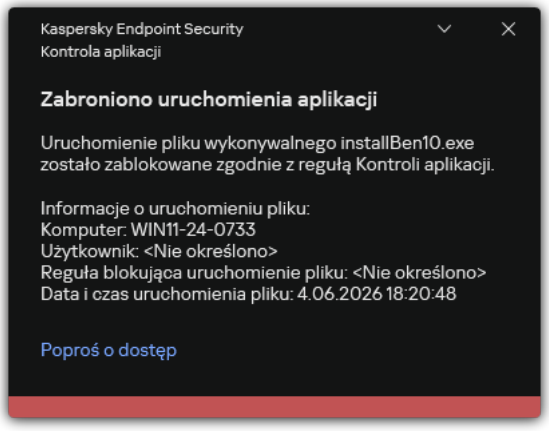
Do utworzenia maski nazwy pliku lub folderu można użyć następujących popularnych znaków:

- Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków (w tym pusty zestaw). Na przykład, maska `C:\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem `txt`, znajdujących się w folderach i podfolderach na dysku (C:).

- Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

Modyfikowanie szablonów wiadomości Kontroli aplikacji

Podczas próby uruchomienia aplikacji, zablokowanej przez regułę Kontroli aplikacji, program Kaspersky Endpoint Security wyświetli wiadomość informująca o zablokowaniu uruchomienia aplikacji. Eksperci Kaspersky udostępniają użytkownikowi szablon wiadomości opisującej powody zablokowania aplikacji (zobacz poniższy rysunek). Do zarządzania szablonami wiadomości dostępne są zmienne specjalne (na przykład `%USER_NAME%`). Zmienne umożliwiają stosowanie tego samego szablonu wiadomości na różnych komputerach. Podczas generowania wiadomości program Kaspersky Endpoint Security pobiera wartość zmiennej z ustawień systemu operacyjnego i wstawia ją do wiadomości odpowiedniej dla danego komputera, użytkownika i zdarzenia.



Powiadomienie Kontroli aplikacji

Jeżeli użytkownik ma pewność, że uruchomienie aplikacji zostało zablokowane przez pomyłkę, powinien użyć odnośnika dostępnego w wiadomości w celu przesłania zgłoszenia do administratora lokalnej sieci firmowej. Aby to zrobić, użytkownik musi kliknąć przycisk **Poproś o dostęp** i wysłać wiadomość do administratora opisując sytuację. Możesz również przygotować szablon wiadomości do administratora, uzupełniając go danymi, które mogą pomóc Ci podjąć decyzję o umożliwieniu lub zablokowaniu dostępu do aplikacji. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania uruchomienia aplikacji**. Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkownika**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

Jak edytować szablon wiadomości dotyczącej kontroli aplikacji w konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
4. W sekcji **Ustawienia szablonu wiadomości** kliknij przycisk **Szablony**.
5. Spowoduje to otwarcie okna; w tym oknie należy skonfigurować szablony kontroli aplikacji:

   - **Wiadomość dotycząca blokowania**. Szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła Kontroli aplikacji, która blokuje uruchamianie aplikacji.

     Nie możesz skonfigurować szablonów wiadomości dla Kontroli aplikacji w trybie testowym. Kontrola aplikacji w trybie testowym wyświetla predefiniowane powiadomienia.

   - **Wiadomość do administratora**. Szablon wiadomości, którą użytkownik może wysłać do administratora korporacyjnej sieci LAN, jeśli uważa, że aplikacja została przypadkowo zablokowana.

   Aby dodać zmienną do tekstu szablonu, umieść kursor w odpowiednim miejscu, kliknij przycisk **Zmienna** i wybierz wymaganą zmienną z listy dostępnych opcji.

   Możesz również przywrócić domyślny tekst szablonu za pomocą przycisku **Domyślny**.

6. Zapisz swoje zmiany.

Jak zmienić szablon wiadomości dotyczącej kontroli aplikacji w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

5. W sekcji **Szablony wiadomości** kliknij odnośnik **Wiadomości o blokadzie uruchamiania aplikacji** i skonfiguruj szablony dla wiadomości Kontroli aplikacji:

   - **Wiadomość do użytkownika**. Szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła Kontroli aplikacji, która blokuje uruchamianie aplikacji.

     Nie możesz skonfigurować szablonów wiadomości dla Kontroli aplikacji w trybie testowym. Kontrola aplikacji w trybie testowym wyświetla predefiniowane powiadomienia.

   - **Wiadomość do administratora**. Szablon wiadomości, którą użytkownik może wysłać do administratora korporacyjnej sieci LAN, jeśli uważa, że aplikacja została przypadkowo zablokowana.

   Aby dodać zmienną do tekstu szablonu, umieść kursor w odpowiednim miejscu, kliknij przycisk **Dodaj zmienną** i wybierz wymaganą zmienną z listy dostępnych opcji.

   Możesz również przywrócić domyślny tekst szablonu za pomocą przycisku **Resetuj do ustawień domyślnych**.

6. Zapisz swoje zmiany.

Jak zmienić szablon wiadomości dotyczącej kontroli aplikacji w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

3. W sekcji **Szablony wiadomości o blokowaniu aplikacji** skonfiguruj szablony dla wiadomości Kontroli aplikacji:

   - **Wiadomość dotycząca blokowania**. Szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła Kontroli aplikacji, która blokuje uruchamianie aplikacji.

     Nie możesz skonfigurować szablonów wiadomości dla Kontroli aplikacji w trybie testowym. Kontrola aplikacji w trybie testowym wyświetla predefiniowane powiadomienia.

   - **Wiadomość do administratora**. Szablon wiadomości, którą użytkownik może wysłać do administratora korporacyjnej sieci LAN, jeśli uważa, że aplikacja została przypadkowo zablokowana.

   Aby dodać zmienną do tekstu szablonu, umieść kursor w odpowiednim miejscu, kliknij przycisk **Dodaj zmienną** i wybierz wymaganą zmienną z listy dostępnych opcji.

   Możesz również przywrócić domyślny tekst szablonu za pomocą przycisku **Resetuj**.

4. Zapisz swoje zmiany.

Zmienne w szablonach wiadomości komponentu Kontrola aplikacji

W szablonach wiadomości użytkownika lub szablonach wiadomości administratora można używać następujących zmiennych:

- **Nazwa reguły, która została wywołana** – `%RULE%`.

  Nazwa reguły, która zablokowała wykonanie pliku.

- **Bieżąca data** – `%DATE%`.

  Data zablokowania wykonania pliku w formacie DD.MM.RRRR.

- **Bieżący czas** – `%TIME%`.

  Czas zablokowania wykonania pliku w formacie GG:MM.

- **Nazwa użytkownika** – `%USER_NAME%`.

  Nazwa bieżącego konta użytkownika na komputerze, na którym zablokowano wykonanie pliku, w formacie `<device name>\<user alias>` (na przykład `DESKTOP-123\John.Smith`).

- **Nazwa komputera** – `%COMPUTER_NAME%`.

  Nazwa komputera, na którym zablokowano wykonanie pliku.

- **Nazwa pliku wykonywalnego** – `%FILE_NAME%`.

  Nazwa pliku wykonywalnego zablokowanej aplikacji.

- **Kategoria KL pliku wykonywalnego** – `%KL_CAT%`.

  Kategoria KL, do której należy zablokowana aplikacja (na przykład *Przeglądarki* lub inna kategoria).

- **Ścieżka dostępu wykonywalnego** – `%FILE_PATH%`.

  Pełna ścieżka dostępu do pliku wykonywalnego zablokowanej aplikacji.

- **Wersja pliku wykonywalnego** – `%FILE_VERSION%`.

  Wersja pliku wykonywalnego zablokowanej aplikacji.

- **Oryginalna nazwa pliku wykonywalnego** – `%ORIGINAL_FILE_NAME%`.

  Oryginalna nazwa pliku wykonywalnego zablokowanej aplikacji. Nazwa pliku jest określona we właściwościach pliku wykonywalnego aplikacji.

- **Producent** – `%FILE_PUBLISHER%`.

  Producent zablokowanej aplikacji.

- **Nazwa aplikacji** – `%FILE_PRODUCT_NAME%`.

  Nazwa zablokowanej aplikacji.

- **Wersja aplikacji** – `%PRODUCT_VERSION%`.

  Wersja zablokowanej aplikacji.

- **Suma kontrolna pliku wykonywalnego** – `%FILE_HASH%`.

  Skrót pliku wykonywalnego zablokowanej aplikacji.

- **Wydawca certyfikatu** – `%CERT_ISSUER%`.

  Wystawca certyfikatu, którym podpisany jest plik wykonywalny.

- **Podmiot certyfikatu** – `%CERT_SUBJECT%`.

  Podmiot certyfikatu, którym podpisany jest plik wykonywalny.

- **Odcisk palca certyfikatu** – `%CERT_THUMBPRINT%`.

  Odcisk palca certyfikatu, którym podpisany jest plik wykonywalny.

Praktyczne zastosowanie aplikacji w celu zaimplementowania listy dozwolonych aplikacji

Podczas planowania implementacji listy zezwolonych aplikacji zalecane jest wykonanie następujących działań:

1. Utwórz następujące typy grup:

   - Grupy użytkowników. Grupy użytkowników, dla których musisz zezwolić na korzystanie z różnych zestawów aplikacji.

   - Grupy administracyjne. Jeden lub kilka grup komputerów, do których Kaspersky Security Center zastosuje listę zezwolonych aplikacji. Konieczne jest utworzenie kilku grup komputerów, jeśli dla tych grup zostały użyte różne ustawienia listy zezwolonych.

2. Utworzenie listy aplikacji, których uruchamianie musi być dozwolone.

   Przed utworzeniem listy, zalecane jest wykonanie następujących czynności:

   a. Uruchom zadanie inwentaryzacji.

      Informacje o utworzeniu, ponownej konfiguracji i uruchomieniu zadania inwentaryzacji są dostępne w sekcji Zarządzanie zadaniami.

   b. Przejrzyj listę plików wykonywalnych.

Konfigurowanie trybu listy zezwolonych aplikacji

Podczas konfigurowania trybu listy zezwolonych zalecane jest wykonanie następujących działań:

1. Utworzenie kategorii aplikacji zawierających aplikacje, których uruchamianie ma być dozwolone.

   Możesz wybrać jedną z następujących metod tworzenia kategorii aplikacji:

   - **Kategoria z zawartością dodaną ręcznie**. Możesz ręcznie dodać tę kategorię, korzystając z następujących warunków:

     - Metadane plików. Kaspersky Security Center doda wszystkie pliki wykonywalne z określonymi metadanymi do kategorii aplikacji.

     - Suma kontrolna pliku. Kaspersky Security Center doda wszystkie pliki wykonywalne z określoną sumą kontrolną do kategorii aplikacji.

       Użycie tego warunku wykluczy możliwość automatycznego zainstalowania uaktualnień, ponieważ różne wersje plików będą posiadać różne sumy kontrolne.

     - Certyfikat pliku. Kaspersky Security Center doda wszystkie pliki wykonywalne podpisane określonym certyfikatem do kategorii aplikacji.

     - Kategoria KL. Kaspersky Security Center doda wszystkie aplikacje, które znajdują się w określonej kategorii KL, do kategorii aplikacji.

- Folder aplikacji. Kaspersky Security Center doda wszystkie pliki wykonywalne z tego folderu do kategorii aplikacji.

  Użycie warunku **Folder aplikacji** może nie być bezpieczne, ponieważ każda aplikacja z określonego folderu będzie mogła być uruchamiana. Zalecane jest zastosowanie reguł, które używają kategorii aplikacji z warunkiem **Folder aplikacji**, tylko do tych użytkowników, dla których musi być dozwolona automatyczna instalacja uaktualnień.

- **Kategoria zawierająca pliki wykonywalne z określonego folderu**. Możesz określić folder, z którego pliki wykonywalne będą automatycznie przydzielane do utworzonej kategorii aplikacji.

- **Kategoria zawierająca pliki wykonywalne z wybranych urządzeń**. Możesz określić komputer, z którego wszystkie pliki wykonywalne będą automatycznie przydzielane do utworzonej kategorii aplikacji.

  Jeśli użyjesz tej metody do utworzenia kategorii aplikacji, Kaspersky Security Center będzie otrzymywał informacje o aplikacjach na komputerze z folderu **Pliki wykonywalne**.

2. Wybierz tryb listy zezwolonych dla komponentu Kontrola aplikacji.

3. Utwórz reguły Kontroli aplikacji, korzystając z utworzonych kategorii aplikacji.

   Reguła **Obraz systemu** oraz reguła **Zaufane programy aktualizujące** jest wstępnie definiowana dla trybu Lista zezwolonych. Te reguły Kontroli aplikacji odpowiadają kategoriom KL. Kategoria KL *Obraz systemu* obejmuje programy, które zapewniają normalne działanie systemu operacyjnego. Kategoria KL *Zaufane programy aktualizujące* zawiera programy aktualizujące dla większości zaufanych producentów oprogramowania. Nie możesz usunąć tych reguł. Ustawienia dla tych reguł nie mogą być modyfikowane. Domyślnie, reguła **Obraz systemu** jest włączona, a reguła **Zaufane programy aktualizujące** jest wyłączona. Wszyscy użytkownicy mogą uruchamiać aplikacje odpowiadające warunkom wyzwalającym te reguły.

4. Określ aplikacje, dla których dozwolona musi być automatyczna instalacja uaktualnień.

   Możesz zezwolić na automatyczną instalację uaktualnień w jeden z następujących sposobów:

   - Określ rozszerzoną listę dozwolonych aplikacji, zezwalając na uruchamianie wszystkich aplikacji, które należą do dowolnej kategorii KL.

   - Określ rozszerzoną listę dozwolonych aplikacji, zezwalając na uruchamianie wszystkich aplikacji, które są podpisane certyfikatami.

     Aby zezwolić na uruchomienie wszystkich aplikacji podpisanych certyfikatami, możesz utworzyć kategorię z warunkiem opartym o certyfikat, który używa tylko parametru **Temat** z wartością `*`.

   - Dla reguł Kontroli aplikacji wybierz parametr **Zaufane programy aktualizujące**. Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security traktuje aplikacje, uwzględnione w regule, jako Zaufane programy aktualizujące. Kaspersky Endpoint Security zezwala na uruchamianie aplikacji, które zostały zainstalowane lub zaktualizowane przez aplikacje uwzględnione w regule, jeśli nie są do nich stosowane żadne reguły blokujące.

     Jeśli przenosisz ustawienia Kaspersky Endpoint Security, lista plików wykonywalnych utworzonych przez zaufane programy aktualizujące także zostanie przeniesiona.

- Utwórz folder i umieść w nim pliki wykonywalne aplikacji, dla których chcesz zezwolić na automatyczną instalację aktualizacji. Następnie utwórz kategorię aplikacji z warunkiem **Folder aplikacji** i określ ścieżkę do tego folderu. Kolejnym krokiem jest utworzenie reguły zezwalającej i wybranie tej kategorii.

  Użycie warunku **Folder aplikacji** może nie być bezpieczne, ponieważ każda aplikacja z określonego folderu będzie mogła być uruchamiana. Zalecane jest zastosowanie reguł, które używają kategorii aplikacji z warunkiem **Folder aplikacji**, tylko do tych użytkowników, dla których musi być dozwolona automatyczna instalacja uaktualnień.

Testowanie trybu listy zezwolonych

Aby upewnić się, że reguły Kontroli aplikacji nie będą blokowały aplikacji niezbędnych do pracy, po utworzeniu nowych reguł zalecane jest włączenie testowania reguł Kontroli aplikacji i sprawdzenie ich działania. Jeśli testowanie jest włączone, Kaspersky Endpoint Security nie zablokuje aplikacji, których uruchamianie jest zabronione przez reguły Kontroli aplikacji, ale zamiast tego wyśle informacje o ich uruchomieniu do Serwera administracyjnego.

Podczas testowania listy zezwolonych zalecane jest wykonanie następujących działań:

1. Określenie okresu testowego (liczącego od kilku dni do dwóch miesięcy).
2. Włącz testowanie reguł Kontroli aplikacji.
3. Sprawdź zdarzenia będące wynikiem testowania działania Kontroli aplikacji i raporty dotyczące zablokowanych aplikacji w trybie testowym w celu przeanalizowania wyników testu.
4. W oparciu o wyniki analizy, wprowadź zmiany w ustawieniach trybu listy zezwolonych.

   W szczególności na podstawie wyników testu można dodać pliki wykonywalne związane ze zdarzeniami do kategorii aplikacji.

Obsługa listy zezwolonych aplikacji

Po wybraniu akcji blokowania dla Kontroli aplikacji, zalecane jest kontynuowanie wsparcia trybu listy zezwolonych poprzez wykonanie następujących czynności:

- Sprawdź zdarzenia będące wynikiem działania Kontroli aplikacji i raporty dotyczące zablokowanych uruchomień w celu przeanalizowania efektywności działania Kontroli aplikacji.
- Przeanalizuj prośby użytkowników o dostęp do aplikacji.
- Analizuj nieznane pliki wykonywalne, sprawdzając ich reputację w Kaspersky Security Network.
- Przed zainstalowaniem uaktualnień dla systemu operacyjnego lub dla oprogramowania, zainstaluj te uaktualnienia na testowej grupie komputerów, aby sprawdzić sposób ich przetwarzania przez reguły Kontroli aplikacji.
- Dodaj odpowiednie aplikacje do kategorii użytych w regułach Kontroli aplikacji.

Monitorowanie portów sieciowych

Podczas działania Kaspersky Endpoint Security komponenty Kontrola sieci, Ochrona poczty, Ochrona WWW, Wykrywanie zachowań i Ochrona przed exploitami monitorują strumienie danych, które są przesyłane za pośrednictwem określonych protokołów i które przechodzą przez określone otwarte porty TCP i UDP na komputerze użytkownika. Na przykład, komponent Ochrona poczty analizuje informacje przesyłane poprzez protokół SMTP, a komponent Ochrona WWW analizuje informacje przesyłane poprzez protokół HTTP i FTP.

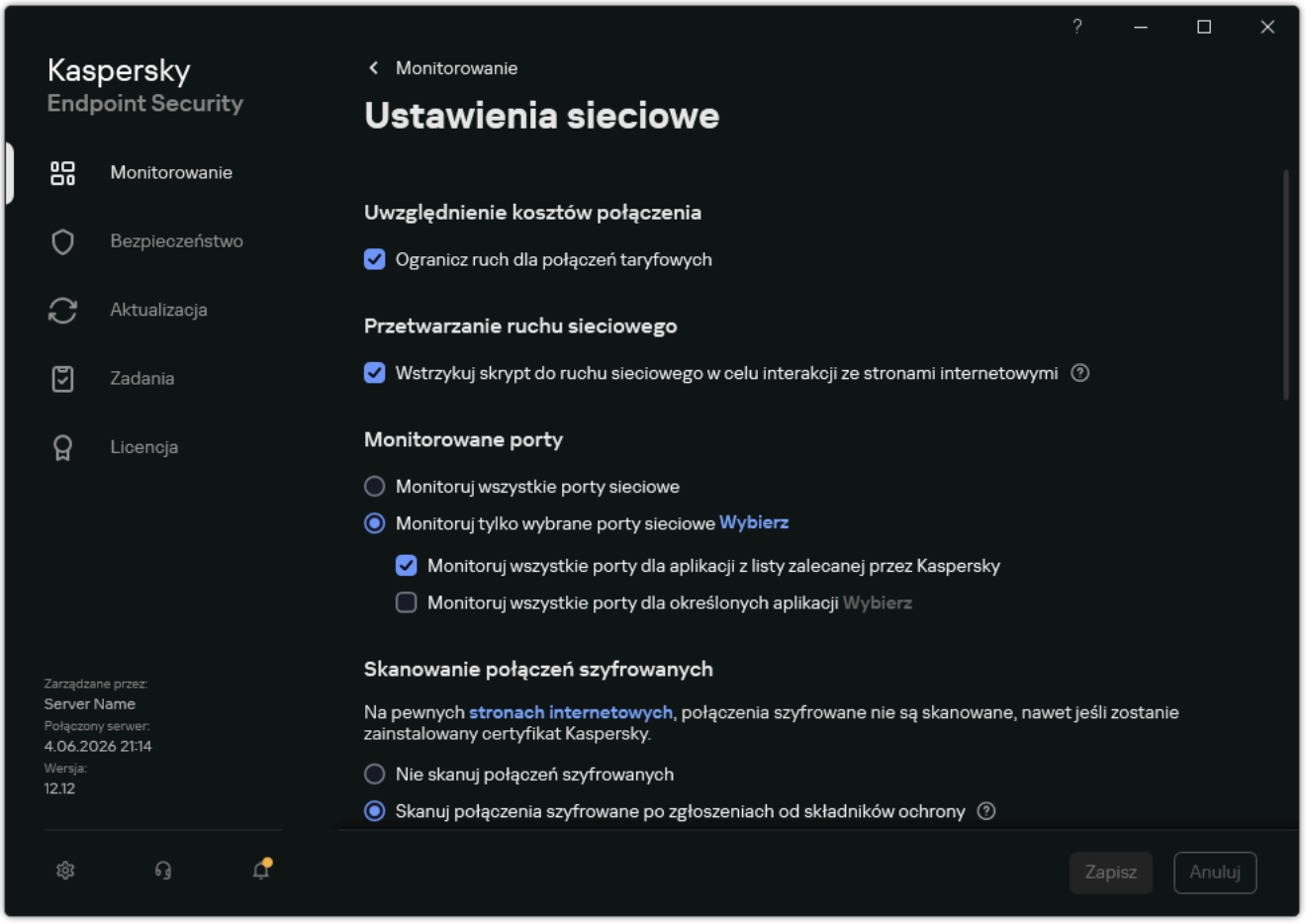
Kaspersky Endpoint Security dzieli porty TCP i UDP komputera użytkownika na kilka grup, w zależności od prawdopodobieństwa ich zagrożenia. Niektóre porty sieciowe są zarezerwowane dla usług podatnych na ataki. Zalecane jest monitorowanie tych portów z większą dokładnością, ponieważ istnieje większe prawdopodobieństwo, że staną się one celem ataku sieciowego. Jeśli korzystasz z niestandardowych usług polegających na niestandardowych portach, te porty sieciowe również mogą stać się celem atakującego komputera. Możesz określić listę portów sieciowych i listę aplikacji, które żądają dostępu do sieci. Te porty i aplikacje będą pod specjalnym nadzorem modułów Ochrona poczty i Ochrona WWW podczas monitorowania ruchu sieciowego.

Aby zapewnić bezpieczeństwo komputera, komponenty Wykrywanie zachowań i Ochrona przed exploitami monitorują również strumienie danych przechodzące przez porty sieciowe. Komponenty te stale monitorują ruch sieciowy w poszukiwaniu poszczególnych procesów, które mogą stanowić zagrożenie.

Włączanie monitorowania wszystkich portów sieciowych

W celu włączenia monitorowania wszystkich portów sieciowych:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.



Ustawienia monitoringu portów sieciowych

3. W bloku **Monitorowane porty** wybierz **Monitoruj wszystkie porty sieciowe**.
4. Zapisz swoje zmiany.

Tworzenie listy monitorowanych portów sieciowych

Zmiana listy monitorowanych portów sieciowych może zostać zablokowana przez właściwości zasady nadrzędnej. Aby zmienić listę, musisz zezwolić na zmianę ustawień strefy zaufanej w Web Console (kłódka musi być odblokowana).

Strefy zaufane są grupowane w różny sposób w Konsoli administracyjnej (MMC) i Web Console. Sposoby zapobiegania zmianom parametrów strefy zaufanej również mogą się różnić („kłódki" mogą być inne). Zalecamy korzystanie wyłącznie z Web Console do zarządzania aplikacją. Jeśli skonfigurujesz strefę zaufaną w różnych konsolach, wtyczka zarządzająca może przywrócić „kłódkę" do stanu domyślnego.

W celu utworzenia listy monitorowanych portów sieciowych:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
3. W bloku **Monitorowane porty** wybierz **Monitoruj tylko wybrane porty sieciowe**.
4. Kliknij **Wybierz**.

   Spowoduje to otwarcie listy portów sieciowych, które są zazwyczaj używane do przesyłania ruchu sieciowego i pocztowego. Lista portów sieciowych jest zawarta w pakiecie Kaspersky Endpoint Security.
5. Użyj przełącznika w kolumnie **Stan**, aby włączyć lub wyłączyć monitorowanie portu sieciowego.
6. Jeśli post sieciowy nie jest wyświetlany na liście portów sieciowych, dodaj go w następujący sposób:

   a. Kliknij **Dodaj**.

   b. W otwartym oknie wprowadź numer portu sieciowego oraz krótki opis.

   c. Ustaw stan **Aktywny** lub **Nieaktywny** dla monitorowania portu sieciowego.
7. Zapisz swoje zmiany.

Jeśli protokół FTP działa w trybie pasywnym, połączenie będzie można nawiązać poprzez losowy port sieciowy, który nie został dodany do listy monitorowanych portów sieciowych. Aby chronić takie połączenia, włącz monitorowanie wszystkich portów sieciowych lub skonfiguruj kontrolę portów sieciowych dla aplikacji, które nawiązują połączenia z FTP.

Tworzenie listy aplikacji, dla których monitorowane są wszystkie porty sieciowe

Możesz utworzyć listę aplikacji, dla których Kaspersky Endpoint Security monitoruje wszystkie porty sieciowe.

Zalecamy uwzględnić aplikacje odbierające lub przesyłające dane przez protokół FTP na liście aplikacji, dla których Kaspersky Endpoint Security monitoruje wszystkie porty sieciowe.

W celu utworzenia listy aplikacji, dla których monitorowane są wszystkie porty sieciowe:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.
3. W bloku **Monitorowane porty** wybierz **Monitoruj tylko wybrane porty sieciowe**.
4. Zaznacz pole **Monitoruj wszystkie porty dla aplikacji z listy zalecanej przez Kaspersky**.

   Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security monitoruje wszystkie porty dla następujących aplikacji:

   - Adobe Acrobat Reader.
   - Apple Application Support.
   - Google Chrome.
   - Microsoft Edge.
   - Mozilla Firefox.
   - Internet Explorer.
   - Java.
   - mIRC.
   - Opera.
   - Pidgin.
   - Safari.
   - Mail.ru Agent.
   - Yandex Browser.
5. Zaznacz pole **Monitoruj wszystkie porty dla określonych aplikacji**.

6. Kliknij **Wybierz**.

   Spowoduje to otwarcie listy aplikacji, dla których Kaspersky Endpoint Security monitoruje porty sieciowe.

7. Użyj przełącznika w kolumnie **Stan**, aby włączyć lub wyłączyć monitorowanie portu sieciowego.

8. Jeśli aplikacja nie znajduje się na liście aplikacji, dodaj ją w następujący sposób:

   a. Kliknij **Dodaj**.

   b. W otwartym oknie wprowadź ścieżkę do pliku wykonywalnego aplikacji oraz krótki opis.

   c. Ustaw stan **Aktywny** lub **Nieaktywny** dla monitorowania portów sieciowych.

9. Zapisz swoje zmiany.

Eksportowanie i importowanie list monitorowanych portów

Kaspersky Endpoint Security używa następujących list monitorowania portów sieciowych: listy portów sieciowych i listy aplikacji, których porty są monitorowane przez Kaspersky Endpoint Security. Możesz wyeksportować listy monitorowanych portów do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę portów z tym samym opisem. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej list monitorowanych portów lub przeniesienia list na inny serwer.

Eksportowanie i importowanie list monitorowanych portów w Konsoli administracyjnej (MMC)

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne** → **Ustawienia sieciowe**.

5. W celu wyeksportowania listy portów sieciowych:

   a. W bloku **Monitorowane porty** wybierz **Monitoruj tylko wybrane porty sieciowe**.

   b. Kliknij odnośnik **wybranych N portów**.

      Zostanie otwarte okno **Porty sieciowe**. W oknie **Porty sieciowe** wyświetlana jest lista portów sieciowych, które są zazwyczaj używane do przesyłania ruchu sieciowego i pocztowego. Lista portów sieciowych jest zawarta w pakiecie Kaspersky Endpoint Security.

   c. Z listy portów sieciowych wybierz porty, które chcesz wyeksportować.

   d. Kliknij **Eksportuj**.

   e. W otwartym oknie wprowadź nazwę pliku XML, do którego chcesz wyeksportować listę portów sieciowych, i wybierz folder, w którym chcesz zapisać ten plik.

   f. Zapisz plik.

      Kaspersky Endpoint Security eksportuje całą listę portów sieciowych do pliku XML.

6. W celu wyeksportowania listy aplikacji, których porty są monitorowane przez Kaspersky Endpoint Security:

   a. W sekcji **Monitorowane porty** zaznacz pole **Monitoruj wszystkie porty dla określonych aplikacji**.

   b. Kliknij odnośnik **wybranych N aplikacji**.

   c. Z listy aplikacji wybierz aplikacje, które chcesz wyeksportować.

   d. Kliknij **Eksportuj**.

   e. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę aplikacji, i wybierz folder, w którym chcesz zapisać ten plik.

   f. Zapisz plik.

   Kaspersky Endpoint Security wyeksportuje całą listę aplikacji do pliku XML.

7. W celu zaimportowania listy portów sieciowych:

   a. Na liście portów sieciowych kliknij przycisk **Importuj**.

   W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę portów sieciowych.

   b. Otwórz plik.

   Jeśli komputer ma już listę portów sieciowych, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

8. W celu zaimportowania listy aplikacji, których porty są monitorowane przez Kaspersky Endpoint Security:

   a. Na liście aplikacji kliknij przycisk **Importuj**.

   W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę aplikacji.

   b. Otwórz plik.

   Jeśli komputer ma już listę aplikacji, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

9. Zapisz swoje zmiany.

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Ustawienia ogólne → Ustawienia sieciowe**.

4. W bloku **Monitorowane porty** wybierz **Monitoruj tylko wybrane porty sieciowe**.

5. Kliknij **Ustawienia**.

   Zostanie otwarte okno **Porty sieciowe**. W oknie **Porty sieciowe** wyświetlana jest lista portów sieciowych, które są zazwyczaj używane do przesyłania ruchu sieciowego i pocztowego. Lista portów sieciowych jest zawarta w pakiecie Kaspersky Endpoint Security.

6. W celu wyeksportowania listy portów sieciowych:

   a. Z listy portów sieciowych wybierz porty, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.

      Jeśli nie wybrałeś żadnego portu, Kaspersky Endpoint Security wyeksportuje wszystkie porty.

   b. Kliknij **Eksportuj**.

   c. W otwartym oknie wprowadź nazwę pliku XML, do którego chcesz wyeksportować listę portów sieciowych, i wybierz folder, w którym chcesz zapisać ten plik.

   d. Zapisz plik.

      Kaspersky Endpoint Security eksportuje całą listę portów sieciowych do pliku XML.

7. W celu wyeksportowania listy aplikacji, których porty są monitorowane przez Kaspersky Endpoint Security:

   a. Zaznacz pole **Monitoruj wszystkie porty dla określonych aplikacji**.

   b. Z listy aplikacji wybierz aplikacje, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.

      Jeśli nie wybrałeś żadnej aplikacji, Kaspersky Endpoint Security wyeksportuje wszystkie aplikacje.

   c. Kliknij **Eksportuj**.

   d. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę aplikacji, i wybierz folder, w którym chcesz zapisać ten plik.

   e. Zapisz plik.

      Kaspersky Endpoint Security wyeksportuje całą listę aplikacji do pliku XML.

8. W celu zaimportowania listy portów sieciowych:

   a. Na liście portów sieciowych kliknij przycisk **Importuj**.

      W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę portów sieciowych.

   b. Otwórz plik.

      Jeśli komputer ma już listę portów sieciowych, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

9. W celu zaimportowania listy aplikacji, których porty są monitorowane przez Kaspersky Endpoint Security:

   a. Na liście aplikacji kliknij przycisk **Importuj**.

      W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę aplikacji.

   b. Otwórz plik.

      Jeśli komputer ma już listę aplikacji, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

10. Zapisz swoje zmiany.

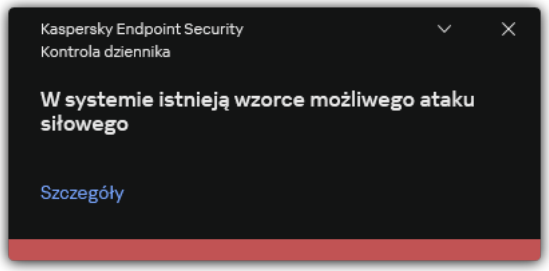
Kontrola dziennika

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych.

Począwszy od wersji 11.11.0 Kaspersky Endpoint Security for Windows zawiera komponent Kontrola dziennika. Komponent Kontrola dziennika monitoruje integralność chronionego środowiska na podstawie analizy dziennika zdarzeń systemu Windows. Gdy aplikacja wykryje oznaki nietypowego zachowania w systemie, informuje o tym administratora, gdyż zachowanie to może świadczyć o próbie cyberataku.

Kaspersky Endpoint Security analizuje dzienniki zdarzeń systemu Windows i wykrywa naruszenia zgodnie z regułami. Komponent ten zawiera wstępnie zdefiniowane reguły. Wstępnie zdefiniowane reguły są oparte na analizie heurystycznej. Można również dodać własne reguły (reguły niestandardowe). W momencie uruchomienia reguły aplikacja tworzy zdarzenie o stanie *Krytyczny* (patrz rysunek poniżej).

Jeśli chcesz użyć komponentu Kontrola dziennika, upewnij się, że skonfigurowane są ustawienia zabezpieczeń polityki audytu, a system rejestruje odpowiednie zdarzenia (szczegóły znajdziesz na stronie pomocy technicznej firmy Microsoft).



Powiadomienie z kontroli dziennika

Konfiguracja wstępnie zdefiniowanych reguł

Wstępnie zdefiniowane reguły zawierają szablony nieprawidłowej aktywności na chronionym komputerze. Nietypowa aktywność może oznaczać próbę ataku. Wstępnie zdefiniowane reguły są oparte na analizie heurystycznej. Dla funkcji Kontroli dziennika dostępnych jest siedem wstępnie zdefiniowanych reguł. Reguły te można włączać lub wyłączać. Wstępnie zdefiniowanych reguł nie można usunąć.

Można skonfigurować kryteria wyzwalania dla reguł monitorujących zdarzenia dla następujących operacji:

- Wykrywanie ataków siłowych w celu złamania hasła
- Wykrywanie logowania w sieci

Jak skonfigurować wstępnie zdefiniowane reguły w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń → Kontrola dziennika**.
4. Należy upewnić się, że pole **Kontrola dziennika** jest zaznaczone.
5. W sekcji **Wstępnie zdefiniowane reguły** kliknij przycisk **Ustawienia**.
6. Należy zaznaczyć lub wyczyścić pola wyboru, aby skonfigurować wstępnie zdefiniowane reguły:
   - **W systemie istnieją wzorce możliwego ataku siłowego**.
   - **Podczas sesji logowania do sieci wykryto nietypową aktywność**.
   - **W systemie istnieją wzorce możliwego nadużycia dziennika zdarzeń systemu Windows**.
   - **Wykryto nietypowe działania w imieniu nowej zainstalowanej usługi**.
   - **Wykryto nietypowe logowanie wykorzystujące jawne dane uwierzytelniające**.
   - **W systemie istnieją wzorce możliwego ataku Kerberos PAC (MS14-068)**.
   - **Podejrzane zmiany wykryte w uprzywilejowanej wbudowanej grupie Administratorzy**.
7. Jeśli to konieczne, należy skonfigurować regułę **W systemie istnieją wzorce możliwego ataku siłowego**:
   a. Kliknąć przycisk **Ustawienia** poniżej reguły.
   b. W otwartym oknie należy określić liczbę prób oraz czas, w którym muszą nastąpić próby wprowadzenia hasła, aby reguła została uruchomiona.
   c. Kliknij **OK**.
8. W przypadku wybrania reguły **Podczas sesji logowania do sieci wykryto nietypową aktywność** musisz skonfigurować jej ustawienia:
   a. Kliknąć przycisk **Ustawienia** poniżej reguły.
   b. W sekcji **Wykrywanie logowania do sieci**, należy określić początek i koniec przedziału czasowego.

      Kaspersky Endpoint Security uznaje próby logowania wykonane podczas określonego interwału za nieprawidłową aktywność.

      Domyślnie interwał nie jest ustawiony i aplikacja nie monitoruje prób logowania. Aby aplikacja stale monitorowała próby logowania, ustaw przedział czasowy na 00:00–23:59. Początek i koniec interwału nie mogą się pokrywać. Jeśli są takie same, aplikacja nie monitoruje prób logowania.

c. Należy utworzyć listę zaufanych użytkowników i zaufanych adresów IP (IPv4 i IPv6).

Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny. Kaspersky Endpoint Security nie monitoruje prób logowania dla tych użytkowników i komputerów.

d. Kliknij **OK**.

9. Zapisz swoje zmiany.

Jak skonfigurować wstępnie zdefiniowane reguły w konsoli Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń** → **Kontrola dziennika**.
5. Należy upewnić się, że włączony jest przełącznik **Kontrola dziennika WŁĄCZONA**.
6. W sekcji **Wstępnie zdefiniowane reguły**, należy włączyć lub wyłączyć wstępnie zdefiniowane reguły za pomocą przełączników:

   - **W systemie istnieją wzorce możliwego ataku siłowego**.
   - **Podczas sesji logowania do sieci wykryto nietypową aktywność**.
   - **W systemie istnieją wzorce możliwego nadużycia dziennika zdarzeń systemu Windows**.
   - **Wykryto nietypowe działania w imieniu nowej zainstalowanej usługi**.
   - **Wykryto nietypowe logowanie wykorzystujące jawne dane uwierzytelniające**.
   - **W systemie istnieją wzorce możliwego ataku Kerberos PAC (MS14-068)**.

   a. **Podejrzane zmiany wykryte w uprzywilejowanej wbudowanej grupie Administratorzy**.
7. Jeśli to konieczne, należy skonfigurować regułę **W systemie istnieją wzorce możliwego ataku siłowego**:

   a. Kliknąć przycisk **Ustawienia** pod regułą.

   b. W otwartym oknie należy określić liczbę prób oraz czas, w którym muszą nastąpić próby wprowadzenia hasła, aby reguła została uruchomiona.

   c. Kliknij **OK**.
8. W przypadku wybrania reguły **Podczas sesji logowania do sieci wykryto nietypową aktywność** musisz skonfigurować jej ustawienia:

   a. Kliknąć przycisk **Ustawienia** pod regułą.

   b. W sekcji **Wykrywanie logowania do sieci**, należy określić początek i koniec przedziału czasowego.

Kaspersky Endpoint Security uznaje próby logowania wykonane podczas określonego interwału za nieprawidłową aktywność.

Domyślnie interwał nie jest ustawiony i aplikacja nie monitoruje prób logowania. Aby aplikacja stale monitorowała próby logowania, ustaw przedział czasowy na 00:00–23:59. Początek i koniec interwału nie mogą się pokrywać. Jeśli są takie same, aplikacja nie monitoruje prób logowania.

c. W sekcji **Wykluczenia** należy dodać zaufanych użytkowników i zaufane adresy IP (IPv4 i IPv6).

Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny. Kaspersky Endpoint Security nie monitoruje prób logowania dla tych użytkowników i komputerów.

d. Kliknij **OK**.

9. Zapisz swoje zmiany.

Jak skonfigurować wstępnie zdefiniowane reguły w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola dziennika**.
3. Należy upewnić się, że włączony jest przełącznik **Kontrola dziennika**.
4. W sekcji **Wstępnie zdefiniowane reguły** kliknij przycisk **Konfiguruj**.
5. Należy zaznaczyć lub wyczyścić pola wyboru, aby skonfigurować wstępnie zdefiniowane reguły:
   - **W systemie istnieją wzorce możliwego ataku siłowego**.
   - **Podczas sesji logowania do sieci wykryto nietypową aktywność**.
   - **W systemie istnieją wzorce możliwego nadużycia dziennika zdarzeń systemu Windows**.
   - **Wykryto nietypowe działania w imieniu nowej zainstalowanej usługi**.
   - **Wykryto nietypowe logowanie wykorzystujące jawne dane uwierzytelniające**.
   - **W systemie istnieją wzorce możliwego ataku Kerberos PAC (MS14-068)**.

   a. **Podejrzane zmiany wykryte w uprzywilejowanej wbudowanej grupie Administratorzy**.
6. Jeśli to konieczne, należy skonfigurować regułę **W systemie istnieją wzorce możliwego ataku siłowego**:

   a. Kliknąć przycisk **Ustawienia** pod regułą.

   b. W otwartym oknie należy określić liczbę prób oraz czas, w którym muszą nastąpić próby wprowadzenia hasła, aby reguła została uruchomiona.
7. W przypadku wybrania reguły **Podczas sesji logowania do sieci wykryto nietypową aktywność** musisz skonfigurować jej ustawienia:

   a. Kliknąć przycisk **Ustawienia** pod regułą.

   b. W sekcji **Wykrywanie logowania do sieci**, należy określić początek i koniec przedziału czasowego.

Kaspersky Endpoint Security uznaje próby logowania wykonane podczas określonego interwału za nieprawidłową aktywność.

Domyślnie interwał nie jest ustawiony i aplikacja nie monitoruje prób logowania. Aby aplikacja stale monitorowała próby logowania, ustaw przedział czasowy na 00:00–23:59. Początek i koniec interwału nie mogą się pokrywać. Jeśli są takie same, aplikacja nie monitoruje prób logowania.

c. W sekcji **Wykluczenia** należy dodać zaufanych użytkowników i zaufane adresy IP (IPv4 i IPv6).

Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny. Kaspersky Endpoint Security nie monitoruje prób logowania dla tych użytkowników i komputerów.

8. Zapisz swoje zmiany.

W rezultacie, gdy reguła zostanie uruchomiona, Kaspersky Endpoint Security utworzy *Zdarzenie krytyczne*.

Dodawanie reguł niestandardowych

Można ustawić własne kryteria wyzwalania reguły kontroli dziennika. Aby to zrobić, należy wprowadzić identyfikator zdarzenia i wybrać źródło zdarzenia. Identyfikator zdarzenia można sprawdzić na stronie internetowej pomocy technicznej firmy Microsoft. Można wybrać źródło zdarzeń spośród standardowych dzienników: *Application*, *Security* lub *System*. Można również określić dziennik aplikacji innej firmy. Nazwę dziennika aplikacji innej firmy można poznać za pomocą narzędzia Event Viewer. Dzienniki aplikacji innych firm są przechowywane w folderze Application and Services Logs (na przykład dziennik programu *Windows PowerShell*).

Aplikacja nie sprawdza, czy określony dziennik jest rzeczywiście obecny w dzienniku zdarzeń systemu Windows. Jeśli w nazwie dziennika jest błąd, aplikacja nie monitoruje zdarzeń z tego dziennika.

Na liście reguł niestandardowych znajdują się już trzy reguły stworzone przez ekspertów firmy Kaspersky.

Jak dodawać reguły niestandardowe w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola dziennika**.
4. Należy upewnić się, że pole **Kontrola dziennika** jest zaznaczone.
5. W sekcji **Reguły niestandardowe** kliknij przycisk **Ustawienia**.
6. W otwartym oknie zaznacz pola wyboru obok reguł niestandardowych, które chcesz włączyć.
7. W razie konieczności, kliknij **Dodaj**, aby stworzyć własne reguły niestandardowe.
8. Spowoduje to otwarcie okna; w tym oknie należy skonfigurować regułę niestandardową:
   - **Nazwa reguły**.
   - **Nazwa dziennika**. Dzienniki zdarzeń systemu Windows. Dostępne są następujące dzienniki: *Application*, *Security*, *System*.

- **Źródło**. Dzienniki aplikacji innych firm. Nazwę dziennika aplikacji innej firmy można poznać za pomocą narzędzia Event Viewer. Dzienniki aplikacji innych firm są przechowywane w folderze Application and Services Logs (na przykład dziennik programu *Windows PowerShell*).

- **Identyfikatory zdarzenia**. Identyfikatory zdarzeń w dzienniku zdarzeń systemu Windows. Identyfikator zdarzenia można sprawdzić w dokumentacji technicznej firmy Microsoft.

9. Zapisz swoje zmiany.

Jak dodać regułę niestandardową w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń** → **Kontrola dziennika**.
5. Należy upewnić się, że włączony jest przełącznik **Kontrola dziennika WŁĄCZONA**.
6. W sekcji **Reguły niestandardowe** wybierz reguły niestandardowe, które chcesz włączyć.
7. W razie konieczności, kliknij **Dodaj**, aby stworzyć własne reguły niestandardowe.
8. Spowoduje to otwarcie okna; w tym oknie należy skonfigurować regułę niestandardową:

   - **Nazwa reguły**.
   - **Niestandardowa nazwa dziennika**. Dzienniki zdarzeń systemu Windows. Dostępne są następujące dzienniki: *Application*, *Security*, *System*.
   - **Pochodzenie**. Dzienniki aplikacji innych firm. Nazwę dziennika aplikacji innej firmy można poznać za pomocą narzędzia Event Viewer. Dzienniki aplikacji innych firm są przechowywane w folderze Application and Services Logs (na przykład dziennik programu *Windows PowerShell*).
   - **Identyfikatory zdarzenia**. Identyfikatory zdarzeń w dzienniku zdarzeń systemu Windows. Identyfikator zdarzenia można sprawdzić w dokumentacji technicznej firmy Microsoft.
9. Zapisz swoje zmiany.

Jak dodać regułę niestandardową w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola dziennika**.
3. Należy upewnić się, że włączony jest przełącznik **Kontrola dziennika**.
4. W sekcji **Reguły niestandardowe** kliknij przycisk **Konfiguruj**.
5. W otwartym oknie zaznacz pola wyboru obok reguł niestandardowych, które chcesz włączyć.
6. W razie konieczności, kliknij **Dodaj**, aby stworzyć własne reguły niestandardowe.

7. Spowoduje to otwarcie okna; w tym oknie należy skonfigurować regułę niestandardową:

   - **Nazwa reguły**.
   - **Nazwa dziennika**. Dzienniki zdarzeń systemu Windows. Dostępne są następujące dzienniki: *Application*, *Security*, *System*.
   - **Źródło**. Dzienniki aplikacji innych firm. Nazwę dziennika aplikacji innej firmy można poznać za pomocą narzędzia Event Viewer. Dzienniki aplikacji innych firm są przechowywane w folderze Application and Services Logs (na przykład dziennik programu *Windows PowerShell*).
   - **Identyfikator zdarzenia**. Identyfikatory zdarzeń w dzienniku zdarzeń systemu Windows. Identyfikator zdarzenia można sprawdzić w dokumentacji technicznej firmy Microsoft.

8. Zapisz swoje zmiany.

W rezultacie, gdy reguła zostanie uruchomiona, Kaspersky Endpoint Security utworzy zdarzenie *krytyczne*.

Monitor integralności systemu

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych.

Począwszy odd wersji 12.6 Kaspersky Endpoint Security for Windows zawiera komponent Monitorowanie integralności systemu zamiast komponentu Monitora integralności plików. Komponent Monitorowanie integralności systemu zawiera całą funkcjonalność Monitora integralności plików oraz dodatkowo pozwala na monitorowanie zmian w rejestrze i podłączania urządzeń zewnętrznych.

Monitorowanie integralności systemu monitoruje zmiany w systemie operacyjnym, które mogą wskazywać na naruszenia bezpieczeństwa komputera. Po wykryciu takich zmian Kaspersky Endpoint Security generuje odpowiednie zdarzenia i powiadamia administratora. Monitorowanie integralności systemu może działać w trybie czasu rzeczywistego i może również przeprowadzać sprawdzanie integralności systemu na żądanie.

Monitorowanie integralności systemu w czasie rzeczywistym

W trybie czasu rzeczywistego Monitor integralności systemu śledzi zmiany w obiektach, które włączono w zakres komponentu (*zakres monitorowania*). Monitorowanie integralności systemu umożliwia także blokowanie nieuprawnionego dostępu do takich obiektów w czasie rzeczywistym.

Sprawdzanie integralności systemu na żądanie

Sprawdzanie integralności systemu na żądanie to zadanie, które możesz uruchomić ręcznie lub zgodnie z harmonogramem. Aby uruchomić zadanie *Sprawdzanie integralności systemu*, musisz skonfigurować zakres komponentu (*zakres monitorowania*) i utworzyć punkt odniesienia. *Punkt odniesienia* to zarejestrowany status obiektów w systemie, który aplikacja wykorzystuje jako odniesienie przy porównywaniu ze stanem bieżącym.

Migracja ustawień Monitora integralności plików

Kiedy aktualizujesz Kaspersky Endpoint Security do wersji 12.6, ustawienia Monitora integralności plików ulegają automatycznej migracji. W ramach migracji, aplikacja przenosi reguły monitorowania do Monitorowania integralności systemu. Reguły Monitora integralności plików są również przenoszone do Monitorowania integralności systemu podczas migracji z KSWS do KES.

Aby zapewnić prawidłowe działanie Monitora integralności systemu, aplikacja Kaspersky Endpoint Security i wtyczka zarządzająca powinny zostać zaktualizowane do wersji 12.6. Jeśli masz zainstalowaną wcześniejszą wersję wtyczki zarządzającej, nie możesz skonfigurować Monitora integralności systemu, ponieważ wtyczka zarządzająca nie ma sekcji **Monitor integralności systemu**.

Informacje o regułach monitorowania integralności systemu

Aby Monitor integralności systemu działał, musisz dodać co najmniej jedną regułę. *Reguła Monitorowania integralności systemu* to zbiór kryteriów definiujących dostęp użytkowników do plików i rejestru. Monitorowanie integralności systemu wykrywa zmiany w plikach i rejestrze w określonym *zakresie monitorowania*. Zakres monitorowania jest jednym z kryteriów reguły Monitorowania integralności systemu.

Monitorowanie integralności systemu umożliwia monitorowanie następujących obiektów:

- Plików
- Rejestru
- Urządzeń zewnętrznych

Specjalne aspekty związane z monitorowaniem plików

Monitorowanie integralności systemu monitoruje zmiany w plikach i folderach oraz pliki dodawane do zakresu monitorowania lub z niego usuwane. Zmiany te mogą świadczyć o naruszeniu bezpieczeństwa komputera. Zalecamy dodawanie obiektów rzadko modyfikowanych lub obiektów, do których dostęp ma tylko administrator. Pomaga to zmniejszyć liczbę zdarzeń Monitorowania integralności systemu.

Monitorowanie integralności systemu nie monitoruje zmian w plikach znajdujących się w folderach współdzielonych na serwerze. Monitorowanie integralności systemu można stosować wyłącznie lokalnie.

Kaspersky Endpoint Security monitoruje zmiany plików i folderów tylko na tych dyskach, które zostały podłączone, gdy zaczęło działać Monitorowanie integralności systemu w czasie rzeczywistym. Jeżeli dysk nie był podłączony w momencie rozpoczęcia działania Monitorowania integralności systemu w czasie rzeczywistym, aplikacja nie monitoruje zmian w plikach i folderach na tym dysku nawet jeśli pliki i foldery zostają dodane do zakresu monitorowania.

Specjalne aspekty związane z monitorowaniem rejestru

Monitorowanie integralności systemu monitoruje rejestr. Zmiany te mogą świadczyć o naruszeniu bezpieczeństwa komputera.

Monitorowanie integralności systemu monitoruje następujące klucze główne rejestru:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG` (dostępne tylko w Monitorze integralności systemu w czasie rzeczywistym)
- `HKEY_CURRENT_USER` (dostępne tylko w Monitorze integralności systemu w czasie rzeczywistym)

> Zadanie *Sprawdzanie integralności systemu* nie obsługuje klucza `HKEY_CURRENT_USER`. Możesz określić klucz w obszarze `HKEY_USERS` jako `HKEY_USERS\<user profile ID>\<key>`.

Specjalne aspekty związane z monitorowaniem urządzeń zewnętrznych

Monitorowanie integralności systemu monitoruje podłączanie i odłączanie urządzeń zewnętrznych. Jest to konieczne, aby chronić komputer przed zagrożeniami bezpieczeństwa, które mogą wynikać z wymiany plików z takimi urządzeniami. Monitorowanie integralności systemu nie monitoruje dostępu do urządzeń zewnętrznych i nie blokuje wymiany plików. Możesz skonfigurować dostęp do urządzeń za pomocą innego komponentu aplikacji, Kontroli urządzeń.

> Podczas uruchamiania zadania *Podstawowe monitorowanie integralności systemu* aplikacja ignoruje ponowne podłączanie urządzeń zewnętrznych, jeżeli mają one tę samą literę dysku w systemie operacyjnym. Aby można było podłączyć urządzenie, musi ono mieć inną literę dysku.

Monitorowanie integralności systemu monitoruje podłączanie następujących typów urządzeń zewnętrznych:

- Dysk wymienny (w tym dyski flash USB)
- Dysk twardy
- Zewnętrzna karta sieciowa

- Napęd CD/DVD/Blu-ray
- Skaner / kamery

Monitorowanie integralności systemu w czasie rzeczywistym

Monitorowanie integralności systemu umożliwia śledzenie zmian w systemie operacyjnym w czasie rzeczywistym. Możesz śledzić zmiany, które mogą wskazywać na naruszenia bezpieczeństwa w komputerze. Komponent umożliwia blokowanie tych zmian lub jedynie rejestrowanie zdarzeń zmian.

Aby Monitorowanie integralności systemu działało, musisz dodać co najmniej jedną regułę. *Reguła Monitorowania integralności systemu* to zbiór kryteriów definiujących dostęp użytkowników do plików i rejestru. Monitorowanie integralności systemu wykrywa zmiany w plikach i rejestrze w określonym *zakresie monitorowania*. Zakres monitorowania jest jednym z kryteriów reguły Monitorowania integralności systemu.

Tryby Monitorowania integralności systemu w czasie rzeczywistym

Aby mieć pewność, że reguły Monitorowania integralności systemu nie blokują żadnych działań z zasobami o znaczeniu krytycznym dla funkcjonowania systemu operacyjnego lub innych usług, zalecamy włączenie trybu testowego i przeanalizowanie wpływu komponentu na system. Gdy tryb testowy jest włączony, Kaspersky Endpoint Security nie blokuje aktywności użytkownika zabronionej przez reguły, zamiast tego generując zdarzenia *Ostrzeżenie* ⚠.

Komponent Monitorowania integralności systemu w czasie rzeczywistym ma dwa tryby:

- Zablokuj

  W tym trybie Monitorowanie integralności systemu śledzi zmiany w systemie i wykonuje działanie zgodnie z regułami: **Zezwól** lub **Zablokuj**. Monitorowanie integralności systemu generuje również odpowiadające temu zdarzenie i zmienia status urządzenia w konsoli Kaspersky Security Center.

- Poinformuj

  W tym trybie Monitorowanie integralności systemu umożliwia działania na plikach i kluczach rejestru z zakresu monitorowania. Jeżeli akcja na plikach lub rejestrze jest zabroniona, aplikacja generuje zdarzenie: *Niedozwolona operacja była dozwolona w trybie testowym*. Aby przeanalizować, jak reguły wpływają na system, możesz spojrzeć na raporty.

Włączanie Monitorowania integralności systemu w czasie rzeczywistym

Jak włączyć Monitorowanie integralności systemu w czasie rzeczywistym w Konsoli Administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Monitor integralności systemu**.
4. Zaznacz pole **Monitor integralności systemu**.

5. W funkcji **Tryb działania reguł blokowania**, wybierz tryb Monitorowania integralności systemu w czasie rzeczywistym:

   - **Zablokuj**. W tym trybie Monitorowanie integralności systemu blokuje działania na plikach i kluczach rejestru z zakresu monitorowania oraz generuje odpowiadające temu zdarzenie.

   - **Poinformuj**. W tym trybie Monitorowanie integralności systemu zezwala na działania na plikach i kluczach rejestru z zakresu monitorowania oraz generuje odpowiadające temu zdarzenie.

6. W sekcji **Monitorowanie integralności systemu w czasie rzeczywistym** zaznacz pole **Monitorowanie integralności systemu w czasie rzeczywistym**.

7. Skonfiguruj monitorowanie urządzeń zewnętrznych:

   a. Zaznacz pole **Monitoruj urządzenia**.

   b. Z listy rozwijanej **Poziom wagi zdarzenia**, wybierz poziom ważności zdarzeń monitorowania urządzeń zewnętrznych: *Informacyjny*, *Ostrzeżenie*, *Krytyczny*.

   Monitorowanie integralności systemu rejestruje bieżące podłączenie urządzeń zewnętrznych. Aplikacja zaczyna monitorować podłączenie i rozłączenie urządzeń zewnętrznych po włączeniu komponentu w ustawieniach aplikacji. Następnie, po podłączeniu lub odłączeniu urządzenia zewnętrznego, aplikacja generuje odpowiadające temu zdarzenie.

8. Skonfiguruj monitorowanie plików i rejestru:

   a. Zaznacz pole **Monitoruj pliki i rejestr**.

   b. Kliknij **Ustawienia**.

   Spowoduje to otwarcie listy reguł Monitorowania integralności systemu.

   c. Kliknij **Dodaj**.

   Możesz również zaimportować reguły z innego źródła.

   d. Skonfiguruj regułę Monitorowania integralności systemu (patrz: tabela poniżej).

9. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć Monitorowanie integralności systemu w czasie rzeczywistym w konsoli Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Kontrola zabezpieczeń** → **Monitor integralności systemu**.

5. Włącz przełącznik **Monitorowanie integralności systemu WŁĄCZONE**.

6. Wybierz zakładkę **Windows**.

7. W funkcji **Monitorowanie integralności systemu w czasie rzeczywistym**, wybierz tryb Monitorowania integralności systemu w czasie rzeczywistym:

   - **Zastosuj reguły**. W tym trybie Monitorowanie integralności systemu blokuje działania na plikach i kluczach rejestru z zakresu monitorowania oraz generuje odpowiadające temu zdarzenie.
   - **Reguły testowania (do wiadomości)**. W tym trybie Monitorowanie integralności systemu zezwala na działania na plikach i kluczach rejestru z zakresu monitorowania oraz generuje odpowiadające temu zdarzenie.

8. Skonfiguruj monitorowanie plików i rejestru:

   a. Zaznacz pole **Monitoruj pliki i rejestr**.

   b. Kliknij **Reguły**.

   Spowoduje to otwarcie listy reguł Monitorowania integralności systemu.

   c. Kliknij **Dodaj**.

   Możesz również zaimportować reguły z innego źródła.

   d. Skonfiguruj regułę Monitorowania integralności systemu (patrz: tabela poniżej).

9. Skonfiguruj monitorowanie urządzeń zewnętrznych:

   a. Zaznacz pole **Monitoruj urządzenia**.

   b. Z listy rozwijanej **Poziom ważności zdarzenia**, wybierz poziom ważności zdarzeń monitorowania urządzeń zewnętrznych: *Informacyjny*, *Ostrzegawczy*, *Krytyczny*.

   Monitorowanie integralności systemu rejestruje bieżące podłączenie urządzeń zewnętrznych. Aplikacja zaczyna monitorować podłączenie i rozłączenie urządzeń zewnętrznych po włączeniu komponentu w ustawieniach aplikacji. Następnie, po podłączeniu lub odłączeniu urządzenia zewnętrznego, aplikacja generuje odpowiadające temu zdarzenie.

10. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć Monitorowanie integralności systemu w czasie rzeczywistym w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń → Monitor integralności systemu**.
3. Włącz przełącznik **Monitor integralności systemu**.
4. W funkcji **Tryb działania reguł blokowania**, wybierz tryb Monitorowania integralności systemu w czasie rzeczywistym:

   - **Zablokuj**. W tym trybie Monitorowanie integralności systemu blokuje działania na plikach i kluczach rejestru z zakresu monitorowania oraz generuje odpowiadające temu zdarzenie.
   - **Poinformuj**. W tym trybie Monitorowanie integralności systemu zezwala na działania na plikach i kluczach rejestru z zakresu monitorowania oraz generuje odpowiadające temu zdarzenie.

5. W sekcji **Monitorowanie integralności systemu w czasie rzeczywistym** zaznacz pole **Monitorowanie integralności systemu w czasie rzeczywistym**.

6. Skonfiguruj monitorowanie urządzeń zewnętrznych:

   a. Zaznacz pole **Monitoruj urządzenia**.

   b. Z listy rozwijanej **Poziom wagi zdarzenia**, wybierz poziom ważności zdarzeń monitorowania urządzeń zewnętrznych: *Informacyjny*, *Ostrzeżenie*, *Krytyczny*.

   Monitorowanie integralności systemu rejestruje bieżące podłączenie urządzeń zewnętrznych. Aplikacja zaczyna monitorować podłączenie i rozłączenie urządzeń zewnętrznych po włączeniu komponentu w ustawieniach aplikacji. Następnie, po podłączeniu lub odłączeniu urządzenia zewnętrznego, aplikacja generuje odpowiadające temu zdarzenie.

7. Skonfiguruj monitorowanie plików i rejestru:

   a. Zaznacz pole **Monitoruj pliki i rejestr**.

   b. Kliknij **Skonfiguruj**.

   Spowoduje to otwarcie listy reguł Monitorowania integralności systemu.

   c. Kliknij **Dodaj**.

   Możesz również zaimportować reguły z innego źródła.

8. Skonfiguruj regułę Monitorowania integralności systemu (patrz: tabela poniżej).

9. Zapisz swoje zmiany.

Ustawienia reguły Monitorowania integralności systemu w czasie rzeczywistym

Parametr	Opis
Nazwa reguły	Nazwa reguły Monitorowania integralności systemu w czasie rzeczywistym
Operacje na plikach i rejestrze	• **Zezwól**. Monitorowanie integralności systemu zezwala na działania na plikach i kluczach rejestru z zakresu monitorowania. • **Zablokuj**. Zachowanie Monitorowania integralności systemu zależy od wybranego trybu. Jeżeli wybrałeś(aś) *tryb ochrony Systemu*, Monitorowanie integralności systemu blokuje działania na plikach i kluczach rejestru z zakresu monitorowania, generuje odpowiadające temu zdarzenie i zmienia status urządzenia w konsoli Kaspersky Security Center. Jeżeli wybrałeś(aś) *tryb testowy*, Monitorowanie integralności systemu zezwala na działania na plikach i kluczach rejestru z zakresu monitorowania.

Parametr	Opis
Poziom wagi zdarzenia	Kaspersky Endpoint Security rejestruje zdarzenia modyfikacji plików za każdym razem, gdy plik lub klucz rejestru w zakresie monitorowania zostanie zmodyfikowany. Dostępne są poniższe poziomy wagi zdarzenia: *Informacyjny*, *Ostrzeżenie*, *Krytyczny*.
Zakres monitorowania	• **Plik**. Lista plików i folderów monitorowanych przez komponent. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. Użyj masek: • Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach. • Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską. • Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków. • **Rejestr**. Lista kluczy rejestru i wartości monitorowanych przez komponent. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski.
Wykluczenia	• **Plik**. Lista wykluczeń z zakresu monitorowania. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. Na przykład, `C:\Folder\Application\*.log`. Wpisy wykluczające mają wyższy priorytet niż wpisy zakresu monitorowania. Użyj masek: • Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach. • Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską. • Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków. • **Rejestr**. Lista wykluczeń z zakresu monitorowania. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski. Wpisy wykluczające mają wyższy priorytet niż wpisy zakresu monitorowania.
Zaufani użytkownicy i/lub grupy użytkowników	*Zaufany użytkownik* to użytkownik, który może wykonywać działania na plikach i kluczach rejestru w zakresie monitorowania. Jeśli Kaspersky Endpoint Security wykryje działanie wykonane przez zaufanego użytkownika, Monitorowanie integralności systemu wygeneruje zdarzenie *Informacyjny*. Możesz wybrać użytkowników w Active Directory, na liście kont w Kaspersky Security Center lub ręcznie wprowadzając lokalną nazwę użytkownika. Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny.
Markery operacji plikowej / Monitorowane operacje	Znaczniki charakteryzujące działanie z plikami lub kluczami rejestru, które aplikacja będzie monitorować.
Haszowanie	Obliczanie sumy kontrolnej pliku po modyfikacji. Kaspersky Endpoint Security dodaje informacje o sumie kontrolnej pliku po wygenerowaniu zdarzenia.

Sprawdzanie integralności systemu na żądanie

Sprawdzanie integralności systemu na żądanie to zadanie, które możesz uruchomić ręcznie lub zgodnie z harmonogramem. Podczas uruchamiania zadania *Sprawdzanie integralności systemu*, aplikacja porównuje aktualny stan obiektów objętych zakresem monitorowania z ich stanem *punktu odniesienia*. W przeciwieństwie do Monitorowania integralności systemu w czasie rzeczywistym, zadanie *Sprawdzanie integralności systemu* pomaga ograniczyć liczbę zdarzeń i pozwala wygenerować ogólny raport zmian w systemie operacyjnym.

Aby Monitorowanie integralności systemu działało, musisz dodać co najmniej jedną regułę. *Reguła Monitorowania integralności systemu* to zbiór kryteriów definiujących dostęp użytkowników do plików i rejestru. Monitorowanie integralności systemu wykrywa zmiany w plikach i rejestrze w określonym *zakresie monitorowania*. Zakres monitorowania jest jednym z kryteriów reguły Monitorowania integralności systemu. Możesz skonfigurować reguły udostępniane przez Monitorowanie integralności systemu w czasie rzeczywistym i zadanie *Sprawdzanie integralności systemu* lub utworzyć osobne reguły dla zadania. Aby utworzyć punkt odniesienia, Kaspersky Endpoint Security stosuje zakres monitorowania z zadania *Sprawdzanie integralności systemu* do zadania *Aktualizacja stanu wyjściowego*.

Tworzenie i aktualizacja punktu odniesienia

Zadanie *Sprawdzanie integralności systemu* wymaga punktu odniesienia, aby działać. *Punkt odniesienia* to zarejestrowany status obiektów w systemie, który aplikacja wykorzystuje jako odniesienie przy porównywaniu ze stanem bieżącym. Jeśli bieżący stan systemu różni się od stanu systemu zarejestrowanego w punkcie odniesienia, Kaspersky Endpoint Security wygeneruje odpowiadające temu zdarzenie. Możesz utworzyć lub zaktualizować punkt odniesienia za pomocą zadania *Aktualizacja stanu wyjściowego*.

Możesz aktualizować punkt odniesienia w następujących trybach:

- Pełna aktualizacja.

  Aplikacja aktualizuje wszystkie obiekty w zakresie monitorowania.

- Aktualizacja przyrostowa.

  Aplikacja wykrywa i aktualizuje tylko zmodyfikowane lub nowe obiekty.

Jak utworzyć lub zaktualizować punkt odniesienia w Konsoli Administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Aktualizacja stanu wyjściowego**.

Krok 2. Wybór trybu aktualizacji punktu odniesienia

Wybierz tryb aktualizacji punktu odniesienia:

- **Pełna aktualizacja**. Aplikacja aktualizuje wszystkie obiekty w zakresie monitorowania.
- **Aktualizacja przyrostowa**. Aplikacja wykrywa i aktualizuje tylko zmodyfikowane lub nowe obiekty.

Krok 3. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 4. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład, *Punkt Odniesienia 2024*.

Krok 5. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Jak utworzyć lub zaktualizować punkt odniesienia w Web Console

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Aktualizacja stanu wyjściowego**.

   c. W polu **Nazwa zadania** wprowadź krótki opis, na przykład, *Punkt Odniesienia 2024*.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.

5. Wybierz konto do uruchomienia zadania. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika.

6. Zakończ działanie Kreatora.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij nowe zadanie.

   Zostanie otwarte okno właściwości zadania.

8. Wybierz zakładkę **Ustawienia aplikacji**.

9. Wybierz tryb aktualizacji punktu odniesienia:

   - **Pełna aktualizacja**. Aplikacja aktualizuje wszystkie obiekty w zakresie monitorowania.
   - **Aktualizacja przyrostowa**. Aplikacja wykrywa i aktualizuje tylko zmodyfikowane lub nowe obiekty.

10. Zapisz swoje zmiany.

11. Zaznacz pole obok zadania.

12. Kliknij **Uruchom**.

Konfigurowanie zakresu monitorowania dla zadania Sprawdzanie integralności systemu

Domyślnie zakres monitorowania zadania *Sprawdzanie integralności systemu* jest taki sam, jak zakres Monitorowania integralności systemu w czasie rzeczywistym. Możesz skonfigurować inny zakres monitorowania dla zadania.

> Monitor integralności systemu nie obsługuje importowania kluczy `HKEY_CURRENT_USER` i `HKEY_CURRENT_CONFIG` dla zadania *Sprawdzanie integralności systemu*. Jeżeli zakres monitorowania zadania zawiera te klucze, aplikacja generuje zdarzenie *Zakres monitorowania obejmuje nieprawidłowe obiekty*.

Jak skonfigurować inny zakres monitorowania dla zadania Sprawdzanie integralności systemu w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Monitor integralności systemu**.

4. Zaznacz pole **Monitor integralności systemu**.

5. W funkcji **Sprawdzanie integralności systemu**, wybierz tryb konfiguracji zadania: **Ustawienia niestandardowe**.

6. Skonfiguruj monitorowanie urządzeń zewnętrznych:

   a. Zaznacz pole **Monitoruj urządzenia**.

   b. Z listy rozwijanej **Poziom wagi zdarzenia**, wybierz poziom ważności zdarzeń monitorowania urządzeń zewnętrznych: *Informacyjny* ⓘ, *Ostrzeżenie* ⚠, *Krytyczny* ⓘ.

   Monitorowanie integralności systemu rejestruje informacje o podłączonych urządzeniach zewnętrznych w momencie tworzenia punktu odniesienia. Następnie, po podłączeniu urządzenia zewnętrznego, aplikacja generuje odpowiadające temu zdarzenie. Podczas uruchamiania zadania *Sprawdzanie integralności systemu*, aplikacja nie monitoruje odłączenia urządzeń zewnętrznych.

7. Skonfiguruj monitorowanie plików i rejestru:

   a. Zaznacz pole **Monitoruj pliki i rejestr**.

   b. Kliknij **Ustawienia**.

      Spowoduje to otwarcie listy reguł Monitorowania integralności systemu.

   c. Kliknij **Dodaj**.

      Możesz również zaimportować reguły z innego źródła.

   d. Skonfiguruj regułę Monitorowania integralności systemu (patrz: tabela poniżej).

8. Zapisz swoje zmiany.

Jak skonfigurować inny zakres monitorowania dla zadania Sprawdzanie integralności systemu w Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Kontrola zabezpieczeń** → **Monitor integralności systemu**.

5. Wybierz zakładkę **Windows**.

6. Włącz przełącznik **Monitorowanie integralności systemu WŁĄCZONE**.

7. W funkcji **Sprawdzanie integralności systemu**, wybierz tryb konfiguracji zadania: **Ustawienia niestandardowe**.

8. Skonfiguruj monitorowanie urządzeń zewnętrznych:

   a. Zaznacz pole **Monitoruj urządzenia**.

   b. Z listy rozwijanej **Poziom ważności zdarzenia**, wybierz poziom ważności zdarzeń monitorowania urządzeń zewnętrznych: *Informacyjny*, *Ostrzegawczy*, *Krytyczny*.

   Monitorowanie integralności systemu rejestruje informacje o podłączonych urządzeniach zewnętrznych w momencie tworzenia punktu odniesienia. Następnie, po podłączeniu urządzenia zewnętrznego, aplikacja generuje odpowiadające temu zdarzenie. Podczas uruchamiania zadania *Sprawdzanie integralności systemu*, aplikacja nie monitoruje odłączenia urządzeń zewnętrznych.

9. Skonfiguruj monitorowanie plików i rejestru:

   a. Zaznacz pole **Monitoruj pliki i rejestr**.

   b. Kliknij **Reguły**.

      Spowoduje to otwarcie listy reguł Monitorowania integralności systemu.

c. Kliknij **Dodaj**.

Możesz również zaimportować reguły z innego źródła.

d. Skonfiguruj regułę Monitorowania integralności systemu (patrz: tabela poniżej).

10. Zapisz swoje zmiany.

Jak skonfigurować inny zakres monitorowania dla zadania Sprawdzanie integralności systemu w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Monitor integralności systemu**.
3. Włącz przełącznik **Monitor integralności systemu**.
4. W funkcji **Sprawdzanie integralności systemu**, wybierz tryb konfiguracji zadania: **Ustawienia niestandardowe**.
5. Skonfiguruj monitorowanie urządzeń zewnętrznych:

   a. Zaznacz pole **Monitoruj urządzenia**.

   b. Z listy rozwijanej **Poziom wagi zdarzenia**, wybierz poziom ważności zdarzeń monitorowania urządzeń zewnętrznych: *Informacyjny* ⓘ, *Ostrzeżenie* ⚠, *Krytyczny* ⓘ.

   Monitorowanie integralności systemu rejestruje informacje o podłączonych urządzeniach zewnętrznych w momencie tworzenia punktu odniesienia. Następnie, po podłączeniu urządzenia zewnętrznego, aplikacja generuje odpowiadające temu zdarzenie. Podczas uruchamiania zadania *Sprawdzanie integralności systemu*, aplikacja nie monitoruje odłączenia urządzeń zewnętrznych.

6. Skonfiguruj monitorowanie plików i rejestru:

   a. Zaznacz pole **Monitoruj pliki i rejestr**.

   b. Kliknij **Skonfiguruj**.

   Spowoduje to otwarcie listy reguł Monitorowania integralności systemu.

   c. Kliknij **Dodaj**.

   Możesz również zaimportować reguły z innego źródła.

   d. Skonfiguruj regułę Monitorowania integralności systemu (patrz: tabela poniżej).

7. Zapisz swoje zmiany.

Ustawienia reguły zadania Sprawdzanie integralności systemu

Parametr	Opis
Nazwa reguły	Nazwa reguły zadania *Sprawdzanie integralności systemu*.
Poziom wagi zdarzenia	Kaspersky Endpoint Security rejestruje zdarzenia modyfikacji plików za każdym razem, gdy plik lub klucz rejestru w zakresie monitorowania zostanie zmodyfikowany. Dostępne są poniższe poziomy wagi zdarzenia: *Informacyjny*, *Ostrzeżenie*, *Krytyczny*.
Zakres monitorowania	• **Plik**. Lista plików i folderów monitorowanych przez komponent. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. Użyj masek: • Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach. • Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską. • Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków. • **Rejestr**. Lista kluczy rejestru i wartości monitorowanych przez komponent. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski.
Wykluczenia	• **Plik**. Lista wykluczeń z zakresu monitorowania. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. Na przykład, `C:\Folder\Application\*.log`. Wpisy wykluczające mają wyższy priorytet niż wpisy zakresu monitorowania. Użyj masek: • Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach. • Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską. • Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków. • **Rejestr**. Lista wykluczeń z zakresu monitorowania. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski. Wpisy wykluczające mają wyższy priorytet niż wpisy zakresu monitorowania.

Uruchamianie zadania Sprawdzanie integralności systemu

Zadanie *Sprawdzanie integralności systemu* umożliwia sprawdzenie plików lub kluczy rejestru pod kątem zmian, a także sprawdzenie podłączenia urządzeń zewnętrznych. Aby sprawdzić pliki pod kątem zmian, możesz uruchomić zadanie *Sprawdzanie integralności systemu* w następujących trybach:

- Szybki Skan.

  Podczas sprawdzania plików pod kątem zmian, aplikacja sprawdza tylko atrybuty plików. Aplikacja nie sprawdza zawartości plików.

- Pełne skanowanie.

  Podczas sprawdzania plików pod kątem zmian, aplikacja sprawdza wszystkie atrybuty plików i zawartość plików.

Tryb, w którym uruchamiane jest zadanie, nie ma wpływu na sprawdzanie rejestru ani urządzeń zewnętrznych.

Jak uruchomić zadanie Sprawdzanie integralności systemu w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zadania**.

   Zostanie otwarta lista zadań.
3. Kliknij **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.
4. Wybierz **Kaspersky Endpoint Security → Podstawowe monitorowanie integralności systemu**. Wybierz tryb Sprawdzenia integralności systemu:

   - **Pełne skanowanie**. W tym trybie aplikacja sprawdza wszystkie atrybuty i skróty plików.
   - **Szybkie skanowanie**. W tym trybie aplikacja sprawdza tylko atrybuty plików.
5. Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

   - Wybierz komputery wykryte w sieci przez Serwer administracyjny: urządzenia nieprzypisane. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
   - Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.
   - Określ wybór urządzeń, dla których chcesz uruchomić zadanie.
   - Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
6. Wybierz konto do uruchomienia zadania. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika.
7. Skonfiguruj terminarz uruchamiania zadania, na przykład ręcznie lub w określonym dniu tygodnia.
8. Wprowadź nazwę zadania.
9. Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Jak uruchomić zadanie Sprawdzanie integralności systemu w Web Console

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.
3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Sprawdzanie integralności systemu**.

c. W polu **Nazwa zadania** wprowadź krótki opis, na przykład *Cotygodniowa Kontrola Integralności Systemu*.

d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.
5. Wybierz konto do uruchomienia zadania. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika.
6. Zakończ działanie Kreatora.

   Nowe zadanie zostanie wyświetlone na liście zadań.
7. Kliknij nowe zadanie.

   Zostanie otwarte okno właściwości zadania.
8. Wybierz zakładkę **Ustawienia aplikacji**.
9. Wybierz tryb Sprawdzenia integralności systemu:

   - **Szybkie skanowanie**. Aplikacja sprawdza tylko atrybuty plików. Aplikacja nie sprawdza zawartości plików.
   - **Pełne skanowanie**. Aplikacja sprawdza wszystkie atrybuty plików, jak również ich zawartość.
10. Zapisz swoje zmiany.
11. Zaznacz pole obok zadania.
12. Kliknij **Uruchom**.

Aby umożliwić pomyślne zakończenie zadania *Sprawdzanie integralności systemu*, zakres monitorowania zadania *Sprawdzanie integralności systemu* musi całkowicie odpowiadać punktowi odniesienia. Jeżeli zakres monitorowania jest inny, zadanie kończy się błędem. Aby zsynchronizować zakresy monitorowania, uruchom zadanie *Aktualizacja stanu wyjściowego* z nowym zakresem monitoringu.

Eksportowanie i importowanie reguł Monitorowania integralności systemu

Możesz wyeksportować listę reguł Monitorowania integralności systemu do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby dodać dużą liczbę rekordów tego samego typu. Możesz użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy reguł Monitorowania integralności systemu lub przeniesienia listy na inny serwer.

Monitor integralności systemu nie obsługuje importowania kluczy `HKEY_CURRENT_USER` i `HKEY_CURRENT_CONFIG` dla zadania *Sprawdzanie integralności systemu*. Jeżeli zakres monitorowania zadania zawiera te klucze, aplikacja generuje zdarzenie *Zakres monitorowania obejmuje nieprawidłowe obiekty*.

Jak wyeksportować i zaimportować listę reguł Monitorowania integralności systemu w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Kontrola zabezpieczeń → Monitor integralności systemu**.
4. Aby wyeksportować lub zaimportować reguły *Monitorowania integralności systemu w czasie rzeczywistym*:
   a. W sekcji **Monitorowanie integralności systemu w czasie rzeczywistym** kliknij przycisk **Ustawienia**.
   b. Aby wyeksportować listę reguł Monitorowania integralności systemu w czasie rzeczywistym:
      1. Wybierz reguły, które chcesz zmienić. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
         Jeśli nie wybrałeś żadnej reguły, Kaspersky Endpoint Security wyeksportuje wszystkie reguły.
      2. Kliknij odnośnik **Eksportuj**.
      3. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę reguł, i wybierz folder, w którym chcesz zapisać ten plik.
      4. Zapisz plik.
         Kaspersky Endpoint Security eksportuje listę reguł do pliku XML.
   c. Aby zaimportować listę reguł Monitorowania integralności systemu w czasie rzeczywistym:
      1. Kliknij odnośnik **Importuj**.
         W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.
      2. Otwórz plik.
         Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
5. Aby wyeksportować lub zaimportować reguły *Sprawdzenia integralności systemu*:
   a. W bloku **Sprawdzanie integralności systemu** wybierz **Ustawienia niestandardowe**.
   b. Kliknij **Ustawienia**.
   c. Aby wyeksportować listę reguł Sprawdzenia integralności systemu:
      1. Wybierz reguły, które chcesz zmienić. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
         Jeśli nie wybrałeś żadnej reguły, Kaspersky Endpoint Security wyeksportuje wszystkie reguły.
      2. Kliknij odnośnik **Eksportuj**.
      3. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę reguł, i wybierz folder, w którym chcesz zapisać ten plik.
      4. Zapisz plik.

   Kaspersky Endpoint Security eksportuje listę reguł do pliku XML.

d. Aby zaimportować listę reguł Sprawdzenia integralności systemu:

1. Kliknij odnośnik **Importuj**.

   W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.

2. Otwórz plik.

Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

6. Zapisz swoje zmiany.

Jak wyeksportować i zaimportować listę reguł Monitora integralności systemu w konsoli Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń** → **Monitor integralności systemu**.
5. Wybierz zakładkę **Windows**.
6. Aby wyeksportować lub zaimportować reguły *Monitorowania integralności systemu w czasie rzeczywistym*:

   a. W sekcji **Monitorowanie integralności systemu w czasie rzeczywistym** kliknij odnośnik **Reguły**.

   b. Aby wyeksportować listę reguł Monitorowania integralności systemu w czasie rzeczywistym:

      1. Wybierz reguły, które chcesz zmienić.
      2. Kliknij przycisk → **Eksportuj**.

         Kaspersky Endpoint Security eksportuje listę reguł do pliku JSON w domyślnym folderze do pobrania.

   c. Aby zaimportować listę reguł Monitorowania integralności systemu w czasie rzeczywistym:

      1. Kliknij przycisk → **Importuj**.

         W oknie, które zostanie otwarte, wybierz plik JSON, z którego chcesz zaimportować listę zaufanych adresów.

      2. Otwórz plik.

         Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku JSON.

7. Aby wyeksportować lub zaimportować reguły *Sprawdzenia integralności systemu*:

   a. W bloku **Sprawdzanie integralności systemu na żądanie** wybierz **Ustawienia niestandardowe**.

   b. Kliknij odnośnik **Reguły**.

c. Aby wyeksportować listę reguł Sprawdzenia integralności systemu:

1. Wybierz reguły, które chcesz zmienić.
2. Kliknij przycisk → **Eksportuj**.

   Kaspersky Endpoint Security eksportuje listę reguł do pliku JSON w domyślnym folderze do pobrania.

d. Aby zaimportować listę reguł Sprawdzenia integralności systemu:

1. Kliknij przycisk → **Importuj**.

   W oknie, które zostanie otwarte, wybierz plik JSON, z którego chcesz zaimportować listę zaufanych adresów.
2. Otwórz plik.

   Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku JSON.

8. Zapisz swoje zmiany.

Podgląd raportów Monitorowania integralności systemu

Aby przeanalizować działanie reguł Monitorowania integralności systemu, możesz przeglądać raporty i zdarzenia generowane przez aplikację. Kaspersky Endpoint Security generuje następujące raporty dotyczące komponentu:

- W interfejsie aplikacji:
  - Raport Monitorowania integralności systemu
  - Raport sprawdzania integralności systemu
  - Raport aktualizacji punktu odniesienia

  Raporty zawierają zdarzenia Monitora integralności systemu.
- w konsoli Kaspersky Security Center Console:
  - Raport dotyczący komputerów, na których reguły monitorowania zostały uruchomione najwięcej razy
  - Raport dotyczący najczęściej uruchamianych reguł monitorowania

  Domyślnie tworzony jest raport za poprzednie 30 dni, włącznie z datą utworzenia raportu.

  Jak przeglądać raporty Monitorowania integralności systemu w Konsoli administracyjnej (MMC)

  1. Otwórz Konsolę administracyjną Kaspersky Security Center.
  2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Raporty**.
  3. Kliknij **Nowy szablon raportu**.

     Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu.

4. Postępuj zgodnie z instrukcjami Kreatora szablonu raportu. W kroku **Wybieranie typu szablonu raportu** wybierz raport Monitorowania integralności systemu (sekcja **Inne**):

   - **10 urządzeń z najczęściej wywołanymi regułami Monitora integralności plików / Monitora integralności systemu**.
   - **10 najważniejszych reguł Monitora integralności plików / Monitora integralności systemu, które były najczęściej wywoływane na urządzeniach**.

   Po zakończeniu pracy Kreatora tworzenia nowego szablonu raportu, nowy szablon raportu pojawi się w tabeli, na zakładce **Raporty**.

5. Otwórz raport, klikając go dwukrotnie.

Zostanie rozpoczęty proces tworzenia raportu. Raport zostanie wyświetlony w nowym oknie.

Jak przeglądać raporty Monitorowania integralności systemu w Web Console

1. W oknie głównym Web Console wybierz **Monitorowanie** → **Raporty**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu.

3. Pod opcją **Typ szablonu**, w sekcji **Inny**, wybierz raport Monitorowania integralności systemu:

   - **10 urządzeń z najczęściej wywołanymi regułami Monitora integralności plików / Monitora integralności systemu**.
   - **10 najważniejszych reguł Monitora integralności plików / Monitora integralności systemu, które były najczęściej wywoływane na urządzeniach**.

   Po zakończeniu pracy z Kreatorem tworzenia nowego szablonu raportu, nowy szablon raportu pojawi się w tabeli.

4. Wybierz i uruchom raport.

Zostanie rozpoczęty proces tworzenia raportu. Raport zostanie wyświetlony w nowym oknie.

Aby przeglądać zdarzenia generowane przez aplikację, możesz także skorzystać z opcji wyboru zdarzeń w konsoli Kaspersky Security Center.

Reset statusu integralności systemu

Komputery w konsoli Kaspersky Security Center mają jeden z następujących statusów: *OK*, *Ostrzeżenie* lub *Krytyczny*. Jeśli Monitorowanie integralności systemu wykryje modyfikację plików lub kluczy rejestru w zakresie monitorowania, status komputera zmieni się na *Ostrzeżenie* lub *Krytyczny*. Status przypisany przez Monitorowanie integralności systemu nazywany jest *statusem integralności systemu*. Możesz zresetować stan integralności systemu, na przykład, jeśli analiza przekonała cię, że wykryta modyfikacja obiektów nie ma negatywnego wpływu na bezpieczeństwo komputera.

Jak zresetować status integralności systemu w Konsoli Administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Reset stanu integralności systemu**.

Krok 2. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 3. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz zadania, na przykład ręcznie.

Krok 4. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład. *Resetowanie statusu po modyfikacji zakresu monitorowania*.

Krok 5. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Jak zresetować status integralności systemu w Web Console

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Reset stanu integralności systemu**.

   c. W polu **Nazwa zadania**, wprowadź krótki opis, na przykład, *Resetowanie statusu po modyfikacji zakresu monitorowania*.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.

5. Wybierz konto do uruchomienia zadania. Domyślnie Kaspersky Endpoint Security uruchamia zadanie z uprawnieniami lokalnego konta użytkownika.

6. Zakończ działanie Kreatora.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Zaznacz pole obok zadania.

8. Kliknij **Uruchom**.

W rezultacie, jeśli status komputera został zmieniony na *Ostrzeżenie* lub *Krytyczny* z powodu zdarzeń Monitorowania integralności systemu, status komputera jest resetowany do *OK*. Jeżeli status komputera został zmieniony także z powodu innych zdarzeń, status komputera pozostaje niezmieniony.

Cloud Discovery

Cloud Discovery umożliwia zarządzanie dostępem użytkowników do usług w chmurze. Usługami w chmurze są przykładowo aplikacje Microsoft Teams, Salesforce i Microsoft Office 365. Usługi w chmurze można podzielić na kategorie, takie jak *Udostępnianie plików*, *Komunikatory*, *Poczta elektroniczna*. Eksperci z Kaspersky regularnie aktualizują kategorie przechowywane w Cloud Discovery i listę usług w chmurze zaliczanych do poszczególnych kategorii. Kaspersky Endpoint Security aktualizuje zestaw kategorii i usług w chmurze wraz z bazami danych aplikacji. Oznacza to, że składnik Cloud Discovery nie wykorzystuje rozwiązania Kaspersky Security Network do podziału usług w chmurze na kategorie.

Cloud Discovery zapewnia następujące funkcjonalności:

- Monitorowanie użycia usług w chmurze
- Blokowanie dostępu użytkowników do usług w chmurze

Wymagania systemowe

Składnika Cloud Discovery można używać, gdy spełnione są następujące warunki:

- Aplikacja jest zainstalowana na komputerze z systemem Windows dla stacji roboczych.

  Składnika nie można używać na serwerach.

- Kaspersky Security Center w wersji 15.1 lub nowszej.

  Komponent nie jest dostępny w Konsoli administracyjnej (MMC). Możesz skonfigurować Cloud Discovery w Kaspersky Security Center Web Console i Kaspersky Security Center Cloud Console.

- Licencja Kaspersky Next.

Włącz funkcje aplikacji wymagane przez komponent Cloud Discovery:

1. **Skanuj połączenia szyfrowane**. Jest to konieczne do monitorowania ruchu sieciowego HTTPS. Tą funkcją można zarządzać w sekcji **Ustawienia sieciowe**.

2. **Wstrzykuj skrypt do ruchu sieciowego w celu interakcji ze stronami internetowymi**. Skrypt włącza rejestrację zdarzeń Cloud Discovery. Skrypt zapewnia również w pełni funkcjonalne blokowanie dostępu do usług w chmurze. Bez tego skryptu aplikacja blokuje dostęp tylko dla domen usług w chmurze. Tą funkcją można zarządzać w sekcji **Ustawienia sieciowe**.

Możesz również włączyć funkcję **Zapisuj informacje o otwarciu dozwolonych stron**. Funkcja ta obejmuje grupowanie zdarzeń, gdy użytkownik odwiedza strony internetowe należące do tej samej domeny. W ten sposób, gdy użytkownik korzysta z usługi w chmurze, Cloud Discovery rejestruje tylko jedno zdarzenie zamiast wielu zdarzeń dla każdej strony internetowej. Tą funkcją można zarządzać w sekcji **Kontrola sieci**.

Monitorowanie usług w chmurze

Kiedy użytkownik rozpocznie korzystanie z usługi w chmurze, rozwiązanie Kaspersky Endpoint Security rejestruje to zdarzenie i tworzy wpis w raporcie. Cloud Discovery monitoruje użycie usługi w chmurze w przeglądarce, jak również w odpowiednich aplikacjach. Monitorowane jest jej wykorzystanie zarówno w protokole HTTP, jak i HTTPS.

Jak włączyć monitorowanie usługi w chmurze w Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Komunikacja i Ochrona WWW** → **Cloud Discovery**.

5. Włącz przełącznik **Cloud Discovery WŁĄCZONE**.

6. Zapisz swoje zmiany.

W rezultacie aplikacja przekazuje informacje o używanych usługach w chmurze do Kaspersky Security Center. Informacje o użyciu usług w chmurze możesz przeglądać w raportach. W razie potrzeby możesz zablokować dostęp do usług w chmurze.

Blokowanie dostępu do usług w chmurze

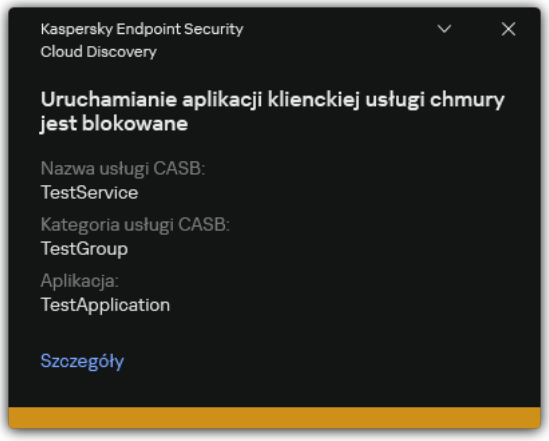
Blokowanie dostępu do usług w chmurze jest dostępne tylko dla licencji Kaspersky Next EDR Optimum i licencji XDR Expert. Ta funkcja nie jest dostępna w przypadku licencji Kaspersky Next EDR Foundations. Porównanie funkcjonalności aplikacji w zależności od typu licencji Kaspersky Next znajduje się w części Pomoc Kaspersky Next.

Administrator może ograniczyć dostęp użytkownika do kategorii Cloud Discovery lub poszczególnych usług w chmurze. Dzięki temu może zezwalać na korzystanie tylko z bezpiecznych usług w chmurze, zapobiegając wyciekom danych. W Cloud Discovery wyświetlane są *informacje o poziomie ryzyka* dla każdej usługi w chmurze. Poziom ryzyka ułatwia wykrywanie usług, które nie spełniają wymagań bezpieczeństwa organizacji.

Poziom ryzyka jest oceną szacunkową i nie stanowi oświadczenia dotyczącego jakości usługi w chmurze ani jego dostawcy. Jest to zaledwie zalecenie ekspertów z Kaspersky.

Poziomy ryzyka usług w chmurze są wyświetlane w obszarze zasad **Cloud Discovery** na liście wszystkich monitorowanych usług w chmurze.

Inne składniki Kaspersky Endpoint Security zapewniają ochronę przed zagrożeniami i umożliwiają monitorowanie podejrzanych działań użytkowników w trakcie używania usług w chmurze.



Powiadomienie Cloud Discovery

Cloud Discovery nie blokuje aplikacji w chmurze, które zostały uruchomione przed Kaspersky Endpoint Security.

Jak zablokować dostęp do usług w chmurze w Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Komunikacja i Ochrona WWW** → **Cloud Discovery**.
5. Włącz przełącznik **Cloud Discovery WŁĄCZONE**.

   Zostanie wyświetlona lista wszystkich usług w chmurze. Usługi w chmurze grupowane są w kategorie, na przykład: *Udostępnianie plików*, *Komunikatory*, *E-mail*. Eksperci z Kaspersky regularnie aktualizują kategorie przechowywane w Cloud Discovery i listę usług w chmurze zaliczanych do poszczególnych kategorii. Kaspersky Endpoint Security aktualizuje zestaw kategorii i usług w chmurze wraz z bazami danych aplikacji.
6. Użyj przełącznika w kolumnie **Dostęp**, aby skonfigurować dostęp do usług w chmurze.
7. Zapisz swoje zmiany.

W rezultacie aplikacja monitoruje użycie usługi w chmurze w przeglądarce, jak również w odpowiednich aplikacjach.

Strefa zaufana

Strefa zaufana jest utworzoną przez administratora listą obiektów i aplikacji, które nie są monitorowane przez Kaspersky Endpoint Security.

Administrator tworzy strefę zaufaną, biorąc pod uwagę cechy i funkcje używanych obiektów oraz zainstalowanych aplikacji. Umieszczenie obiektów i aplikacji w strefie zaufanej może być konieczne, gdy Kaspersky Endpoint Security blokuje dostęp do określonego obiektu lub aplikacji, które według Ciebie są nieszkodliwe. Administrator może także zezwolić użytkownikowi na utworzenie własnej lokalnej strefy zaufanej dla określonego komputera. W ten sposób użytkownicy mogą utworzyć swoje własne lokalne listy wykluczeń i zaufanych aplikacji jako dodatek do ogólnej strefy zaufanej w zasadzie.

Począwszy od Kaspersky Endpoint Security 12.5 for Windows, możesz dodać telemetrię EDR do strefy zaufanej. Umożliwia to optymalizację danych wysyłanych przez aplikację do serwera gromadzenia danych telemetrycznych dla rozwiązania Kaspersky Anti Targeted Attack Platform (EDR).

Począwszy od Kaspersky Endpoint Security 12.6 for Windows, wykluczenia skanowania I zaufane aplikacje są dodawane do strefy zaufanej. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach.

Począwszy od Kaspersky Endpoint Security 12.8 for Windows można instalować aplikację w trybie Light Agent w celu ochrony środowisk wirtualnych. Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje mogą pomóc w szybkiej konfiguracji Kaspersky Endpoint Security w środowiskach wirtualnych Citrix i VMware.

Tworzenie wykluczenia ze skanowania

Wykluczenie ze skanowania to zestaw warunków, które muszą być spełnione, aby Kaspersky Endpoint Security nie skanował określonego obiektu w poszukiwaniu wirusów i innych zagrożeń. Wykluczenia ze skanowania zapewniają możliwość bezpiecznej pracy z legalnymi aplikacjami, które mogą zostać wykorzystane przez hakerów do uszkodzenia komputera lub danych. Nie posiadają one żadnych szkodliwych funkcji, ale mogą zostać wykorzystane przez cyberprzestępców. Szczegółowe informacje na temat legalnego oprogramowania, które może zostać użyte przez cyberprzestępców do uszkodzenia komputera lub danych osobistych, znajdują się na stronie internetowej Encyklopedii IT Kaspersky.

Takie aplikacje mogą być blokowane przez program Kaspersky Endpoint Security. Aby zapobiec blokowaniu tych aplikacji, możesz skonfigurować wykluczenia ze skanowania dla używanych aplikacji. W tym celu dodaj do strefy zaufanej nazwę lub maskę nazwy zgodną z klasyfikacją Encyklopedii IT Kaspersky. Na przykład, często używasz aplikacji Radmin do zdalnego zarządzania komputerami. Kaspersky Endpoint Security wykrywa ten rodzaj aktywności aplikacji jako podejrzany i może go zablokować. Aby zapobiec blokowaniu aplikacji, utwórz wykluczenie ze skanowania z nazwą lub maską nazwy z Encyklopedii IT Kaspersky.

Jeśli na komputerze jest zainstalowana aplikacja, która gromadzi informacje i wysyła je do przetworzenia, Kaspersky Endpoint Security może zaklasyfikować tę aplikację jako szkodliwe oprogramowanie. Aby tego uniknąć, możesz wykluczyć tę aplikację ze skanowania, konfigurując Kaspersky Endpoint Security w sposób opisany w dokumencie.

Wykluczenia ze skanowania mogą być używane przez następujące komponenty i zadania aplikacji, które zostały skonfigurowane przez administratora systemu:

- Wykrywanie zachowań
- Ochrona przed exploitami
- Ochrona przed włamaniami
- Ochrona plików
- Ochrona WWW
- Ochrona poczty
- Zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*

Kaspersky Endpoint Security nie przeskanuje obiektu, jeśli dysk lub folder go zawierający znajduje się w obszarze skanowania w momencie uruchomienia jednego z zadań skanowania. Wykluczenie ze skanowania nie jest stosowane, gdy dla danego obiektu uruchomione zostało skanowanie obiektów.

Zmiana listy wykluczeń skanowania może zostać zablokowana przez właściwości zasady nadrzędnej. Aby zmienić listę, musisz zezwolić na zmianę ustawień strefy zaufanej w Web Console (kłódka musi być odblokowana).

Strefy zaufane są grupowane w różny sposób w Konsoli administracyjnej (MMC) i Web Console. Sposoby zapobiegania zmianom parametrów strefy zaufanej również mogą się różnić („kłódki" mogą być inne). Zalecamy korzystanie wyłącznie z Web Console do zarządzania aplikacją. Jeśli skonfigurujesz strefę zaufaną w różnych konsolach, wtyczka zarządzająca może przywrócić „kłódkę" do stanu domyślnego.

Jak utworzyć wykluczenie ze skanowania w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Wykluczenia i typy obiektów**.
4. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** → **Wykluczenia ze skanowania** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno zawierające listę wykluczeń.
5. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę wykluczeń dla wszystkich komputerów w firmie. Listy wykluczeń w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Wykluczenia z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie wykluczeń zasady nadrzędnej nie jest możliwe.

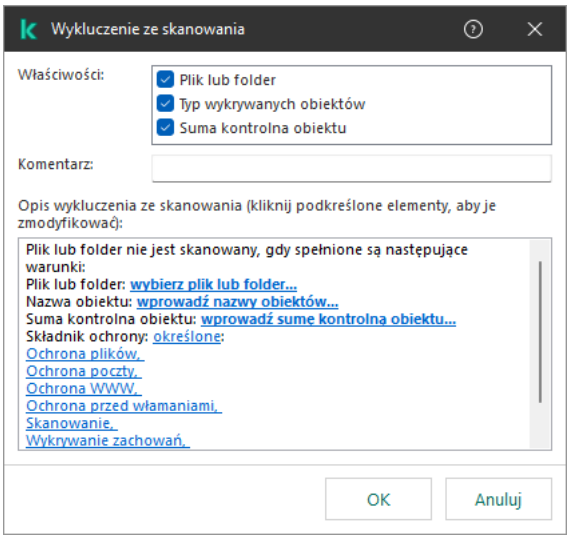
6. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy wykluczeń, zaznacz pole **Zezwól na korzystanie z lokalnych wykluczeń**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę wykluczeń jako dodatek do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

   Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Ponadto jeśli to pole wyboru jest odznaczone, Kaspersky Endpoint Security ukryje skonsolidowaną listę wykluczeń ze skanowania w interfejsie użytkownika aplikacji.

7. Kliknij **Dodaj** i wybierz działanie:

   - **Kategoria**. Możesz grupować wykluczenia ze skanowania w ramach osobnych kategorii. Aby utworzyć nową kategorię, wprowadź nazwę kategorii i dodaj do niej co najmniej jedno wykluczenie ze skanowania.
   - **Nowe wykluczenie**. Kaspersky Endpoint Security dodaje nowe wykluczenie ze skanowania do katalogu głównego listy.
   - **Wybierz wykluczenie z listy**. Aby szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w System Center Configuration Manager, aplikacja zawiera *predefiniowane wykluczenia skanowania*. Dodano także predefiniowane wykluczenia ze skanowania, aby ułatwić konfigurowanie aplikacji w środowiskach wirtualnych Citrix i Vmware. Musisz wybrać predefiniowane wykluczenia ze skanowania w zależności od przeznaczenia chronionego serwera.
   - **Nowe wykluczenie w wybranej kategorii**. Wybierz kategorię, aby dodać nowe wykluczenie skanowania do określonej kategorii.

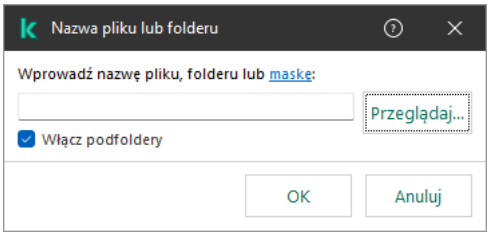
8. W celu wykluczenia pliku lub folderu ze skanowania:



Ustawienia wykluczeń

a. W sekcji **Właściwości** zaznacz pole **Plik lub folder**.

b. W poniższym bloku kliknij odnośnik, aby otworzyć okno **Nazwa pliku lub folderu**.



Wybierz plik lub folder

a. Wprowadź nazwę pliku lub folderu bądź maskę nazwy pliku lub folderu, albo wybierz plik lub folder w drzewie folderów, klikając **Przeglądaj**.

Użyj masek:

- Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.

- Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.

- Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

Możesz użyć masek na początku, w środku lub na końcu ścieżki pliku. Na przykład, jeśli chcesz dodać do wykluczeń folder dla wszystkich użytkowników, należy wprowadzić maskę `?:\Users\*\Folder\`.

Kaspersky Endpoint Security obsługuje zmienne środowiskowe

Można wykluczyć foldery sieciowe. W tym celu należy ręcznie wprowadzić ścieżkę do folderu sieciowego (na przykład: `\\Network Share\*`).

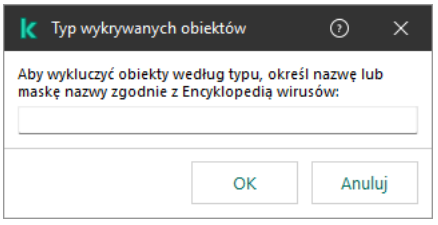
> Kaspersky Endpoint Security nie obsługuje zmiennej środowiskowej `%userprofile%` podczas generowania listy wykluczeń za pomocą konsoli Kaspersky Security Center. Aby zastosować wpis do wszystkich kont użytkowników, możesz użyć znaku `*` (na przykład: `C:\Users\*\Documents\File.exe`). Za każdym razem, gdy dodajesz nową zmienną środowiskową, musisz uruchomić aplikację ponownie.

b. Zapisz swoje zmiany.

9. W celu wykluczenia obiektów o określonej nazwie ze skanowania:

   a. W sekcji **Właściwości** zaznacz pole **Typ wykrywanych obiektów**.

   b. W poniższym bloku kliknij odnośnik, aby otworzyć okno **Typ wykrywanych obiektów**.



Wybierz obiekt

   a. Wprowadź nazwę typu obiektu zgodnie z klasyfikacją Encyklopedii Kaspersky (na przykład: `Email-Worm`, `Rootkit` lub `RemoteAdmin`).

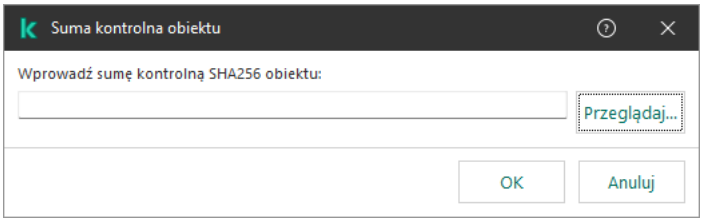
   Możesz użyć masek ze znakiem `?` (zastępuje dowolny pojedynczy znak) oraz znak `*` (zastępuje dowolną liczbę znaków). Na przykład, jeśli określona jest maska `Client*`, Kaspersky Endpoint Security wyklucza obiekty `Client-IRC`, `Client-P2P` i `Client-SMTP` ze skanowania.

   b. Zapisz swoje zmiany.

10. Jeśli chcesz wykluczyć pojedynczy plik ze skanowania:

    a. W sekcji **Właściwości** zaznacz pole **Suma kontrolna obiektu**.

    b. W poniższym bloku kliknij odnośnik, aby otworzyć okno **Suma kontrolna obiektu**.



Wybierz plik

    a. Wprowadź sumę kontrolną pliku lub wybierz plik, klikając przycisk **Przeglądaj**.

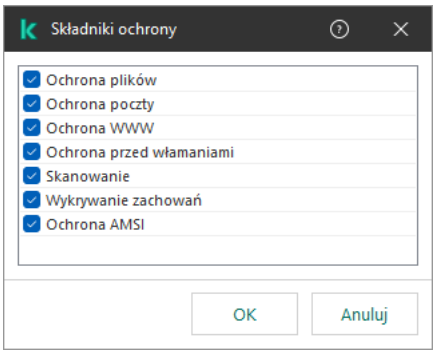
    Jeśli plik został zmodyfikowany, suma kontrolna pliku także zostanie zmodyfikowana. Jeśli taka sytuacja będzie miała miejsce, zmodyfikowany plik nie zostanie dodany do wykluczeń.

    b. Zapisz swoje zmiany.

11. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

12. Wskaż moduły programu Kaspersky Endpoint Security, które będą używać wykluczenia ze skanowania:

    a. W poniższym bloku kliknij odnośnik, aby otworzyć okno **Składniki ochrony**.



Wybierz składniki ochrony

    a. Zaznacz pola obok komponentów, do których mają być stosowane wykluczenia ze skanowania.

       W przypadku określenia komponentów w ustawieniach wykluczenia ze skanowania, to wykluczenie będzie stosowane tylko podczas skanowania przez te moduły programu Kaspersky Endpoint Security.

       W przypadku, gdy komponenty nie zostaną określone w ustawieniach wykluczenia ze skanowania, to wykluczenie będzie stosowane podczas skanowania przez wszystkie moduły programu Kaspersky Endpoint Security.

13. Kliknij **OK**.

    Nowe wykluczenie zostanie dodane do listy. W każdej chwili można wyłączyć wykluczenie za pomocą pola wyboru znajdującego się obok obiektu.

14. Zapisz swoje zmiany.

Jak utworzyć wykluczenie ze skanowania w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Przejdź do sekcji **Strefa zaufana**.

5. W otwartym oknie kliknij odnośnik **Wykluczenia ze skanowania w poszukiwaniu złośliwego oprogramowania**.

6. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę wykluczeń dla wszystkich komputerów w firmie. Listy wykluczeń w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Wykluczenia z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie wykluczeń zasady nadrzędnej nie jest możliwe.

7. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy wykluczeń, zaznacz pole **Zezwól na korzystanie z lokalnych wykluczeń**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę wykluczeń jako dodatek do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

   Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Ponadto jeśli to pole wyboru jest odznaczone, Kaspersky Endpoint Security ukryje skonsolidowaną listę wykluczeń ze skanowania w interfejsie użytkownika aplikacji.

8. Kliknij **Dodaj** i wybierz działanie:

   - **Kategoria**. Możesz grupować wykluczenia ze skanowania w ramach osobnych kategorii. Aby utworzyć nową kategorię, wprowadź nazwę kategorii i dodaj do niej co najmniej jedno wykluczenie ze skanowania.
   - **Nowe wykluczenie**. Kaspersky Endpoint Security dodaje nowe wykluczenie ze skanowania do katalogu głównego listy.
   - **Wybierz wykluczenie z listy**. Aby szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w System Center Configuration Manager, aplikacja zawiera *predefiniowane wykluczenia skanowania*. Dodano także predefiniowane wykluczenia ze skanowania, aby ułatwić konfigurowanie aplikacji w środowiskach wirtualnych Citrix i Vmware. Musisz wybrać predefiniowane wykluczenia ze skanowania w zależności od przeznaczenia chronionego serwera.

   Aby dodać nowe wykluczenie ze skanowania do określonej kategorii, zaznacz pole wyboru znajdujące się obok tej kategorii i zaznacz opcję **Nowe wykluczenie**.

9. Wybierz sposób dodania wykluczenia: **Ścieżka do pliku lub folderu**, **Typ obiektu** lub **Suma kontrolna obiektu**.

10. Aby wykluczyć plik lub folder ze skanowania, wprowadź ścieżkę ręcznie. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`:

    - Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
    - Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.
    - Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

      Możesz użyć masek na początku, w środku lub na końcu ścieżki pliku. Na przykład, jeśli chcesz dodać do wykluczeń folder dla wszystkich użytkowników, należy wprowadzić maskę `?:\Users\*\Folder\`.

      Można wykluczyć foldery sieciowe. W tym celu należy ręcznie wprowadzić ścieżkę do folderu sieciowego (na przykład: `\\Network Share\*`).

11. Jeśli chcesz wykluczyć określony typ obiektu ze skanowania, w polu **Typ obiektu** wprowadź nazwę typu obiektu zgodnie z klasyfikacją Encyklopedii Kaspersky (na przykład: `Email-Worm`, `Rootkit` lub `RemoteAdmin`).

    Możesz użyć masek ze znakiem `?` (zastępuje dowolny pojedynczy znak) oraz znak `*` (zastępuje dowolną liczbę znaków). Na przykład, jeśli określona jest maska `Client*`, Kaspersky Endpoint Security wyklucza obiekty `Client-IRC`, `Client-P2P` i `Client-SMTP` ze skanowania.

12. Jeśli chcesz wykluczyć pojedynczy plik ze skanowania, wprowadź sumę kontrolną pliku w polu **Suma kontrolna obiektu**.

    Jeśli plik został zmodyfikowany, suma kontrolna pliku także zostanie zmodyfikowana. Jeśli taka sytuacja będzie miała miejsce, zmodyfikowany plik nie zostanie dodany do wykluczeń.

13. W sekcji **Zastosuj wykluczenie do** wybierz komponenty, do których ma zostać zastosowane wykluczenie ze skanowania.

14. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

15. Kliknij **OK**.

    Nowe wykluczenie zostanie dodane do listy. W dowolnym momencie możesz użyć przełącznika do zatrzymania wykluczenia.

16. Zapisz swoje zmiany.

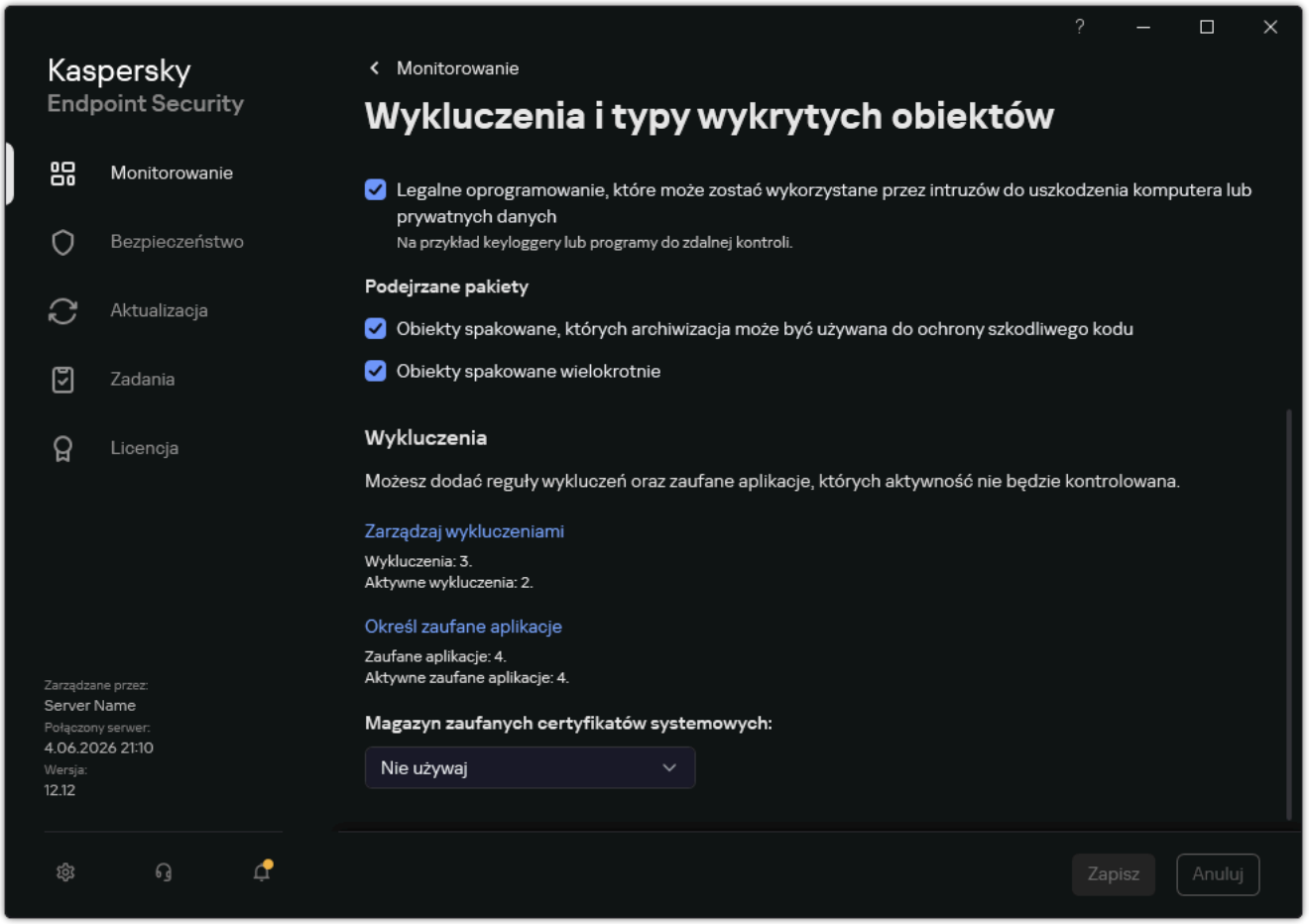
Jak utworzyć wykluczenie ze skanowania w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Wykluczenia i typy wykrytych obiektów**.

3. W sekcji **Wykluczenia** kliknij odnośnik **Zarządzaj wykluczeniami**.

Kaspersky Endpoint Security ukrywa listę wykluczeń ze skanowania w interfejsie użytkownika aplikacji, jeśli konfiguracja wykluczeń ze skanowania została zablokowana przez administratora w konsoli (symbol „zamkniętej kłódki"), a wykluczenia ze skanowania lokalnego są zabronione (pole wyboru **Zezwól na korzystanie z lokalnych wykluczeń** jest odznaczone).



Ustawienia wykluczeń

4. Kliknij **Dodaj** i wybierz działanie:

   - **Kategoria**. Możesz grupować wykluczenia ze skanowania w ramach osobnych kategorii. Aby utworzyć nową kategorię, wprowadź nazwę kategorii i dodaj do niej co najmniej jedno wykluczenie ze skanowania.
   - **Nowe wykluczenie**. Kaspersky Endpoint Security dodaje nowe wykluczenie ze skanowania do katalogu głównego listy.
   - **Wybierz wykluczenie z listy**. Aby szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w System Center Configuration Manager, aplikacja zawiera *predefiniowane wykluczenia skanowania*. Dodano także predefiniowane wykluczenia ze skanowania, aby ułatwić konfigurowanie aplikacji w środowiskach wirtualnych Citrix i Vmware. Musisz wybrać predefiniowane wykluczenia ze skanowania w zależności od przeznaczenia chronionego serwera.

   Aby dodać nowe wykluczenie ze skanowania do określonej kategorii, zaznacz pole wyboru znajdujące się obok tej kategorii i zaznacz opcję **Nowe wykluczenie**.

5. Jeśli chcesz wykluczyć plik lub folder ze skanowania, wybierz plik lub folder, klikając przycisk **Przeglądaj**.

Możesz także wprowadzić ścieżkę ręczne. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`:

- Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.

- Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.

- Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

  Możesz użyć masek na początku, w środku lub na końcu ścieżki pliku. Na przykład, jeśli chcesz dodać do wykluczeń folder dla wszystkich użytkowników, należy wprowadzić maskę `?:\Users\*\Folder\`.

  Można wykluczyć foldery sieciowe. W tym celu należy ręcznie wprowadzić ścieżkę do folderu sieciowego (na przykład: `\\Network Share\*`).

6. Jeśli chcesz wykluczyć określony typ obiektu ze skanowania, w polu **Typy wykrywanych obiektów** wprowadź nazwę typu obiektu zgodnie z klasyfikacją Encyklopedii Kaspersky (na przykład: `Email-Worm`, `Rootkit` lub `RemoteAdmin`).

   Możesz użyć masek ze znakiem `?` (zastępuje dowolny pojedynczy znak) oraz znak `*` (zastępuje dowolną liczbę znaków). Na przykład, jeśli określona jest maska `Client*`, Kaspersky Endpoint Security wyklucza obiekty `Client-IRC`, `Client-P2P` i `Client-SMTP` ze skanowania.

7. Jeśli chcesz wykluczyć pojedynczy plik ze skanowania, wprowadź sumę kontrolną pliku w polu **Suma kontrolna obiektu**.

   Jeśli plik został zmodyfikowany, suma kontrolna pliku także zostanie zmodyfikowana. Jeśli taka sytuacja będzie miała miejsce, zmodyfikowany plik nie zostanie dodany do wykluczeń.

8. W sekcji **Składniki ochrony** wybierz komponenty, do których ma zostać zastosowane wykluczenie ze skanowania.

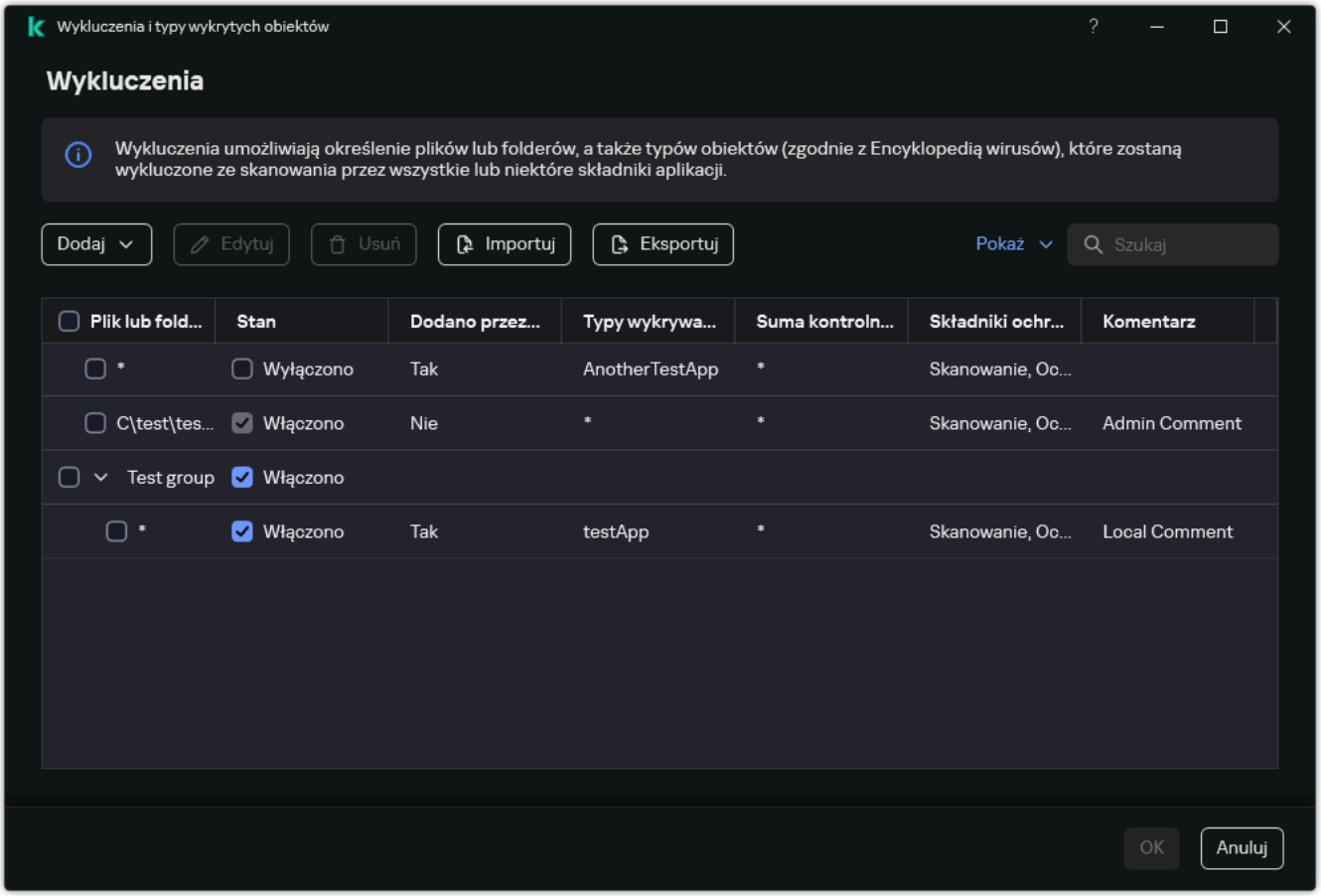
9. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

10. Dla wykluczenia wybierz stan **Aktywny**.

11. Kliknij **Dodaj**.

    Nowe wykluczenie zostanie dodane do listy. W każdej chwili można wyłączyć wykluczenie za pomocą pola wyboru znajdującego się w kolumnie **Stan**.

12. Zapisz swoje zmiany.



Lista wykluczeń

Przykłady masek ścieżek:

Zalecamy określanie ścieżek względnych zamiast ścieżek bezwzględnych. Dzięki temu można wykluczać nie tylko obiekty systemu plików, ale także obiekty bezplikowe. Na przykład, `*\Program Files (x86)\Folder\Subfolder`.

Ścieżki do plików znajdujących się w dowolnym folderze:

- Maska `*.exe` będzie zawierała wszystkie ścieżki do plików, które posiadają rozszerzenie exe.
- Maska `example*` będzie zawierała wszystkie ścieżki do plików o nazwie EXAMPLE.

Ścieżki do plików znajdujących się w określonym folderze:

- Maska `C:\dir\*.*` będzie zawierała wszystkie ścieżki do plików znajdujących się w folderze `C:\dir\`, ale nie w podfolderach `C:\dir\`.
- Maska `C:\dir\*` będzie zawierała wszystkie ścieżki do plików znajdujących się w folderze `C:\dir\`, włączając podfoldery.
- Maska `C:\dir\` będzie zawierała wszystkie ścieżki do plików znajdujących się w folderze `C:\dir\`, włączając podfoldery.
- Maska `C:\dir\*.exe` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem EXE, znajdujących się w folderze `C:\dir\`, ale nie w podfolderach `C:\dir\`.
- Maska `C:\dir\test` będzie zawierała wszystkie ścieżki do plików o nazwie „test" znajdujących się w folderze `C:\dir\`, ale nie w podfolderach `C:\dir\`.
- Maska `C:\dir\*\test` będzie zawierała wszystkie ścieżki do plików o nazwie „test" znajdujących się w folderze `C:\dir\` i w podfolderach `C:\dir\`.
- Maska `C:\dir1\*\dir3\` będzie obejmować wszystkie ścieżki do plików w podfolderach dir3 o jeden poziom niżej z folderu `C:\dir1\`.
- Maska `C:\dir1\**\dirN\` będzie obejmować wszystkie ścieżki do plików w podfolderach dirN na wszystkich poziomach w folderze `C:\dir1\`.

Ścieżki do plików znajdujących się we wszystkich folderach z określoną nazwą:

- Maska `dir\*.*` będzie zawierała wszystkie ścieżki do plików w folderach o nazwie „dir", ale nie w podfolderach tych folderów.
- Maska `dir\*` będzie zawierała wszystkie ścieżki do plików w folderach o nazwie „dir", ale nie w podfolderach tych folderów.
- Maska `dir\` będzie zawierała wszystkie ścieżki do plików w folderach o nazwie „dir", ale nie w podfolderach tych folderów.
- Maska `dir\*.exe` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem EXE, znajdujących się w folderach o nazwie „dir", ale nie w podfolderach tych folderów.
- Maska `dir\test` będzie zawierała wszystkie ścieżki do plików o nazwie „test", znajdujących się w folderach o nazwie „dir", ale nie w podfolderach tych folderów.

Tworzenie wykluczenia według typu wykrytych obiektów

Kaspersky Endpoint Security klasyfikuje wykryte obiekty w następujący sposób:

- **Wirusy i robaki**

  Podkategoria: wirusy i robaki (Viruses_and_Worms)

  Poziom zagrożenia: wysoki

  Klasyczne wirusy i robaki wykonują akcje nieautoryzowane przez użytkownika. Mogą one tworzyć swoje kopie, które także są zdolne do powielania się.

  Klasyczny wirus

Po przeniknięciu klasycznego wirusa do komputera, infekuje on plik, aktywuje się w nim, wykonuje szkodliwe działania i dodaje swoje kopie do innych plików.

Klasyczny wirus rozprzestrzenia się jedynie na zasobach lokalnych komputera; nie może sam przedostać się na inne komputery. Przedostanie się takiego wirusa na inny komputer jest możliwe, jeśli doda on swoją kopię do pliku przechowywanego w folderze współdzielonym lub na nośniku CD, albo gdy użytkownik wyśle wiadomość z zainfekowanym załącznikiem.

Kod klasycznego wirusa może przedostać się do różnych obszarów komputerów, systemów operacyjnych lub aplikacji. W zależności od środowiska wirusy dzieli się na *wirusy plikowe*, *wirusy sektora startowego*, *wirusy skryptowe* oraz *makrowirusy*.

Wirusy mogą infekować pliki, korzystając z szerokiej gamy technik. Wirusy *Overwriting* zapisują swój kod na kodzie zainfekowanego pliku, wymazując zawartość tego pliku. Zainfekowany plik przestaje poprawnie działać oraz nie ma możliwości jego przywrócenia. Wirusy *Parasitic* modyfikują pliki, zezwalając na ich pełne lub częściowe działanie. *Companion* nie modyfikują plików, lecz tworzą ich kopie. Kiedy otwarty zostanie zainfekowany plik, uruchomiona zostanie jego kopia (czyli wirus). Istnieją również inne typy wirusów: *wirusy Link*, *wirusy plików OBJ*, *wirusy bibliotek LIB*, wirusy *infekujące kody źródłowe* oraz wiele innych.

Worm

Podobnie jak w przypadku klasycznego wirusa, kod robaka zostaje aktywowany i wykonuje on szkodliwe działania po przeniknięciu do komputera. Robaki noszą taką nazwę z powodu swojej zdolności do „przepełzania" z jednego komputera na inny i rozprzestrzeniania swoich kopii za pośrednictwem wielu kanałów danych bez wiedzy użytkownika.

Główną cechą, która umożliwia rozróżnianie typów robaków, jest ich sposób rozprzestrzeniania się. Następująca tabela zawiera przegląd różnych typów robaków, klasyfikowanych zgodnie ze sposobem rozprzestrzeniania się.

Sposoby rozprzestrzeniania się robaka

Typ	Nazwa	Opis
Email-Worm	Email-Worm	Rozprzestrzeniają się poprzez pocztę elektroniczną. Zainfekowana wiadomość zawiera załączony plik z kopią robaka lub odnośnik do pliku znajdującego się na stronie internetowej, która może być albo przechwycona przez hakerów, albo stworzona specjalnie w tym celu. Jeśli otworzysz zainfekowany plik, robak zostanie aktywowany. Po kliknięciu odsyłacza, pobraniu i otwarciu pliku, robak również rozpoczyna swoją szkodliwą działalność. Następnie zaczyna rozprzestrzeniać swoje kopie, wyszukując kolejne adresy e-mail i wysyłając na nie zainfekowane wiadomości.
IM-Worm	Robaki klientów komunikatorów internetowych	Rozprzestrzeniają się poprzez klienty komunikatorów internetowych. Z reguły robaki te za pośrednictwem listy kontaktów użytkownika wysyłają wiadomości zawierające odnośnik do pliku ze swoją kopią. Po pobraniu i otwarciu takiego pliku przez użytkownika, robak jest aktywowany.
IRC-Worm	Robaki czatu internetowego	Rozprzestrzeniają się za pośrednictwem kanału Internet Relay Chats – czyli usługi sieciowej pozwalającej na komunikowanie się w internecie w czasie rzeczywistym. Robaki te publikują w czacie internetowym pliki zawierające ich kopie lub odnośniki do pliku. Po pobraniu i otwarciu takiego pliku przez użytkownika, robak jest aktywowany.
Net-Worm	Robaki sieciowe	Rozprzestrzeniają się one w sieciach komputerowych. W przeciwieństwie do innych rodzajów robaków, typowy robak sieciowy rozprzestrzenia się bez udziału użytkownika. Skanuje on sieć lokalną w poszukiwaniu komputerów z programami zawierającymi luki. W tym celu wysyła on specjalny pakiet sieciowy (exploit) zawierający kod robaka lub część kodu. Jeśli komputer posiadający luki znajduje się w sieci, otrzyma taki pakiet sieciowy. Po przeprowadzeniu pełnej penetracji komputera, jest on aktywowany.
P2P-Worm	Robaki sieci wymiany plików	Rozprzestrzeniają się one w sieciach peer-to-peer. Aby dostać się do sieci P2P, robak kopiuje się do foldera wymiany plików, który zazwyczaj znajduje się na komputerze użytkownika. Sieć P2P wyświetli informacje o tym pliku, aby użytkownik "znalazł" zainfekowany plik w sieci, pobrał go i otworzył. Bardziej zaawansowane robaki emulują protokół sieciowy konkretnej sieci P2P: wyświetlają pozytywne wyniki wyszukiwanego obiektu i proponują pobranie swoich własnych kopii.

Typ	Nazwa	Opis
Worm	Inne rodzaje robaków	Inne rodzaje robaków obejmują: • Robaki rozprzestrzeniające swoje kopie w zasobach sieciowych. Przy użyciu funkcji systemu operacyjnego skanują dostępne foldery sieciowe, łączą się z komputerami w Internecie i próbują uzyskać pełen dostęp do ich dysków. W przeciwieństwie do opisanych wyżej robaków, inne typy robaków nie aktywują się automatycznie, lecz w momencie, gdy użytkownik otworzy plik zawierający kopię robaka. • Robaki, które nie rozprzestrzeniają się w żaden z powyższych sposobów (na przykład te robaki, które rozprzestrzeniają się poprzez telefony komórkowe).

- **Trojany (w tym oprogramowanie typu ransomware)**

  Podkategoria: trojany

  Poziom zagrożenia: wysoki

  W przeciwieństwie do wirusów i robaków, trojany nie tworzą swoich kopii. Przenikają one do komputera, na przykład, za pośrednictwem wiadomości e-mail lub przeglądarki internetowej po otwarciu zainfekowanej strony. Trojany uruchamiają się przy udziale użytkownika. Zaczynają wykonywać szkodliwe działania zaraz po uruchomieniu.

  Różne programy typu trojan zachowują się odmiennie na zainfekowanych komputerach. Głównym zadaniem trojanów jest blokowanie, modyfikowanie lub niszczenie informacji, wyłączanie komputera lub sieci. Poza tym, trojany otrzymują lub wysyłają pliki, uruchamiają je, wyświetlają wiadomości na ekranie, pobierają i instalują aplikacje, uruchamiają ponownie komputer oraz żądają połączenia ze stroną internetową.

  Hakerzy często używają "zestawów" trojanów.

  Typowe zachowanie trojanów opisane jest w poniższej tabeli.

  Typy zachowań trojanów na zainfekowanym komputerze

Typ	Nazwa	Opis
Trojan-ArcBomb	Trojany – "archiwa-bomby"	Archiwa, które po rozpakowaniu zwiększają swój rozmiar, co zakłóca działanie komputera. Podczas próby rozpakowania takiego archiwum komputer może spowolnić swoje działanie lub całkowicie się zawiesić, a dysk twardy może zostać wypełniony „pustymi" danymi. Archiwa-bomby są szczególnie niebezpieczne dla serwerów poczty i plików. Jeśli serwer korzysta z automatycznego systemu przetwarzania informacji przychodzących, archiwum-bomba może zatrzymać jego działanie.
Backdoor	Trojany do zdalnej administracji	Uważa się, że jest to najbardziej niebezpieczny rodzaj trojanów. Dzięki swoim funkcjom są one podobne do programów służących do zdalnej administracji aplikacji zainstalowanych na komputerach. Trojany instalują się na komputerze bez wiedzy użytkownika i pozwalają hakerowi na jego zdalne zarządzanie.
Trojan	Trojany	Do trojanów zaliczają się następujące szkodliwe aplikacji: • **Klasyczne trojany**. Wykonują tylko podstawowe funkcje charakterystyczne dla trojanów: blokują, modyfikują lub niszczą informacje, wyłączają komputery lub sieci. W odróżnieniu od trojanów opisanych w tabeli, nie charakteryzują się żadnymi zaawansowanymi funkcjami. • **Wszechstronne trojany**. Posiadają zaawansowane funkcje typowe dla kilku rodzajów trojanów.
Trojan-Ransom	Trojany przeznaczone do wyłudzania pieniędzy	Jako "zakładników" biorą one informacje użytkownika, modyfikują lub blokują je, albo tak wpływają na działanie komputera, że użytkownik nie może korzystać z informacji. Cyberprzestępca żąda okupu od użytkownika, obiecując, że wyśle aplikację, która przywróci działanie komputera oraz przechowywane na nim dane.
Trojan-Clicker	Trojany klikające	Łączą się one ze stronami internetowymi albo przez wysłanie polecenia do przeglądarki albo przez zmianę adresów stron znajdujących się w plikach systemowych. Przy użyciu tych programów hakerzy przeprowadzają ataki sieciowe i zwiększają ranking stron internetowych celem zwiększenia liczby wyświetlania banerów reklamowych.

Typ	Nazwa	Opis
Trojan-Downloader	Trojany pobierające	Uzyskują dostęp do strony internetowej cyberprzestępcy, pobierają z niej szkodliwe aplikacje i instalują je na komputerze użytkownika. Mogą zawierać nazwę pliku szkodliwej aplikacji do pobrania lub uzyskać ją z otwartej strony internetowej.
Trojan-Dropper	Trojany droppery	Zawierają inne trojany, które instalują na dysku twardym. Hakerzy mogą użyć tego typu trojanów do następujących celów: • Instalacji szkodliwej aplikacji w sposób niezauważalny dla użytkownika: Trojan-Dropper to typ programów, które nie wyświetlają żadnych wiadomości lub wyświetlają fałszywe komunikaty informujące, na przykład, o błędzie w archiwum lub niekompatybilnej wersji systemu operacyjnego. • Ochrony innych znanych szkodliwych aplikacji przed wykryciem przez ochronę komputera: nie wszystkie programy antywirusowe są w stanie wykryć szkodliwą aplikację wewnątrz aplikacji Trojan-Dropper.
Trojan-Notifier	Trojany powiadamiające	Informują cyberprzestępcę o możliwości dostępu do zainfekowanego komputera, wysyłając do niego informacje o tym komputerze: adres IP, numer otwartego portu lub adres e-mail. Komunikują się z hakerem, na przykład, za pośrednictwem wiadomości e-mail, serwera FTP lub jego strony internetowej. Trojany typu Notifier często są wykorzystywane w zestawach złożonych z kilku trojanów. Powiadamiają one hakera, że inne trojany zostały pomyślnie zainstalowane na komputerze użytkownika.
Trojan-Proxy	Trojany proxy	Umożliwiają one hakerowi uzyskanie anonimowego dostępu do stron internetowych przy użyciu komputera użytkownika i są często używane do wysyłania spamu.
Trojan-PSW	Oprogramowanie kradnące hasła	Oprogramowanie kradnące hasła to rodzaj trojanów kradnących konta użytkownika, na przykład dane rejestracyjne oprogramowania. Takie trojany odnajdują w plikach systemowych i rejestrze poufne dane, a następnie wysyłają je do atakującego, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej. Niektóre z tych trojanów podzielone są na kategorie oddzielnych typów opisanych w tej tabeli. Należą do nich Trojany kradnące konta bankowe (Trojan-Banker), trojany kradnące informacje od użytkowników komunikatorów internetowych (Trojan-IM) oraz trojany kradnące informacje od graczy online (Trojan-GameThief).
Trojan-Spy	Trojany szpiegujące	Szpiegują one użytkownika, zbierając informacje o jego działaniach podczas pracy na komputerze. Mogą przechwytywać dane wprowadzane przez użytkownika przy użyciu klawiatury, tworzyć zrzuty ekranu lub tworzyć listę aktywnych aplikacji. Po zebraniu informacji, wysyłają je do hakera, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.
Trojan-DDoS	Ataki sieciowe przez trojany	Wysyłają one liczne żądania z komputera użytkownika na serwer zdalny. Serwer nie ma wystarczającej ilości zasobów do przetworzenia wszystkich żądań, w rezultacie przestaje działać (Denial-of-Service lub DoS). Hakerzy często infekują wiele komputerów dzięki takim programom, przez co mogą wykorzystać te komputery do jednoczesnego ataku na pojedynczy serwer. Programy DoS przeprowadzają atak z jednego komputera za wiedzą użytkownika. Programy DDoS (Distributed DoS) przeprowadzają rozproszone ataki z różnych komputerów bez wiedzy użytkownika zainfekowanego komputera.
Trojan-IM	Trojany kradnące informacje od użytkowników komunikatorów internetowych	Kradną numery kont i hasła użytkowników klientów komunikatorów internetowych. Przesyłają dane hakerowi, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.
Rootkit	Rootkity	Ukrywają inne szkodliwe aplikacje i ich aktywność, przedłużając ich obecność w systemie. Mogą również ukrywać pliki i procesy w pamięci zainfekowanego komputera lub kluczach rejestru. Rootkity mogą ukrywać wymianę danych pomiędzy aplikacjami znajdującymi się na komputerze użytkownika i innymi komputerami podłączonymi do sieci.
Trojan-SMS	Trojany wysyłające wiadomości SMS	Infekują one telefony komórkowe, wysyłając wiadomości SMS na numery o podwyższonej opłacie.
Trojan-GameThief	Trojany kradnące informacje od osób grających w sieci	Kradną dane uwierzytelniające kont osób grających w sieci, po czym wysyłają je hakerowi za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.
Trojan-Banker	Trojany kradnące konta bankowe	Kradną dane konta bankowego lub dane systemu płatności elektronicznych, po czym wysyłają je cyberprzestępcy za pośrednictwem poczty elektronicznej, serwera FTP, jego strony internetowej lub przy użyciu innych metod.
Trojan-Mailfinder	Trojany zbierające adresy e-mail	Zbierają one adresy e-mail przechowywane na komputerze i wysyłają je hakerowi, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej. Na zebrane adresy hakerzy mogą wysyłać spam.

- **Szkodliwe narzędzia**

  Podkategoria: szkodliwe narzędzia

  Poziom zagrożenia: Średni

  W odróżnieniu od innych typów szkodliwego oprogramowania, szkodliwe narzędzia nie wykonują swoich akcji zaraz po uruchomieniu. Mogą być bezpiecznie przechowywane i uruchamiane na komputerze użytkownika. Hakerzy często używają funkcji tych programów do tworzenia wirusów, robaków i trojanów oraz do przeprowadzania ataków sieciowych na serwery zdalne, łamania zabezpieczeń komputerów lub wykonywania innych szkodliwych działań.

  Różne funkcje szkodliwych narzędzi pogrupowane są według typów opisanych w poniższej tabeli.

  Funkcje szkodliwych narzędzi

Typ	Nazwa	Opis
Constructor	Konstruktory	Umożliwiają utworzenie nowych wirusów, robaków i trojanów. Niektóre konstruktory posiadają standardowy interfejs oparty na oknach, w którym użytkownik może wybrać typ szkodliwej aplikacji, jaki chce stworzyć, sposób przeciwdziałania debuggerom oraz inne funkcje.
Dos	Ataki sieciowe	Wysyłają one liczne żądania z komputera użytkownika na serwer zdalny. Serwer nie ma wystarczającej ilości zasobów do przetworzenia wszystkich żądań, w rezultacie przestaje działać (Denial-of-Service lub DoS).
Exploit	Exploity	*Exploit* jest zestawem danych lub kodem programu używającym luki aplikacji, w której jest przetwarzany, do wykonania szkodliwych działań na komputerze. Na przykład, exploit może odczytywać lub zapisywać pliki lub uzyskiwać dostęp do „zainfekowanych" stron internetowych. Różne exploity używają luk w różnych aplikacjach lub usługach sieciowych. Wyglądający jak pakiet sieciowy exploit wysyłany jest przez sieć w poszukiwaniu takich komputerów, których usługi sieciowe posiadają luki. Exploit w pliku DOC używa luk występujących w edytorach tekstu. Po otwarciu przez użytkownika zainfekowanego pliku, może on zacząć wykonywać zaprogramowane przez hakera działania. Exploit osadzony w wiadomości elektronicznej wyszukuje luki w dowolnym kliencie pocztowym. Po otwarciu przez użytkownika zainfekowanego pliku w tym programie pocztowym, wykonuje on szkodliwe działanie. Robaki Net-Worms rozprzestrzeniają się w sieci przy pomocy exploitów. Exploity Nuker są pakietami sieciowymi wyłączającymi komputery.
FileCryptor	Narzędzia szyfrujące	Szyfrują one inne szkodliwe aplikacje, aby ukryć je przed programem antywirusowym.
Flooder	Programy „zaśmiecające" sieci	Wysyłają one wiele wiadomości przez kanały sieciowe. Do tego typu narzędzi należy, na przykład, program zaśmiecający Internet Relay Chats (IRC). Wśród narzędzi typu Flooder nie ma programów "zaśmiecających" kanały używane przez programy pocztowe, komunikatory internetowe i systemy komunikacji mobilnej. Programy te wyróżnione są jako oddzielne typy opisane w tej tabeli (Email-Flooder, IM-Flooder oraz SMS-Flooder).
HackTool	Narzędzia hakerskie	Pozwalają na złamanie zabezpieczeń komputera, na którym są zainstalowane, lub na zaatakowanie innego komputera (na przykład, dodając nowe konta systemowe bez wiedzy użytkownika lub wymazując logi systemowe, aby ukryć ślady obecności w systemie operacyjnym). Ten typ narzędzi zawiera sniffery posiadające szkodliwe funkcje, jak choćby przechwytywanie haseł. Sniffery to programy umożliwiające przeglądanie ruchu sieciowego.
Hoax	Żarty (Hoaxes)	Alarmują użytkownika przy użyciu wiadomości podobnej do tej, która używana jest w przypadku wykrycia wirusa: mogą "wykryć wirusa" w nienaruszonym pliku lub powiadomić o formatowaniu dysku, które w rzeczywistości nie ma miejsca.
Spoofer	Narzędzia służące do spoofingu	Wysyłają wiadomości i żądania sieciowe z fałszywym adresem nadawcy. Hakerzy używają narzędzi do spoofingu, na przykład, aby móc podać się za prawdziwych nadawców wiadomości.
VirTool	Narzędzia do modyfikowania szkodliwych aplikacji	Umożliwiają modyfikowanie innego szkodliwego oprogramowania w celu ukrycia go przed aplikacjami antywirusowymi.
Email-Flooder	Programy „zaśmiecające" adresy e-mail	„Zaśmiecają" różne adresy e-mail poprzez wysyłanie na nie licznych wiadomości. Duża liczba wiadomości przychodzących uniemożliwia przejrzenie użytecznych wiadomości znajdujących się w skrzynce odbiorczej.

Typ	Nazwa	Opis
IM-Flooder	Programy „zaśmiecające" ruch wiadomościami klientów komunikatorów internetowych	Wysyłają niechciane wiadomości do użytkowników klientów komunikatorów. Duża liczba odbieranych wiadomości uniemożliwia przeczytanie użytecznych wiadomości.
SMS-Flooder	Programy „zaśmiecające" ruch wiadomościami SMS	Wysyłają one liczne wiadomości SMS na telefony komórkowe.

- **Adware**

  Podkategoria: oprogramowanie reklamujące (adware)

  Poziom zagrożenia: Średni

  Oprogramowanie Adware wyświetla informacje reklamowe użytkownikowi. Programy adware wyświetlają banery reklamowe w interfejsach innych programów i przekierowują wyszukiwanie na strony reklamowe. Niektóre z nich zbierają informacje marketingowe o użytkowniku i wysyłają je do programisty. Do gromadzonych informacji mogą należeć: nazwy stron odwiedzanych przez użytkownika lub wyszukiwana przez niego treść. W odróżnieniu od programów typu Trojan-Spy, programy adware przesyłają te informacje do twórcy za zgodą użytkownika.

- **Auto-dialery**

  Podkategoria: automatyczne dialery (Dialer).

  Poziom zagrożenia: Średni

  Automatyczne dialery umożliwiają dyskretne nawiązywanie połączeń telefonicznych za pomocą modemu.

- **Legalne oprogramowanie, które może zostać wykorzystane przez intruzów do uszkodzenia komputera lub prywatnych danych**

  Podkategoria: Legalne oprogramowanie, które może zostać wykorzystane przez przestępców do uszkodzenia komputera i prywatnych danych.

  Poziom zagrożenia: Średni

  Wiele z tych programów to nieszkodliwe oprogramowanie, z którego korzysta wielu użytkowników. Do tych programów zaliczają się: klienty IRC, auto-dialery, programy pobierające pliki, monitory aktywności systemu komputerowego, narzędzia do haseł, serwery usług FTP, HTTP i Telnet.

  Jednakże, jeśli haker uzyska dostęp do tego typu programów lub jeśli zainstaluje te programy na komputerze użytkownika, to niektóre z ich funkcji mogą zostać użyte do naruszenia ochrony.

  Aplikacje te mają różne funkcje; ich typy zostały opisane w poniższej tabeli.

Typ	Nazwa	Opis
Client-IRC	Klienty czatów internetowych	Użytkownicy instalują programy tego typu, aby móc rozmawiać z innymi w czasie rzeczywistym. Hakerzy używają ich do rozsyłania szkodliwych programów.
Downloader	Programy do pobierania	Mogą pobierać pliki ze stron internetowych w trybie ukrycia.
Monitor	Programy do monitorowania	Umożliwiają monitorowanie aktywności na komputerze, na którym są zainstalowane (sprawdzają, które aplikacje są aktywne i w jaki sposób wymieniają dane z aplikacjami zainstalowanymi na innych komputerach).
PSWTool	Programy do przywracania haseł	Umożliwiają przeglądanie i przywracanie zapomnianych haseł. Hakerzy umieszczają je na komputerze w tym samym celu, w sposób niezauważalny dla użytkownika.

Typ	Nazwa	Opis
RemoteAdmin	Programy do zdalnej administracji	Są używane przez administratorów systemów. Programy te pozwalają uzyskać dostęp do interfejsu zdalnego komputera w celu jego monitorowania i zarządzania. W tym właśnie celu hakerzy niezauważenie umieszczają je na komputerze użytkownika. Legalne programy do zdalnej administracji różnią się od trojanów typu backdoor do zdalnej administracji. Trojany potrafią niezależnie spenetrować system i zainstalować się; legalne programy nie potrafią tego.
Server-FTP	Serwery FTP	Działają jak serwery FTP. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu FTP.
Server-Proxy	Serwery proxy	Działają jak serwery proxy. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
Server-Telnet	Serwery Telnet	Działają jak serwery Telnet. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu Telnet.
Server-Web	Serwery sieciowe	Działają jak serwery sieciowe. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu HTTP.
RiskTool	Narzędzia wykorzystywane do pracy na lokalnym komputerze	Umożliwiają one użytkownikowi korzystanie z dodatkowych funkcji podczas jego pracy na komputerze. Narzędzia te pozwalają użytkownikowi ukryć pliki lub okna uruchomionych aplikacji i zakończyć aktywne procesy.
NetTool	Narzędzia sieciowe	Umożliwiają użytkownikowi korzystanie z dodatkowych funkcji podczas pracy z innymi komputerami w sieci. Posiadają one także możliwość ich ponownego uruchomienia, wykrywania otwartych portów oraz uruchamiania aplikacji zainstalowanych na komputerach.
Client-P2P	Klienty sieciowe P2P	Pozwalają pracować w sieciach peer-to-peer. Mogą być wykorzystywane przez hakerów do rozprzestrzeniania szkodliwego oprogramowania.
Client-SMTP	Klienty SMTP	Wysyłają wiadomości e-mail bez wiedzy użytkownika. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
WebToolbar	Paski narzędzi w przeglądarkach internetowych	Dodają one paski narzędzi w interfejsie innych aplikacji umożliwiające korzystanie z wyszukiwarek internetowych.
FraudTool	Pseudo-programy	Podają się za inne programy. Na przykład, istnieją fałszywe programy antywirusowe, które wyświetlają wiadomości o wykryciu szkodliwego oprogramowania. W rzeczywistości nie skanują ani nie leczą niczego.

- **Obiekty spakowane, których archiwizacja może być używana do ochrony szkodliwego kodu**

  Podkategoria: Spakowane pliki, które mogą wyrządzić szkody.

  Poziom zagrożenia: Średni.

  Plik pakowany jest za pomocą specjalnego narzędzia pakującego, które służy do pakowania złośliwego oprogramowania: wirusów, robaków i trojanów. Kaspersky Endpoint Security skanuje moduł wypakowujący znajdujący się w archiwach SFX (samorozpakowujących się).

  Aby uniemożliwić wykrycie złośliwego oprogramowania przez oprogramowanie antywirusowe, hakerzy pakują je za pomocą specjalnych programów pakujących. Eksperci firmy Kaspersky zidentyfikowali narzędzia pakujące najpopularniejsze wśród hakerów.

- **Obiekty spakowane wielokrotnie**

  Podkategoria: Pliki spakowane wielokrotnie.

  Poziom zagrożenia: Średni.

  Plik jest pakowany przy użyciu jednego lub większej liczby programów pakujących trzy lub więcej razy.

  Aby uniemożliwić wykrycie złośliwego oprogramowania przez program antywirusowy, hakerzy mogą spakować plik wielokrotnie. Kaspersky Endpoint Security skanuje spakowane pliki.

Domyślnie Kaspersky Endpoint Security wykrywa wszystkie typy obiektów. Aby zwiększyć bezpieczeństwo komputera, zalecamy pozostawienie włączonej opcji wykrywania wszystkich typów obiektów. Jeżeli korzystasz z narzędzi wewnętrznych, które aplikacja wykrywa jako złośliwe, dodaj te narzędzia do listy wykluczeń, ale nie wyłączaj wykrywania całego typu obiektów.

Jak wybrać typy wykrywanych obiektów w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Ustawienia ogólne** → **Wykluczenia i typy obiektów**.
5. W sekcji **Typy wykrywanych obiektów** kliknij przycisk **Ustawienia**.
6. W oknie, które zostanie otwarte, zaznacz pola wyboru obok typów obiektów, które Kaspersky Endpoint Security ma wykrywać.
7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak wybrać typy wykrywalnych obiektów w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

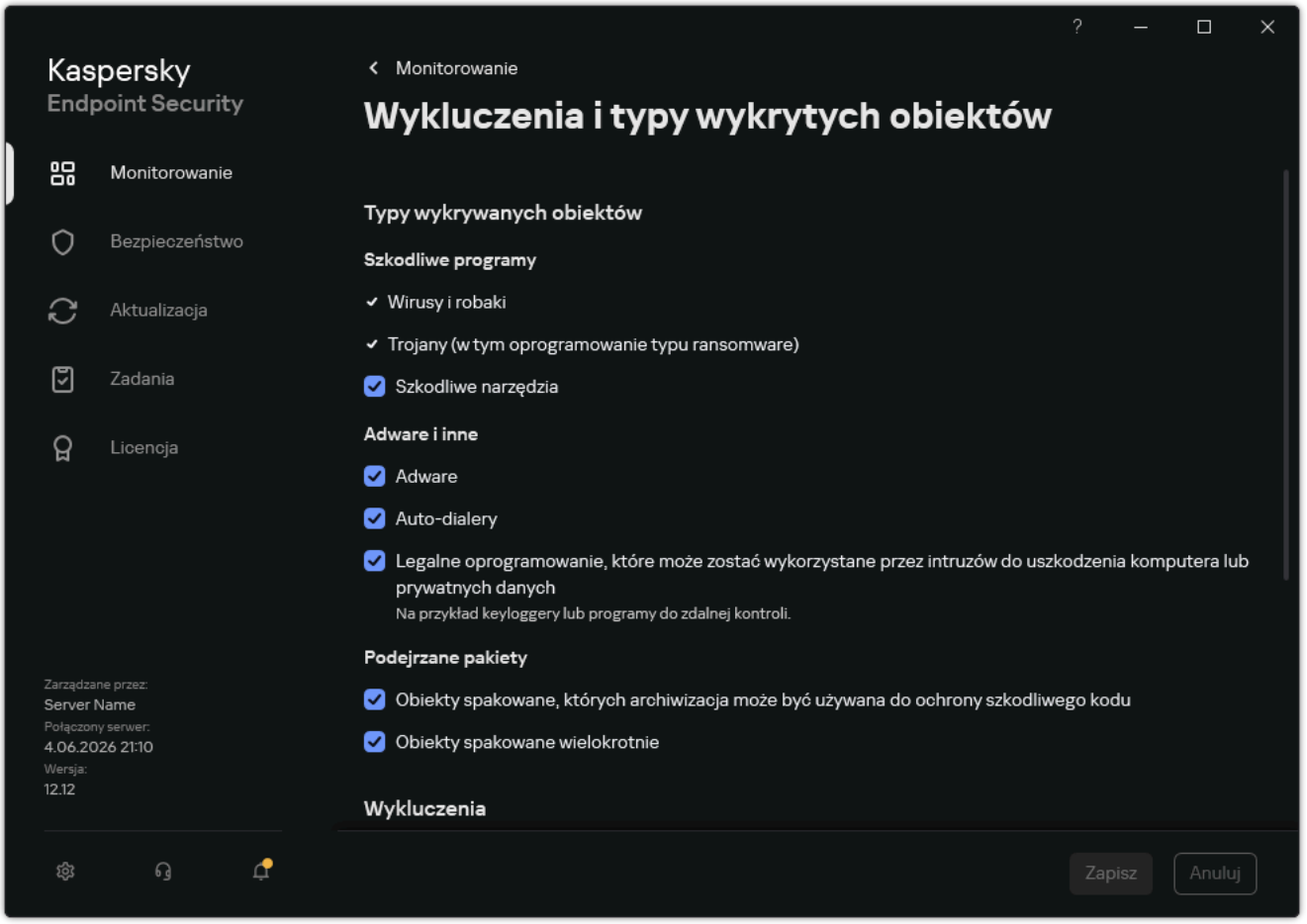
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Ustawienia wykrywania**.
5. W sekcji **Wykrywanie innych typów obiektów** zaznacz pola obok typów obiektów, które Kaspersky Endpoint Security ma wykrywać.
6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak wybrać typy wykrywalnych obiektów w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Wykluczenia i typy wykrytych obiektów**.

3. W sekcji **Typy wykrywanych obiektów** zaznacz pola obok typów obiektów, które Kaspersky Endpoint Security ma wykrywać.

4. Zapisz swoje zmiany.



Typy wykrywalnych obiektów

Modyfikowanie listy zaufanych aplikacji

Lista zaufanych aplikacji jest listą aplikacji, których aktywność sieciowa i plikowa (włączając w to szkodliwą aktywność) oraz dostęp do rejestru systemowego nie są monitorowane przez Kaspersky Endpoint Security. Domyślnie program Kaspersky Endpoint Security monitoruje obiekty otwierane, uruchamiane lub zapisywane przez proces dowolnej aplikacji i kontroluje aktywność wszystkich aplikacji oraz ruch sieciowy będący wynikiem ich działania. Po dodaniu aplikacji do listy zaufanych aplikacji, Kaspersky Endpoint Security przestaje monitorować jej aktywność.

Różnica pomiędzy wykluczeniami skanowania a aplikacjami zaufanymi polega na tym, że w przypadku wykluczeń Kaspersky Endpoint Security nie skanuje plików, natomiast w przypadku aplikacji zaufanych nie kontroluje zainicjowanych procesów. Jeżeli aplikacja zaufana utworzy szkodliwy plik w folderze, który nie jest zawarty w wykluczeniach skanowania, Kaspersky Endpoint Security wykryje plik i wyeliminuje zagrożenie. Jeżeli folder zostanie dodany do wykluczeń, Kaspersky Endpoint Security pominie ten plik.

Na przykład jeżeli uważasz, że obiekty używane przez Notatnik firmy Microsoft Windows są nieszkodliwe (tzn. ufasz tej aplikacji), dodaj Notatnik firmy Microsoft Windows do listy zaufanych aplikacji, aby obiekty używane przez tę aplikację nie były monitorowane. Zwiększy to wydajność komputera, co jest szczególnie ważne przy korzystaniu z aplikacji serwerowych.

Oprócz tego pewne akcje zaklasyfikowane przez Kaspersky Endpoint Security jako podejrzane mogą być traktowane przez inne aplikacje jako nieszkodliwe. Na przykład przechwytywanie danych wprowadzanych z klawiatury jest charakterystyczne dla aplikacji, które automatycznie przełączają układ klawiatury (np. Punto Switcher). Aby korzystać z właściwości takich aplikacji i wyłączyć monitorowanie ich aktywności, dodaj je do listy zaufanych aplikacji.

Aplikacje zaufane pomagają uniknąć problemów z kompatybilnością pomiędzy Kaspersky Endpoint Security a innymi aplikacjami (na przykład: problem podwójnego skanowania ruchu sieciowego komputera osoby trzeciej przez Kaspersky Endpoint Security i przez inną aplikację antywirusową).

Należy pamiętać, że pliki wykonywalne oraz procesy zaufanych aplikacji będą nadal skanowane w poszukiwaniu wirusów i szkodliwych programów. Aplikacja może zostać całkowicie wykluczona ze skanowania wykonywanego przez program Kaspersky Endpoint Security przy użyciu wykluczeń ze skanowania.

Zmiana listy zaufanych aplikacji może zostać zablokowana przez właściwości zasady nadrzędnej. Aby zmienić listę, musisz zezwolić na zmianę ustawień strefy zaufanej w Web Console (kłódka musi być odblokowana).

Strefy zaufane są grupowane w różny sposób w Konsoli administracyjnej (MMC) i Web Console. Sposoby zapobiegania zmianom parametrów strefy zaufanej również mogą się różnić („kłódki" mogą być inne). Zalecamy korzystanie wyłącznie z Web Console do zarządzania aplikacją. Jeśli skonfigurujesz strefę zaufaną w różnych konsolach, wtyczka zarządzająca może przywrócić „kłódkę" do stanu domyślnego.

Dodawanie aplikacji do listy zaufanych w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Wykluczenia i typy obiektów**.
4. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** → **Zaufane aplikacje** kliknij przycisk **Ustawienia**.

   Zostanie otwarte okno zawierające listę zaufanych aplikacji.
5. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę zaufanych aplikacji dla wszystkich komputerów w firmie. Listy zaufanych aplikacji w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Zaufane aplikacje z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie zaufanych aplikacji zasady nadrzędnej nie jest możliwe.
6. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy zaufanych aplikacji, zaznacz pole **Zezwól na korzystanie z lokalnych zaufanych aplikacji**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę zaufanych aplikacji jako dodatek do ogólnej listy zaufanych aplikacji, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

   Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy zaufanych aplikacji, wygenerowanej w zasadzie. Ponadto jeśli to pole wyboru jest odznaczone, Kaspersky Endpoint Security ukryje skonsolidowaną listę zaufanych aplikacji w interfejsie użytkownika aplikacji.

7. Kliknij **Dodaj** i wybierz działanie:

- **Kategoria**. Możesz grupować zaufane aplikacje w ramach osobnych kategorii. Aby utworzyć nową kategorię, wprowadź nazwę kategorii i dodaj do niej przynajmniej jedną zaufaną aplikację.
- **Nowe wykluczenie**. Kaspersky Endpoint Security dodaje nową zaufaną aplikację do katalogu głównego listy.
- **Wybierz wykluczenie z listy**. Aby szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menadżerze konfiguracji System Center Configuration Manager, aplikacja zawiera *predefiniowane zaufane aplikacje*. Dodano także wstępnie zdefiniowane zaufane aplikacje, aby ułatwić konfigurowanie aplikacji w środowiskach wirtualnych Citrix i VMware. Musisz wybrać predefiniowane zaufane aplikacje w zależności od przeznaczenia chronionego serwera.
- **Nowe wykluczenie w wybranej kategorii**. Wybierz kategorię, aby dodać nową zaufaną aplikację do określonej kategorii.

8. Wybierz kryteria zaufania:

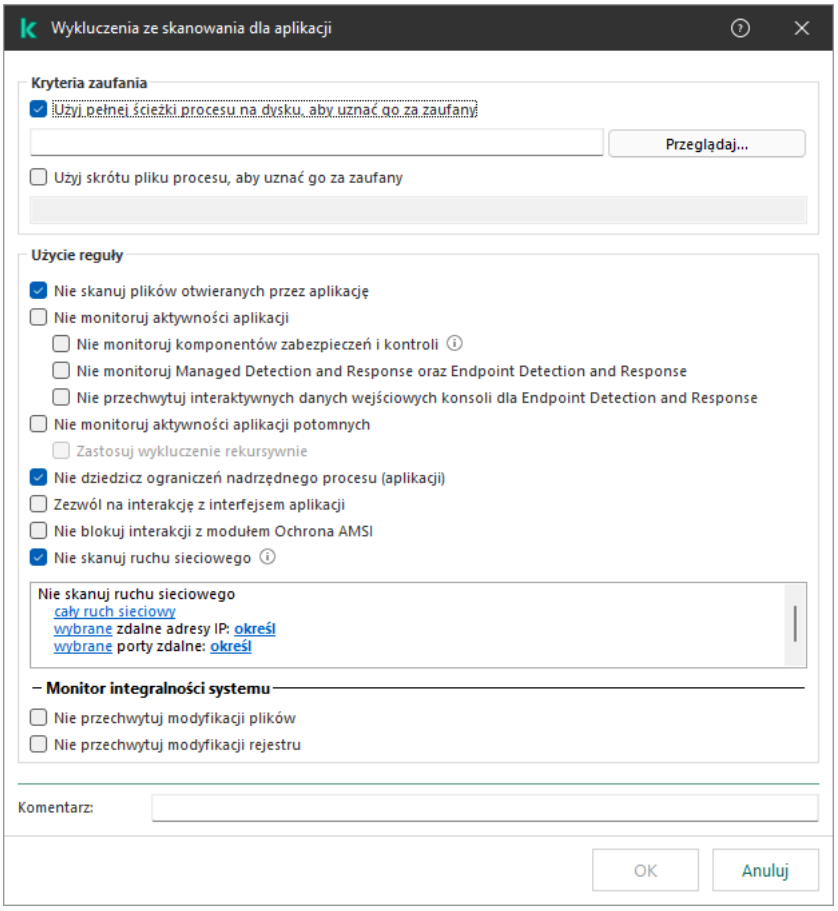
- **Użyj pełnej ścieżki procesu na dysku, aby uznać go za zaufany**. Wprowadź ścieżkę do pliku wykonywalnego zaufanej aplikacji.

  Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

  Kaspersky Endpoint Security rozróżnia wielkość liter w nazwie pliku zaufanej aplikacji. Jeśli w nazwie pliku wpisana zostanie nieprawidłowa wielkość liter, Kaspersky Endpoint Security nie rozpozna zaufanej aplikacji.

- **Użyj skrótu pliku procesu, aby uznać go za zaufany**.

Kaspersky Endpoint Security nie obsługuje zmiennej środowiskowej `%userprofile%` podczas generowania listy zaufanych aplikacji w konsoli Kaspersky Security Center. Aby zastosować wpis do wszystkich kont użytkowników, możesz użyć znaku * (na przykład: `C:\Users\*\Documents\File.exe`). Za każdym razem, gdy dodajesz nową zmienną środowiskową, musisz uruchomić aplikację ponownie.



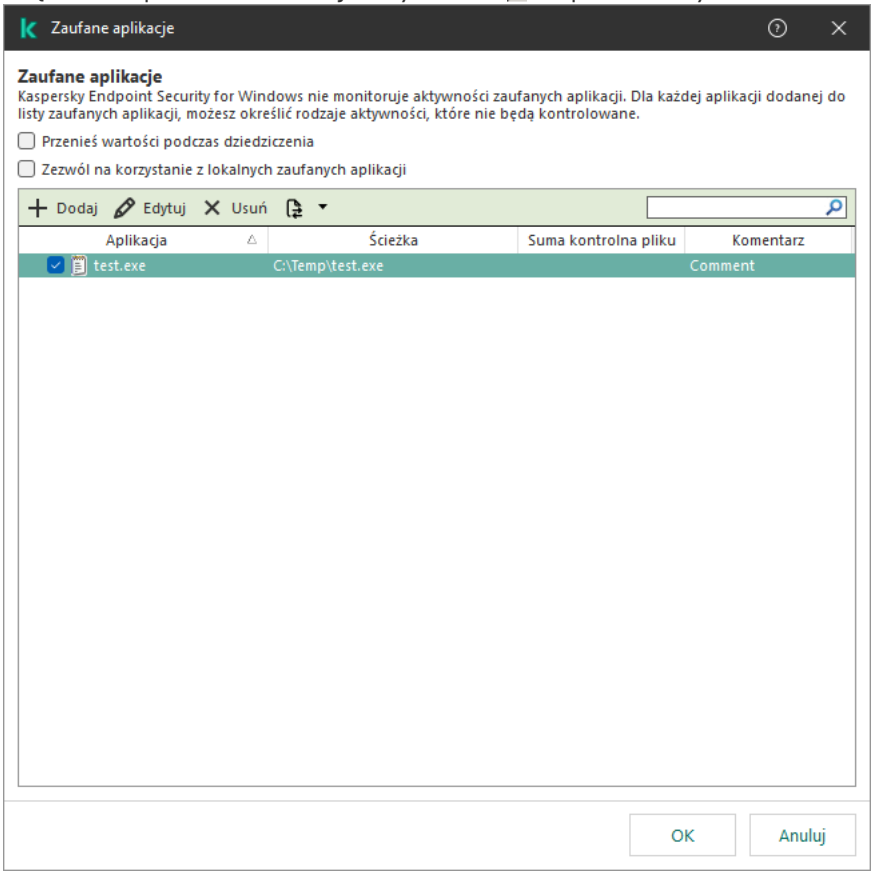
Ustawienia zaufanej aplikacji

9. Skonfiguruj zaawansowane ustawienia zaufanej aplikacji (zapoznaj się z poniższą tabelą).

10. Kliknij **OK**.

    Nowa zaufana aplikacja zostanie dodana do listy. W każdej chwili można wyłączyć aplikację ze strefy zaufanej za pomocą pola wyboru znajdującego się obok obiektu.

11. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.



Lista zaufanych aplikacji

Jak dodać aplikację do listy zaufanych w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do sekcji **Strefa zaufana**.
5. W otwartym oknie kliknij odnośnik **Aplikacje**.

   Zostanie otwarte okno zawierające listę zaufanych aplikacji.
6. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę zaufanych aplikacji dla wszystkich komputerów w firmie. Listy zaufanych aplikacji w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Zaufane aplikacje z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie zaufanych aplikacji zasady nadrzędnej nie jest możliwe.
7. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy zaufanych aplikacji, zaznacz pole **Zezwól na korzystanie z lokalnych wykluczeń**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę zaufanych aplikacji jako dodatek do ogólnej listy zaufanych aplikacji, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

   Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy zaufanych aplikacji, wygenerowanej w zasadzie. Ponadto jeśli to pole wyboru jest odznaczone, Kaspersky Endpoint Security ukryje skonsolidowaną listę zaufanych aplikacji w interfejsie użytkownika aplikacji.

8. Kliknij **Dodaj** i wybierz działanie:

   - **Kategoria**. Możesz grupować zaufane aplikacje w ramach osobnych kategorii. Aby utworzyć nową kategorię, wprowadź nazwę kategorii i dodaj do niej przynajmniej jedną zaufaną aplikację.
   - **Nowe wykluczenie**. Kaspersky Endpoint Security dodaje nową zaufaną aplikację do katalogu głównego listy.
   - **Wybierz wykluczenie z listy**. Aby szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menadżerze konfiguracji System Center Configuration Manager, aplikacja zawiera *predefiniowane zaufane aplikacje*. Dodano także wstępnie zdefiniowane zaufane aplikacje, aby ułatwić konfigurowanie aplikacji w środowiskach wirtualnych Citrix i VMware. Musisz wybrać predefiniowane zaufane aplikacje w zależności od przeznaczenia chronionego serwera.

   Aby dodać nową zaufaną aplikację do określonej kategorii, zaznacz pole wyboru znajdujące się obok tej kategorii i zaznacz opcję **Nowe wykluczenie**.

9. Wybierz kryteria zaufania:

   - **Ścieżka do pliku lub folderu**. Wprowadź ścieżkę do pliku wykonywalnego zaufanej aplikacji.

     Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

     Kaspersky Endpoint Security rozróżnia wielkość liter w nazwie pliku zaufanej aplikacji. Jeśli w nazwie pliku wpisana zostanie nieprawidłowa wielkość liter, Kaspersky Endpoint Security nie rozpozna zaufanej aplikacji.

   - **Skrót aplikacji**.

   > Kaspersky Endpoint Security nie obsługuje zmiennej środowiskowej %userprofile% podczas generowania listy zaufanych aplikacji w konsoli Kaspersky Security Center. Aby zastosować wpis do wszystkich kont użytkowników, możesz użyć znaku `*` (na przykład: `C:\Users\*\Documents\File.exe`). Za każdym razem, gdy dodajesz nową zmienną środowiskową, musisz uruchomić aplikację ponownie.

10. Skonfiguruj zaawansowane ustawienia zaufanej aplikacji (zapoznaj się z poniższą tabelą).

11. Kliknij **OK**.

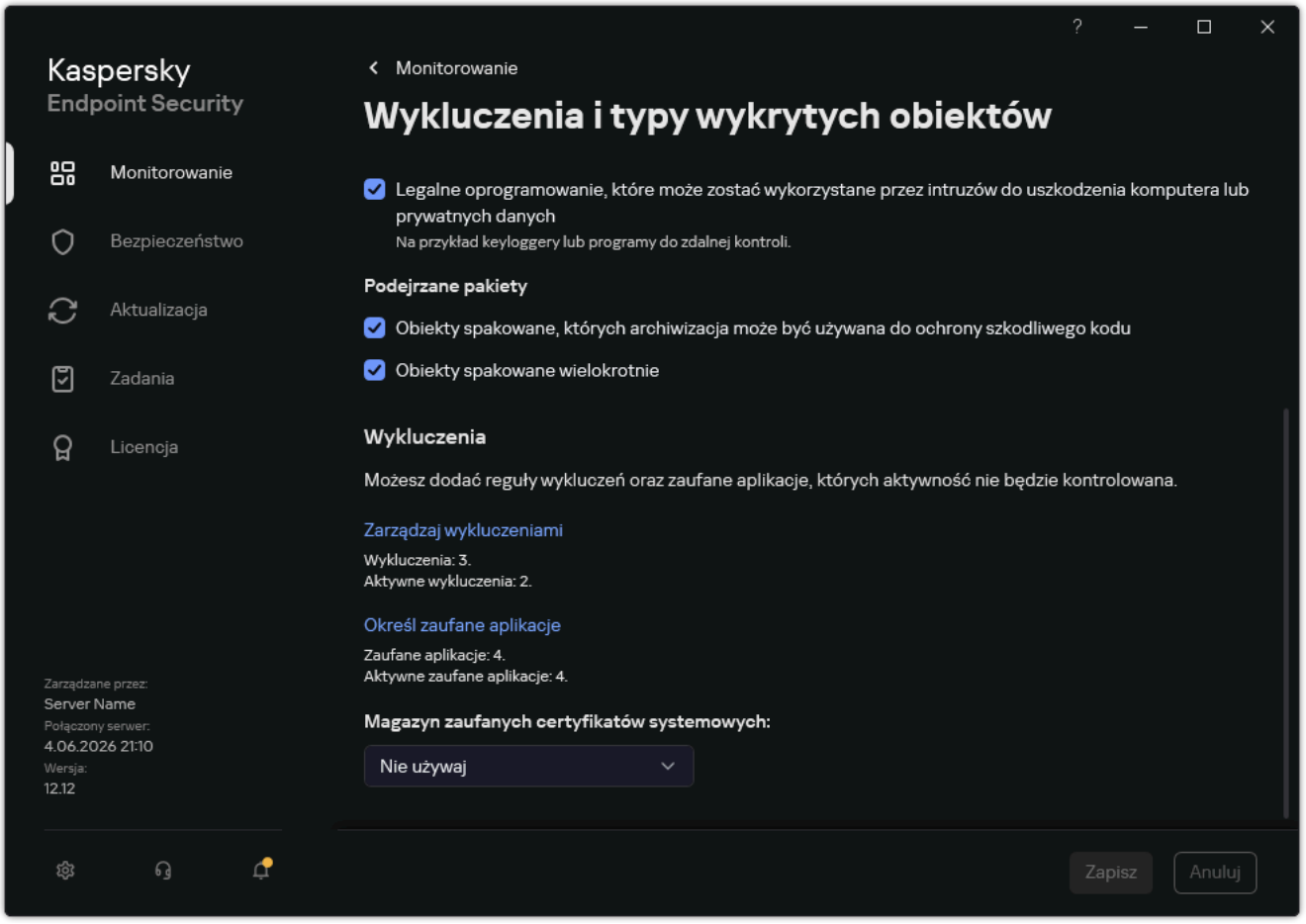
    Nowa zaufana aplikacja zostanie dodana do listy. W każdej chwili można wyłączyć aplikację ze strefy zaufanej za pomocą pola wyboru znajdującego w kolumnie **Stan**.

12. Zapisz swoje zmiany.

Dodawanie aplikacji do listy zaufanych z poziomu interfejsu aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Wykluczenia i typy wykrytych obiektów**.
3. W sekcji **Wykluczenia** kliknij odnośnik **Określ zaufane aplikacje**.

Kaspersky Endpoint Security ukrywa skonsolidowaną listę zaufanych aplikacji w interfejsie użytkownika aplikacji, jeśli konfiguracja zaufanych aplikacji została zablokowana przez administratora w konsoli (symbol „zamkniętej kłódki"), a lokalne zaufane aplikacje są zabronione (pole wyboru **Zezwól na korzystanie z lokalnych zaufanych aplikacji** jest odznaczone).



Ustawienia wykluczeń

4. Kliknij **Dodaj** i wybierz działanie:

   - **Kategoria**. Możesz grupować zaufane aplikacje w ramach osobnych kategorii. Aby utworzyć nową kategorię, wprowadź nazwę kategorii i dodaj do niej przynajmniej jedną zaufaną aplikację.
   - **Nowe wykluczenie**. Kaspersky Endpoint Security dodaje nową zaufaną aplikację do katalogu głównego listy.
   - **Wybierz wykluczenie z listy**. Aby szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menadżerze konfiguracji System Center Configuration Manager, aplikacja zawiera *predefiniowane zaufane aplikacje*. Dodano także wstępnie zdefiniowane zaufane aplikacje, aby ułatwić konfigurowanie aplikacji w środowiskach wirtualnych Citrix i VMware. Musisz wybrać predefiniowane zaufane aplikacje w zależności od przeznaczenia chronionego serwera.

   Aby dodać nową zaufaną aplikację do określonej kategorii, zaznacz pole wyboru znajdujące się obok tej kategorii i zaznacz opcję **Nowe wykluczenie**.

5. Wybierz kryteria zaufania:

   - **Użyj pełnej ścieżki procesu na dysku, aby uznać go za zaufany**. Wprowadź ścieżkę do pliku wykonywalnego zaufanej aplikacji.

     Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

Kaspersky Endpoint Security rozróżnia wielkość liter w nazwie pliku zaufanej aplikacji. Jeśli w nazwie pliku wpisana zostanie nieprawidłowa wielkość liter, Kaspersky Endpoint Security nie rozpozna zaufanej aplikacji.

- **Użyj skrótu pliku procesu, aby uznać go za zaufany**.

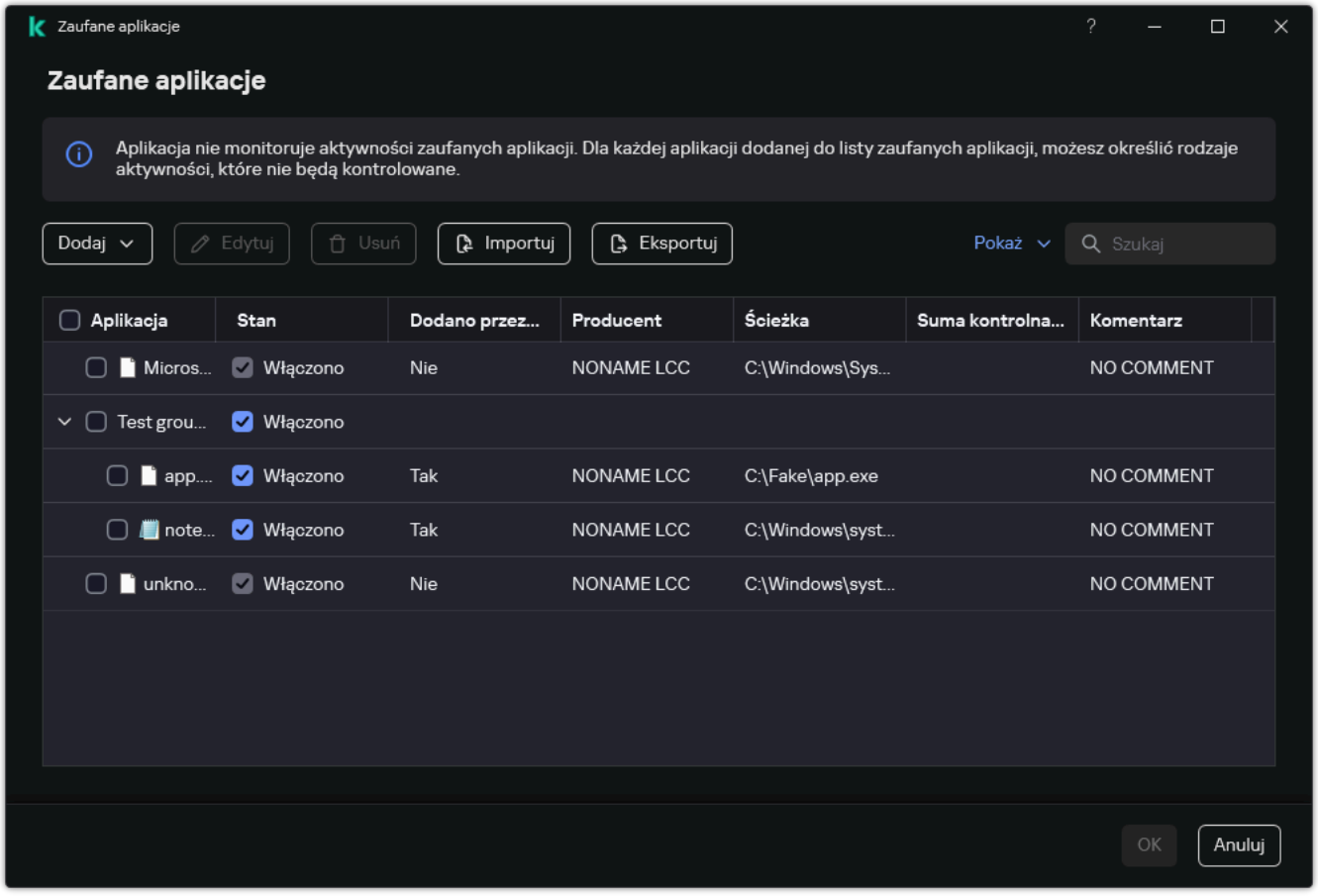
Kaspersky Endpoint Security obsługuje zmienne środowiskowe i konwertuje ścieżkę w lokalnym interfejsie aplikacji. Innymi słowy, jeśli wprowadzisz ścieżkę do pliku `%userprofile%\Documents\File.exe`, w lokalnym interfejsie aplikacji dla użytkownika Fred123 dodaj wpis `C:\Users\Fred123\Documents\File.exe`. Zgodnie z tym ustawieniem, program Kaspersky Endpoint Security ignoruje zaufany program `File.exe` dla innych użytkowników. Aby zastosować wpis do wszystkich kont użytkowników, możesz użyć znaku `*` (na przykład: `C:\Users\*\Documents\File.exe`). Za każdym razem, gdy dodajesz nową zmienną środowiskową, musisz uruchomić aplikację ponownie.

6. W oknie właściwości zaufanej aplikacji skonfiguruj ustawienia zaawansowane.

7. Kliknij **OK**.

   Nowa zaufana aplikacja zostanie dodana do listy. W każdej chwili można wyłączyć aplikację ze strefy zaufanej za pomocą pola wyboru znajdującego w kolumnie **Stan**.

8. Zapisz swoje zmiany.



Lista zaufanych aplikacji

Parametr	Opis
Nie skanuj plików otwieranych przez aplikację	Wszystkie pliki, które są otwierane przez aplikację, zostają wykluczone ze skanowania wykonywanego przez program Kaspersky Endpoint Security. Na przykład, jeśli używasz aplikacji do tworzenia kopii zapasowej plików, ta funkcja pomaga w zmniejszeniu zużycia zasobów przez Kaspersky Endpoint Security.
Nie monitoruj aktywności aplikacji	Kaspersky Endpoint Security nie będzie monitorował aktywności sieciowej i plikowej aplikacji w systemie operacyjnym. Możesz skonfigurować monitorowanie aktywności aplikacji dla różnych komponentów Kaspersky Endpoint Security: • **Nie monitoruj komponentów zabezpieczeń i kontroli**. Aktywność aplikacji jest monitorowana przez następujące komponentów: Wykrywanie zachowań, Ochrona przed exploitami, Ochrona przed włamaniami, Silnik korygujący i Zapora sieciowa. • **Nie monitoruj Managed Detection and Response oraz Endpoint Detection and Response**. Aktywność aplikacji jest monitorowana przez wbudowanego agenta MDR I wbudowanego agenta EDR (KATA). • **Nie przechwytuj interaktywnych danych wejściowych konsoli dla Endpoint Detection and Response**. Kaspersky Endpoint Security nie wysyła danych telemetrycznych dotyczących zarządzania aplikacją na konsoli. Dane telemetryczne są używane przez Kaspersky Anti Targeted Attack Platform (EDR).
Nie monitoruj aktywności aplikacji potomnych	Kaspersky Endpoint Security nie będzie monitorował aktywności plikowej i sieciowej aplikacji, które są uruchamiane przez tę aplikację. Możesz zastosować wykluczenie cyklicznie. Aby aplikacja nie monitorowała aktywności całego łańcucha aplikacji podrzędnych.
Nie dziedzicz ograniczeń nadrzędnego procesu (aplikacji)	Ograniczenia skonfigurowane dla procesu nadrzędnego nie będą stosowane przez program Kaspersky Endpoint Security do procesu podrzędnego. Proces nadrzędny jest uruchamiany przez aplikację, dla której skonfigurowano uprawnienia aplikacji (Ochrona przed włamaniami) i reguły sieciowe dla aplikacji (Zapora sieciowa).
Nie monitoruj aktywności aplikacji potomnych	Kaspersky Endpoint Security nie będzie monitorował aktywności plikowej i sieciowej aplikacji, które są uruchamiane przez tę aplikację. Możesz zastosować wykluczenie cyklicznie. Aby aplikacja nie monitorowała aktywności całego łańcucha aplikacji podrzędnych.
Zezwól na interakcję z interfejsem aplikacji	Autoochrona Kaspersky Endpoint Security blokuje wszystkie próby zarządzania usługami aplikacji ze zdalnego komputera. Jeśli pole jest zaznaczone, aplikacja do zdalnej administracji może zarządzać ustawieniami Kaspersky Endpoint Security poprzez interfejs Kaspersky Endpoint Security.
Nie blokuj interakcji z modułem Ochrona AMSI	Kaspersky Endpoint Security nie będzie monitorował żądań zaufanej aplikacji dla obiektów skanowanych przez składnik Ochrona AMSI.
Nie skanuj ruchu sieciowego	Ruch sieciowy zainicjowany przez aplikację zostanie wykluczony ze skanowania wykonywanego przez Kaspersky Endpoint Security. Ze skanowania można wykluczyć cały ruch sieciowy lub tylko zaszyfrowany ruch sieciowy. Ze skanowania możesz także wykluczyć pojedyncze adresy IP i numery portów. Kaspersky Endpoint Security w wersji 14.0 lub wcześniejszej nie obsługuje wykluczania ruchu sieciowego, jeśli dla zaufanej aplikacji zamiast ścieżki określono skrót.
Nie przechwytuj modyfikacji plików *(dostępny tylko w Kaspersky Security Center Console)*	Kaspersky Endpoint Security nie monitoruje zmian w plikach z zakresu monitoringu Monitora integralności systemu. Aplikacja stosuje wykluczenie do wszystkich Monitora integralności systemu: Monitorowanie integralności systemu w czasie rzeczywistym i Sprawdzanie integralności systemu na żądanie.
Nie przechwytuj modyfikacji rejestru *(dostępny tylko w Kaspersky Security Center Console)*	Kaspersky Endpoint Security nie monitoruje zmian w kluczach rejestru z zakresu monitoringu Monitora integralności systemu. Aplikacja stosuje wykluczenie do wszystkich Monitora integralności systemu: Monitorowanie integralności systemu w czasie rzeczywistym i Sprawdzanie integralności systemu na żądanie.
Komentarz	Jeśli to konieczne, możesz wpisać krótki komentarz dla zaufanej aplikacji. Komentarze pomagają uprościć wyszukiwanie i sortowanie zaufanych aplikacji.
Stan	Stan zaufanej aplikacji: • Stan **Aktywny** oznacza, że aplikacja znajduje się w strefie zaufanej. • Stan **Nieaktywny** oznacza, że aplikacja zostanie wykluczona ze strefy zaufanej.

Tworzenie lokalnej strefy zaufanej

Użytkownik może teraz stworzyć własną lokalnej strefę zaufaną dla określonego komputera. W ten sposób użytkownik mogą utworzyć swoje własne lokalne listy wykluczeń ze skanowania i zaufanych aplikacji jako dodatek do ogólnej strefy zaufanej w ramach stosowanych zasad. Administrator może zezwolić na lub zablokować użycie lokalnych wykluczeń lub lokalnych zaufanych aplikacji w ranach ustawień zasad. Aby to zrobić, użyj pól wyboru **Zezwól na korzystanie z lokalnych wykluczeń** oraz **Zezwól na korzystanie z lokalnych zaufanych aplikacji** w sekcji **Wykluczenia** zasad.

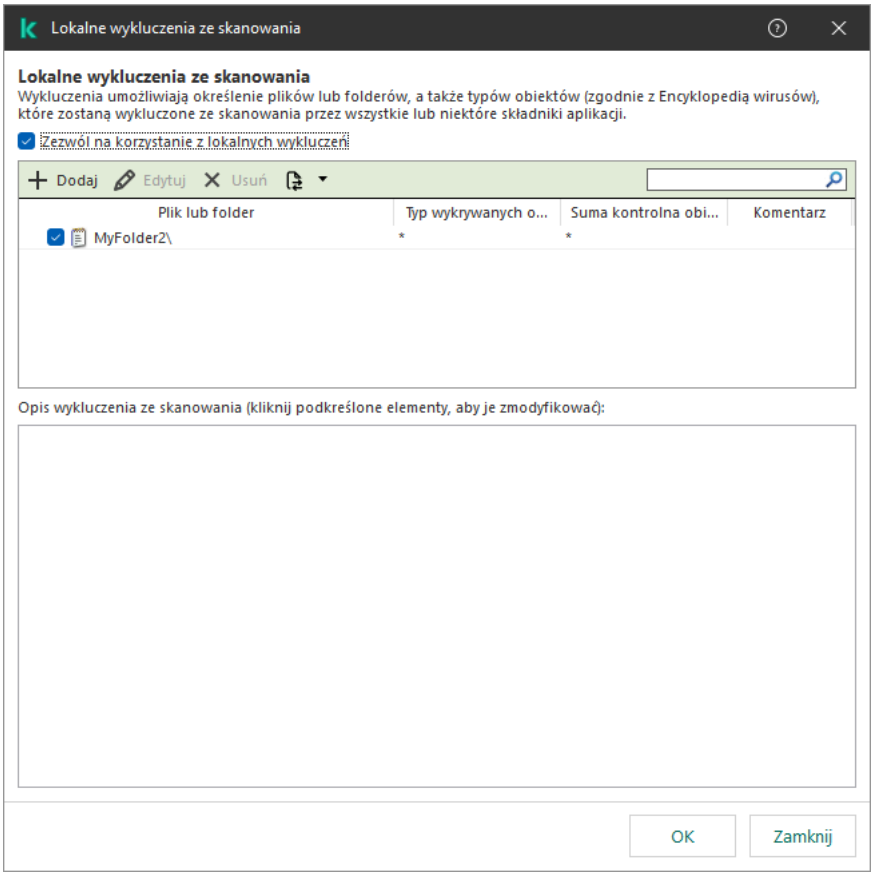
Jeśli administrator zezwolił na utworzenie lokalnej strefy zaufanej, użytkownik może dodać własne wykluczenia ze skanowania I zaufane aplikacje w interfejsie użytkownika aplikacji. Jednocześnie użytkownik nie ma uprawnień do modyfikowania lub usuwania obiektów ze skonfigurowanej w zasadach strefy zaufanej. Administrator może także przeglądać, dodawać, modyfikować lub usuwać pozycje listy w konsoli Kaspersky Security Center, jeśli konieczne jest dodanie wykluczeń dla konkretnego komputera.

Kaspersky Endpoint Security ukrywa listy wykluczeń ze skanowania i zaufanych aplikacji w interfejsie użytkownika aplikacji, jeśli konfiguracja strefy zaufanej została zablokowana przez administratora w konsoli (symbol „zamkniętej kłódki"), a lokalne wykluczenia ze skanowania i zaufane aplikacje są zabronione.

Dodawanie obiektów do lokalnej strefy zaufanej w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Kliknij dwukrotnie komputer, aby otworzyć okno właściwości komputera.
5. W oknie ustawień komputera wybierz sekcję **Aplikacje**.
6. Na liście aplikacji Kaspersky zainstalowanych na komputerze wybierz **Kaspersky Endpoint Security for Windows (14.1)** i kliknij ją dwukrotnie, aby otworzyć właściwości aplikacji.
7. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Wykluczenia i typy obiektów**.
8. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** → **Lokalne wykluczenia ze skanowania** kliknij przycisk **Ustawienia**.

Funkcja ta pozwala otworzyć okno zawierające listę wykluczeń.



Ustawienia strefy zaufanej

9. Utwórz listę wykluczeń na podstawie skanowania lokalnego.

   Zasady tworzenia wykluczeń ze skanowania lokalnego są takie same jak w przypadku wykluczeń ogólnych. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki * i ?.

10. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** → **Lokalne zaufane aplikacje** kliknij przycisk **Ustawienia**.

    Zostanie otwarte okno zawierające listę lokalnych zaufanych aplikacji.

11. Utwórz listę lokalnych zaufanych aplikacji.

    Zasady dodawania aplikacji do listy lokalnych zaufanych aplikacji są takie same jak w przypadku zasad dodawania ich do listy ogólnej. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki * i ?.

12. Zapisz swoje zmiany.

Jak dodać obiekt do listy strefy zaufanej w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Kliknij nazwę komputera, na którym chcesz zezwolić użytkownikowi na wykonywanie zablokowanego działania.
3. Wybierz zakładkę **Aplikacje**.
4. Kliknij **Kaspersky Endpoint Security for Windows**.

   Spowoduje to otwarcie lokalnych ustawień aplikacji.

5. Wybierz zakładkę **Ustawienia aplikacji**.

6. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Wykluczenia i typy wykrytych obiektów**.

7. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** kliknij odnośnik **Lokalne wykluczenia ze skanowania**.

8. Utwórz listę wykluczeń na podstawie skanowania lokalnego.

   Zasady tworzenia wykluczeń lokalnych są takie same jak w przypadku zasady tworzenia wyłączeń ogólnych. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

9. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** kliknij odnośnik **Lokalne zaufane aplikacje**.

10. Utwórz listę lokalnych zaufanych aplikacji.

    Zasady dodawania aplikacji do listy lokalnych zaufanych aplikacji są takie same jak w przypadku zasad dodawania ich do listy ogólnej. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

11. Zapisz swoje zmiany.

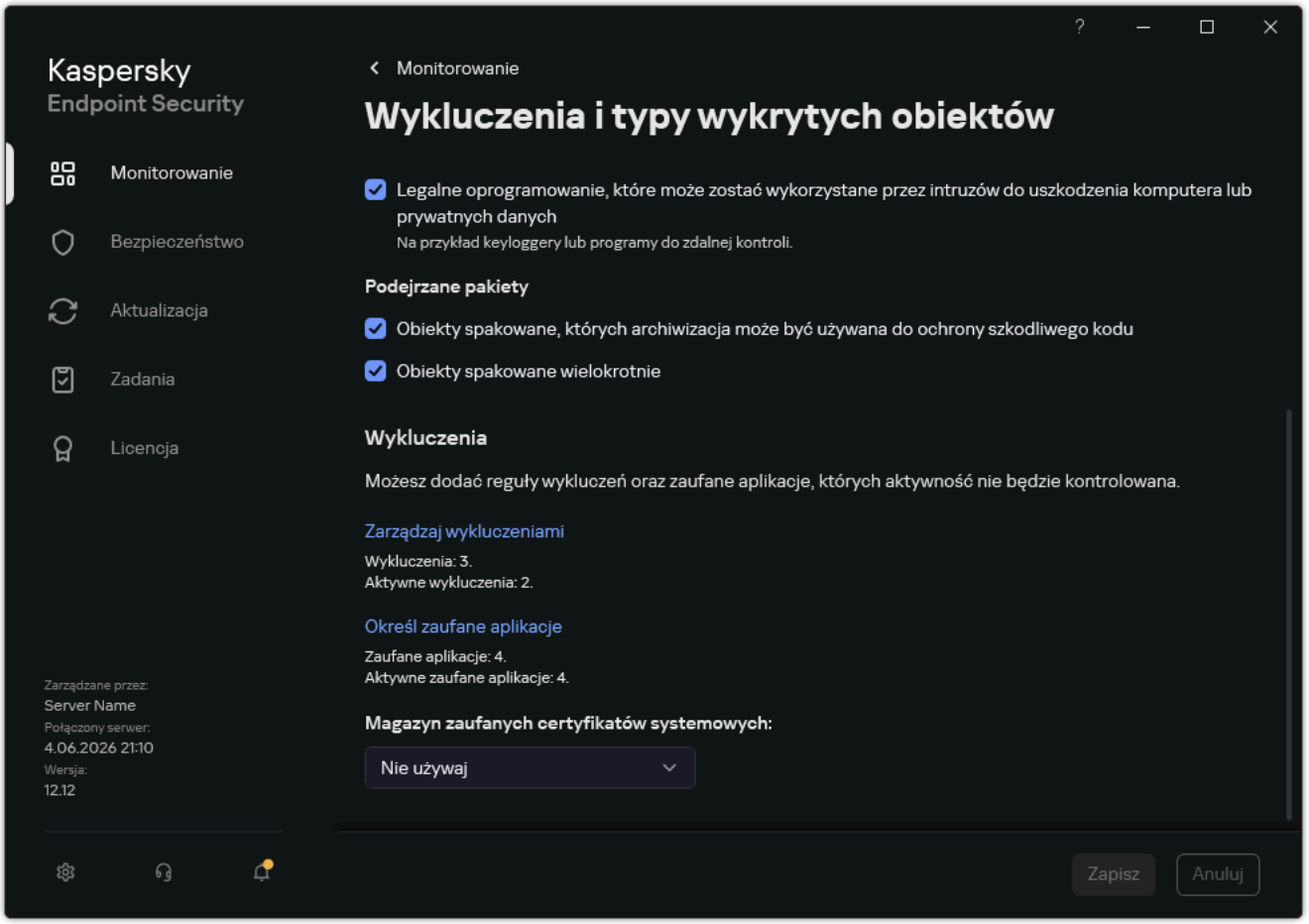
Jak utworzyć wykluczenie ze skanowania lokalnego w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Wykluczenia i typy wykrytych obiektów**.

3. W sekcji **Wykluczenia** kliknij odnośnik **Zarządzaj wykluczeniami**.

Kaspersky Endpoint Security ukrywa listę wykluczeń ze skanowania w interfejsie użytkownika aplikacji, jeśli konfiguracja wykluczeń ze skanowania została zablokowana przez administratora w konsoli (symbol „zamkniętej kłódki"), a wykluczenia ze skanowania lokalnego są zabronione (pole wyboru **Zezwól na korzystanie z lokalnych wykluczeń** jest odznaczone).



Ustawienia wykluczeń

4. Kliknij **Dodaj** i wybierz działanie:

   - **Kategoria**. Możesz grupować wykluczenia ze skanowania w ramach osobnych kategorii. Aby utworzyć nową kategorię, wprowadź nazwę kategorii i dodaj do niej co najmniej jedno wykluczenie ze skanowania.
   - **Nowe wykluczenie**. Kaspersky Endpoint Security dodaje nowe wykluczenie ze skanowania do katalogu głównego listy.
   - **Wybierz wykluczenie z listy**. Aby szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w System Center Configuration Manager, aplikacja zawiera *predefiniowane wykluczenia skanowania*. Dodano także predefiniowane wykluczenia ze skanowania, aby ułatwić konfigurowanie aplikacji w środowiskach wirtualnych Citrix i Vmware. Musisz wybrać predefiniowane wykluczenia ze skanowania w zależności od przeznaczenia chronionego serwera.

   Aby dodać nowe wykluczenie ze skanowania do określonej kategorii, zaznacz pole wyboru znajdujące się obok tej kategorii i zaznacz opcję **Nowe wykluczenie**.

5. Jeśli chcesz wykluczyć plik lub folder ze skanowania, wybierz plik lub folder, klikając przycisk **Przeglądaj**.

Możesz także wprowadzić ścieżkę ręczne. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`:

- Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.

- Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.

- Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

  Możesz użyć masek na początku, w środku lub na końcu ścieżki pliku. Na przykład, jeśli chcesz dodać do wykluczeń folder dla wszystkich użytkowników, należy wprowadzić maskę `?:\Users\*\Folder\`.

  Można wykluczyć foldery sieciowe. W tym celu należy ręcznie wprowadzić ścieżkę do folderu sieciowego (na przykład: `\\Network Share\*`).

6. Jeśli chcesz wykluczyć określony typ obiektu ze skanowania, w polu **Typy wykrywanych obiektów** wprowadź nazwę typu obiektu zgodnie z klasyfikacją Encyklopedii Kaspersky (na przykład: `Email-Worm`, `Rootkit` lub `RemoteAdmin`).

   Możesz użyć masek ze znakiem `?` (zastępuje dowolny pojedynczy znak) oraz znak `*` (zastępuje dowolną liczbę znaków). Na przykład, jeśli określona jest maska `Client*`, Kaspersky Endpoint Security wyklucza obiekty `Client-IRC`, `Client-P2P` i `Client-SMTP` ze skanowania.

7. Jeśli chcesz wykluczyć pojedynczy plik ze skanowania, wprowadź sumę kontrolną pliku w polu **Suma kontrolna obiektu**.

   Jeśli plik został zmodyfikowany, suma kontrolna pliku także zostanie zmodyfikowana. Jeśli taka sytuacja będzie miała miejsce, zmodyfikowany plik nie zostanie dodany do wykluczeń.

8. W sekcji **Składniki ochrony** wybierz komponenty, do których ma zostać zastosowane wykluczenie ze skanowania.

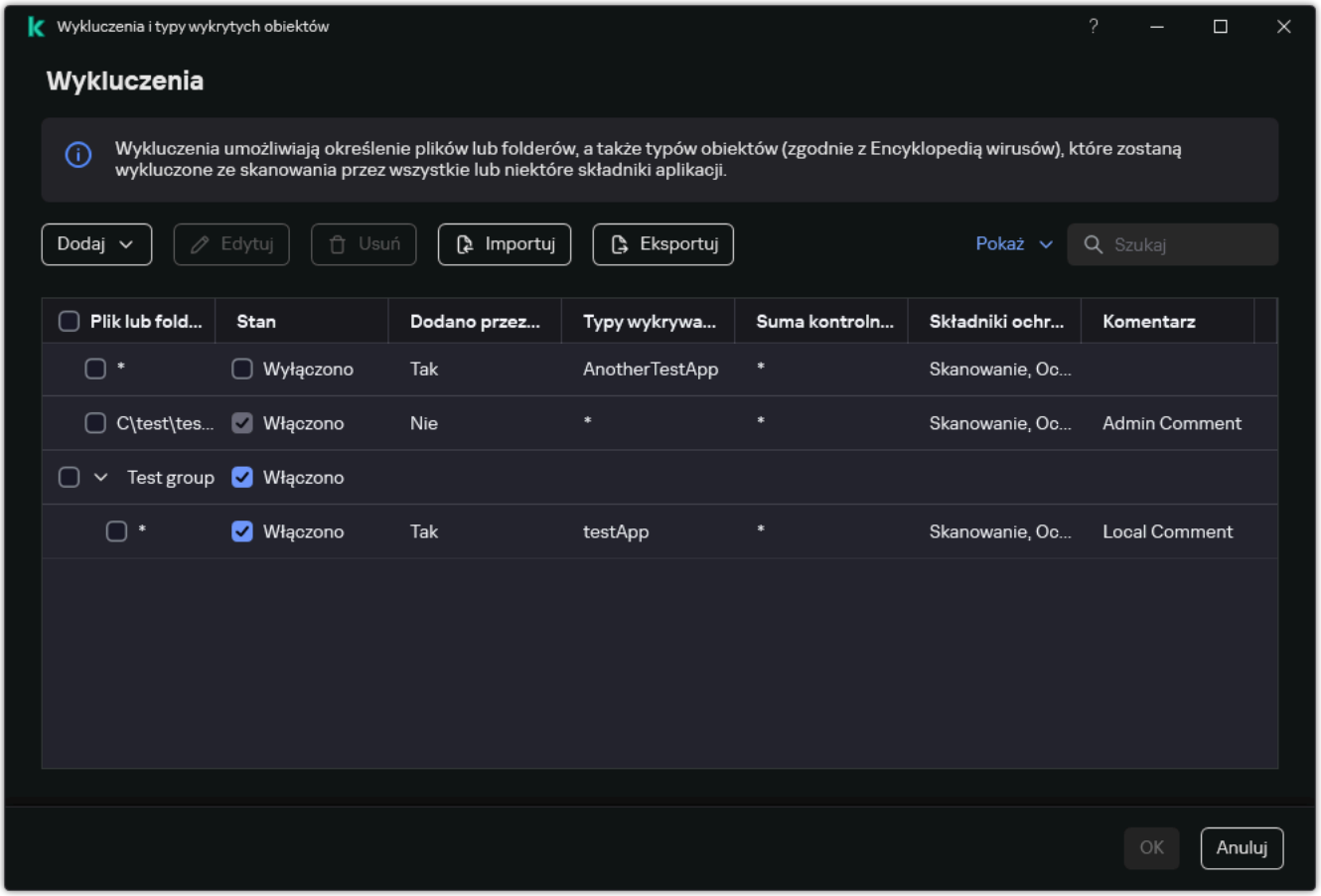
9. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

10. Dla wykluczenia wybierz stan **Aktywny**.

11. Kliknij **Dodaj**.

    Nowe wykluczenie zostanie dodane do listy. W każdej chwili można wyłączyć wykluczenie za pomocą pola wyboru znajdującego się w kolumnie **Stan**.

12. Zapisz swoje zmiany.

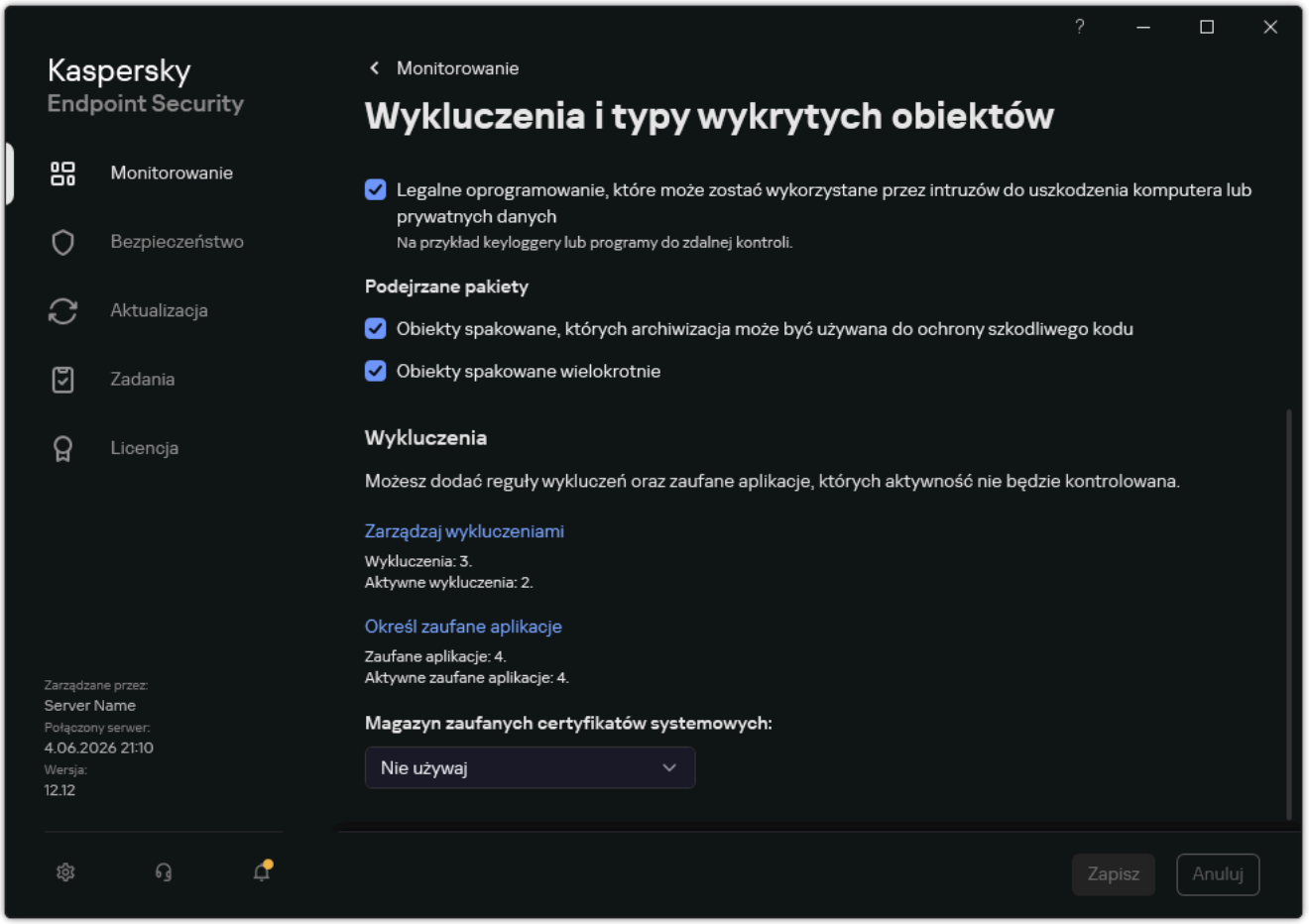


Lista wykluczeń

Dodawanie aplikacji do listy zaufanych aplikacji z poziomu interfejsu aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne → Wykluczenia i typy wykrytych obiektów**.
3. W sekcji **Wykluczenia** kliknij odnośnik **Określ zaufane aplikacje**.

Kaspersky Endpoint Security ukrywa skonsolidowaną listę zaufanych aplikacji w interfejsie użytkownika aplikacji, jeśli konfiguracja zaufanych aplikacji została zablokowana przez administratora w konsoli (symbol „zamkniętej kłódki"), a lokalne zaufane aplikacje są zabronione (pole wyboru **Zezwól na korzystanie z lokalnych zaufanych aplikacji** jest odznaczone).



Ustawienia wykluczeń

4. Kliknij **Dodaj** i wybierz działanie:

   - **Kategoria**. Możesz grupować zaufane aplikacje w ramach osobnych kategorii. Aby utworzyć nową kategorię, wprowadź nazwę kategorii i dodaj do niej przynajmniej jedną zaufaną aplikację.
   - **Nowe wykluczenie**. Kaspersky Endpoint Security dodaje nową zaufaną aplikację do katalogu głównego listy.
   - **Wybierz wykluczenie z listy**. Aby szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menadżerze konfiguracji System Center Configuration Manager, aplikacja zawiera *predefiniowane zaufane aplikacje*. Dodano także wstępnie zdefiniowane zaufane aplikacje, aby ułatwić konfigurowanie aplikacji w środowiskach wirtualnych Citrix i VMware. Musisz wybrać predefiniowane zaufane aplikacje w zależności od przeznaczenia chronionego serwera.

   Aby dodać nową zaufaną aplikację do określonej kategorii, zaznacz pole wyboru znajdujące się obok tej kategorii i zaznacz opcję **Nowe wykluczenie**.

5. Wybierz kryteria zaufania:

   - **Użyj pełnej ścieżki procesu na dysku, aby uznać go za zaufany**. Wprowadź ścieżkę do pliku wykonywalnego zaufanej aplikacji.

     Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

Kaspersky Endpoint Security rozróżnia wielkość liter w nazwie pliku zaufanej aplikacji. Jeśli w nazwie pliku wpisana zostanie nieprawidłowa wielkość liter, Kaspersky Endpoint Security nie rozpozna zaufanej aplikacji.

- **Użyj skrótu pliku procesu, aby uznać go za zaufany**.

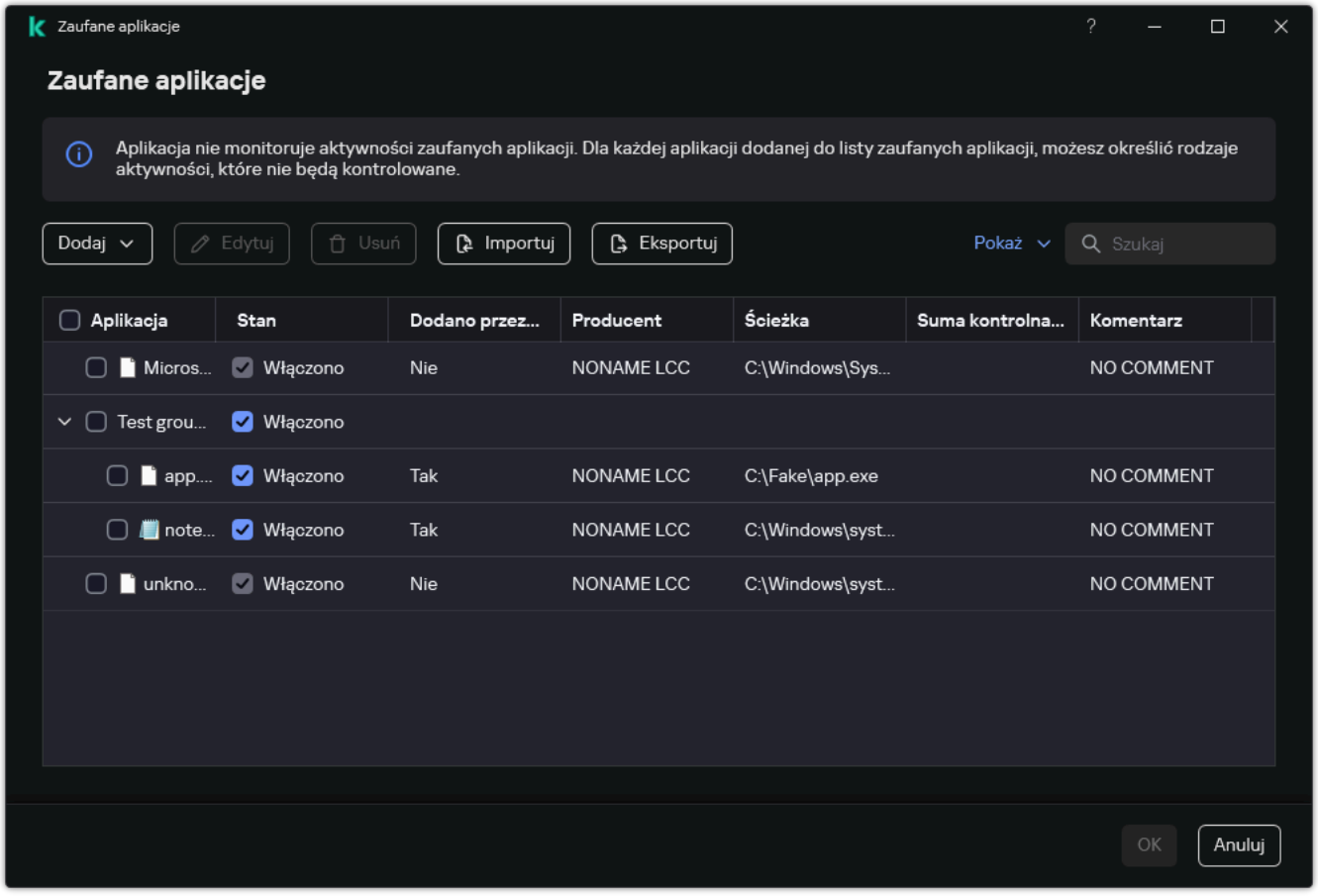
Kaspersky Endpoint Security obsługuje zmienne środowiskowe i konwertuje ścieżkę w lokalnym interfejsie aplikacji. Innymi słowy, jeśli wprowadzisz ścieżkę do pliku `%userprofile%\Documents\File.exe`, w lokalnym interfejsie aplikacji dla użytkownika Fred123 dodaj wpis `C:\Users\Fred123\Documents\File.exe`. Zgodnie z tym ustawieniem, program Kaspersky Endpoint Security ignoruje zaufany program `File.exe` dla innych użytkowników. Aby zastosować wpis do wszystkich kont użytkowników, możesz użyć znaku `*` (na przykład: `C:\Users\*\Documents\File.exe`). Za każdym razem, gdy dodajesz nową zmienną środowiskową, musisz uruchomić aplikację ponownie.

6. W oknie właściwości zaufanej aplikacji skonfiguruj ustawienia zaawansowane.

7. Kliknij **OK**.

   Nowa zaufana aplikacja zostanie dodana do listy. W każdej chwili można wyłączyć aplikację ze strefy zaufanej za pomocą pola wyboru znajdującego w kolumnie **Stan**.

8. Zapisz swoje zmiany.



Lista zaufanych aplikacji

Eksportowanie i importowanie zaufanych stref

Strefa zaufana jest utworzoną przez administratora listą obiektów i aplikacji, które nie są monitorowane przez Kaspersky Endpoint Security. Strefa zaufana składa się z następujących list: *wykluczenia ze skanowania* oraz *zaufane aplikacje*. Możesz eksportować te listy do plików XML i innych formatów. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę wykluczeń tego samego typu. Możesz także użyć funkcji eksportowania/importowania, aby wykonać kopię zapasową listy wykluczeń i listy zaufanych aplikacji lub przenieść listy na inny serwer.

Aplikacja wykorzystuje następujące formaty eksportu i importu *listy wykluczeń*:

- XML jest dostępny w Konsoli administracyjnej (MMC), Web Console i Cloud Console.
- DAT jest dostępny tylko do importu w Konsoli administracyjnej (MMC). Celem tego formatu jest zachowanie zgodności ze starszymi wersjami aplikacji. Możesz przekonwertować plik DAT na format XML w Konsoli administracyjnej (MMC), aby przeprowadzić migrację list wykluczeń do Web Console.
- CSV jest dostępny tylko w lokalnym interfejsie aplikacji.

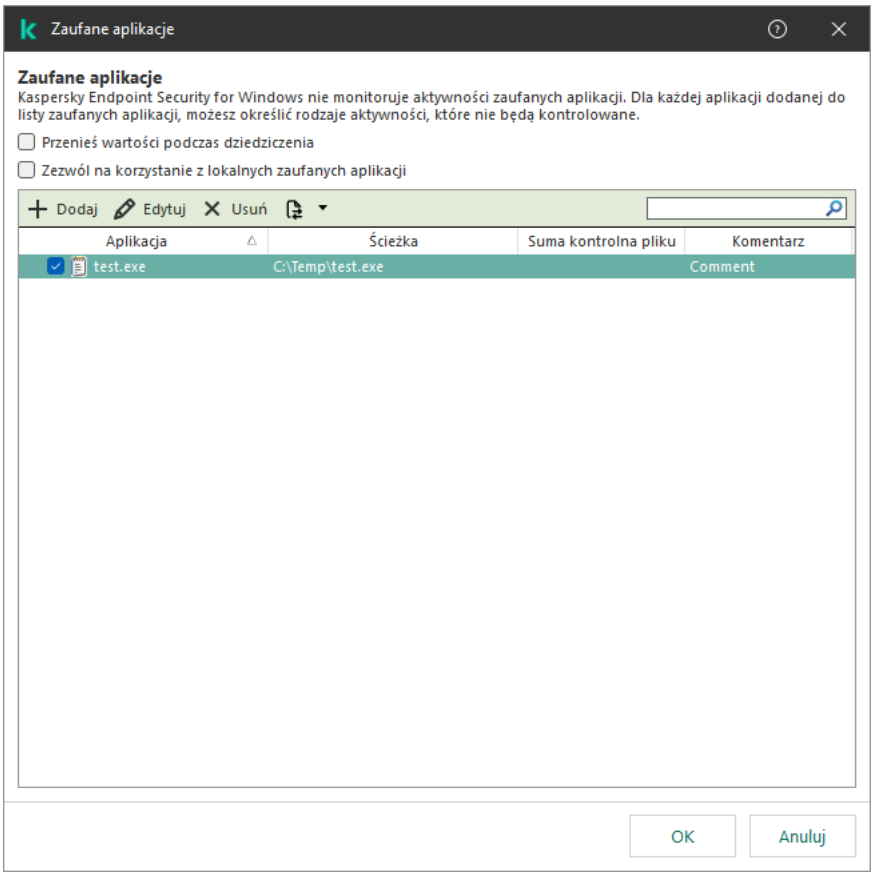
Kaspersky Endpoint Security używa formatu XML do eksportowania i importowania *listy zaufanych aplikacji*.

Eksportowanie i importowanie strefy zaufanej w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Wykluczenia i typy obiektów**.
4. W obszarze **Wykluczenia ze skanowania i aplikacje zaufane** wybierz składnik strefy zaufanej, który chcesz wyeksportować lub zaimportować: **Wykluczenia ze skanowania** lub **Zaufane aplikacje**.
5. Kliknij **Ustawienia**.
6. W celu wyeksportowania listy reguł:
   a. Wybierz wykluczenia, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
      Jeśli nie wybrałeś żadnego wykluczenia, Kaspersky Endpoint Security wyeksportuje wszystkie wykluczenia.
   b. Kliknij przycisk → **Eksportuj**.
   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.

d. Zapisz plik.

Kaspersky Endpoint Security eksportuje całą listę wykluczeń do pliku XML. Kaspersky Endpoint Security obsługuje również eksportowanie listy wykluczeń do pliku DAT.



Lista zaufanych aplikacji

7. W celu zaimportowania listy wykluczeń:

a. Kliknij przycisk → **Importuj**.

b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.

c. Otwórz plik.

Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML. Kaspersky Endpoint Security obsługuje również importowanie listy wykluczeń z pliku DAT.

8. Zapisz swoje zmiany.

Jak wyeksportować lub zaimportować strefę zaufaną w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Przejdź do sekcji **Strefa zaufana**.

5. W celu wyeksportowania listy reguł:

   a. Kliknij odnośnik **Wykluczenia ze skanowania w poszukiwaniu złośliwego oprogramowania**.

   b. Wybierz wykluczenia, które chcesz wyeksportować.

   c. Kliknij przycisk → **Eksportuj**.

      Kaspersky Endpoint Security eksportuje listę wykluczeń do pliku JSON w domyślnym folderze Pobrane.

6. W celu wyeksportowania listy zaufanych aplikacji:

   a. Wybierz zaufane aplikacje, które chcesz wyeksportować.

   b. Kliknij przycisk → **Eksportuj**.

      Kaspersky Endpoint Security eksportuje listę aplikacji zaufanych do pliku JSON w domyślnym folderze Pobrane.

7. W celu zaimportowania listy wykluczeń:

   a. Kliknij odnośnik **Wykluczenia ze skanowania w poszukiwaniu złośliwego oprogramowania**.

   b. Kliknij przycisk → **Importuj**.

      W oknie, które zostanie otwarte, wybierz plik JSON, z którego chcesz zaimportować listę wykluczeń.

   c. Otwórz plik.

      Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku JSON.

8. W celu zaimportowania listy zaufanych aplikacji:

   a. Kliknij odnośnik **Aplikacje**.

   b. Kliknij przycisk → **Importuj**.

      Spowoduje to otwarcie okna; w tym oknie wybierz plik JSON, z którego chcesz zaimportować listę zaufanych aplikacji.

   c. Otwórz plik.

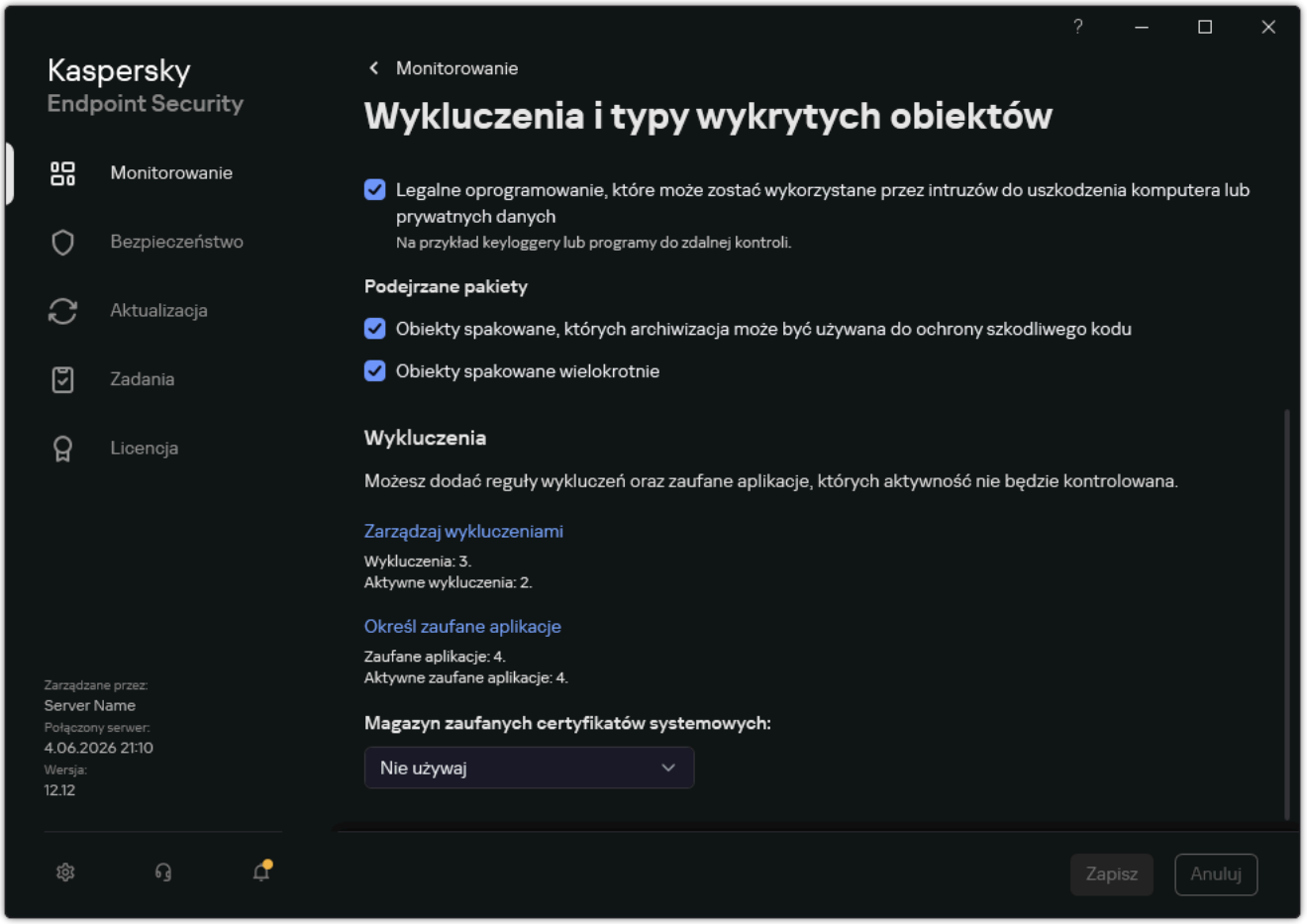
      Jeśli komputer ma już listę zaufanych aplikacji, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku JSON.

9. Zapisz swoje zmiany.

Jak wyeksportować lub zaimportować strefę zaufaną w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne → Wykluczenia i typy wykrytych obiektów**.



Ustawienia wykluczeń

3. W celu wyeksportowania listy reguł:

   a. W sekcji **Wykluczenia** kliknij odnośnik **Zarządzaj wykluczeniami**.

   b. Wybierz wykluczenia, które chcesz wyeksportować.

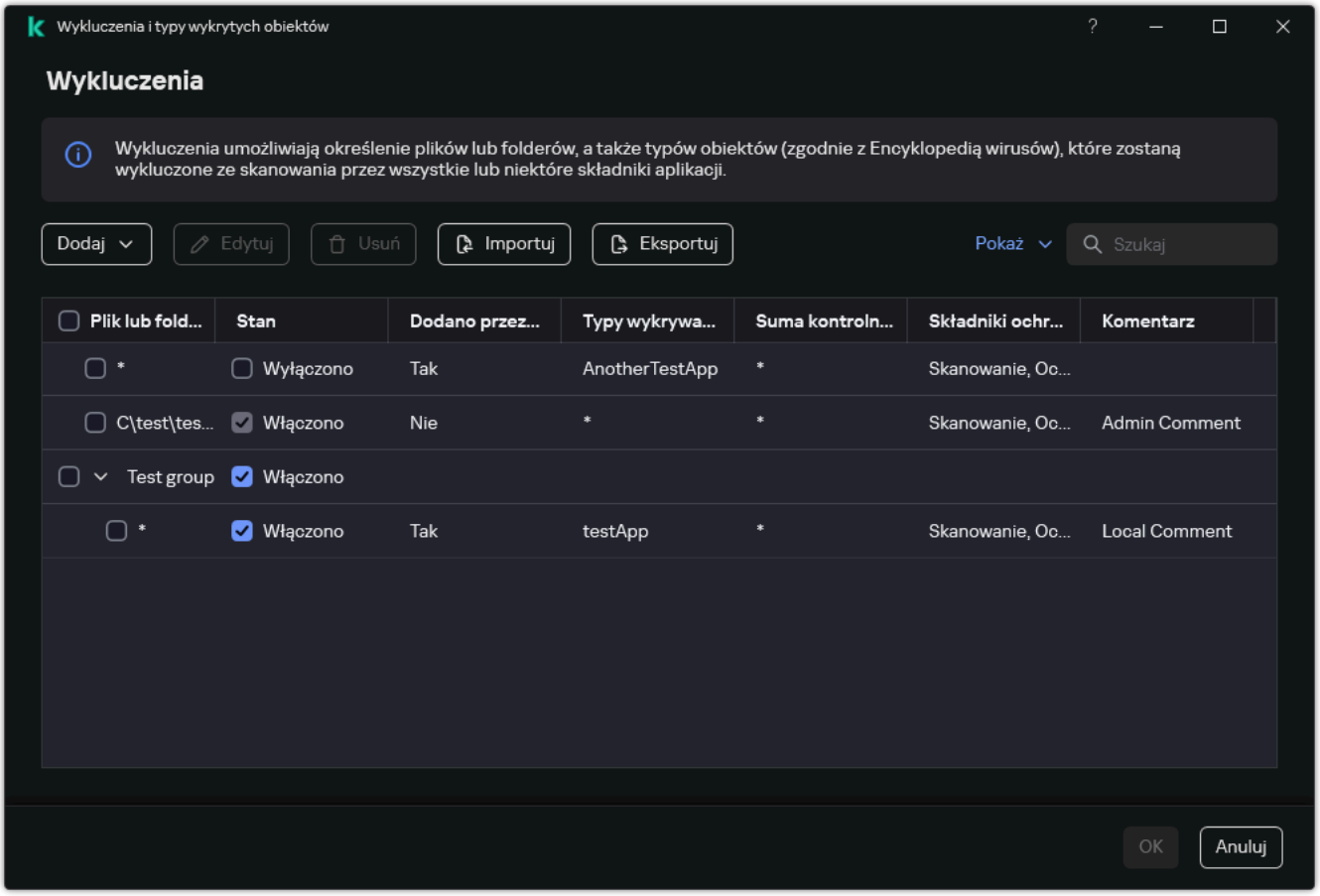
   c. Kliknij **Eksportuj**.

   d. Potwierdź chęć wyeksportowania tylko wybranych wykluczeń lub wyeksportuj całą listę wykluczeń.

   e. W otwartym oknie określ nazwę pliku CSV, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.

f. Zapisz plik.

Kaspersky Endpoint Security eksportuje całą listę wykluczeń do pliku CSV.



Lista wykluczeń

4. W celu wyeksportowania listy zaufanych aplikacji:

   a. W sekcji **Wykluczenia** kliknij odnośnik **Określ zaufane aplikacje**.

   b. Wybierz zaufane aplikacje, które chcesz wyeksportować.

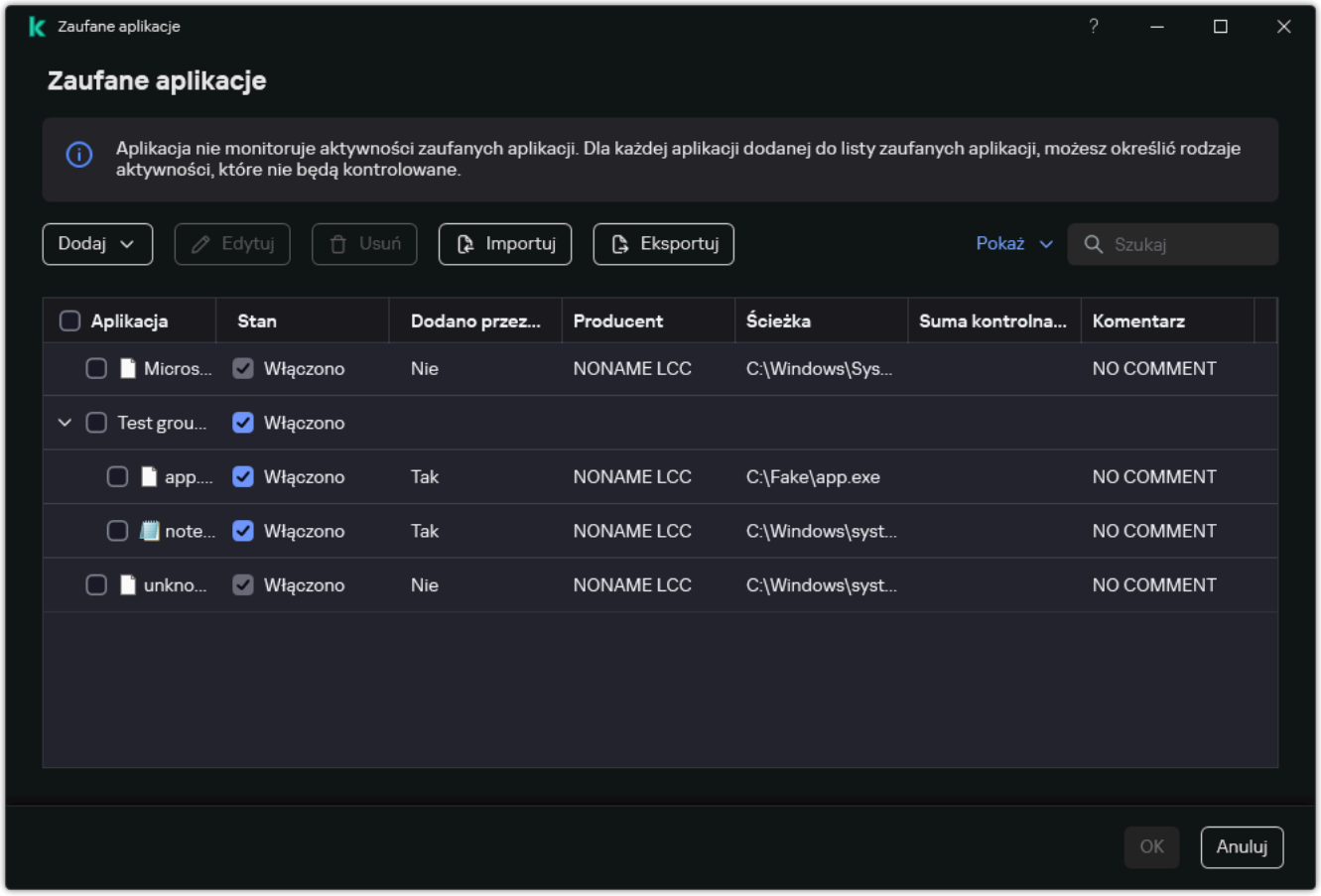
   c. Kliknij **Eksportuj**.

   d. Potwierdź chęć wyeksportowania tylko wybranych zaufanych aplikacji lub wyeksportuj całą listę.

   e. Spowoduje to otwarcie okna; w oknie tym wprowadź nazwę pliku XML, do którego chcesz wyeksportować listę zaufanych aplikacji oraz wybierz folder, w którym chcesz zapisać ten plik.

f. Zapisz plik.

Kaspersky Endpoint Security eksportuje całą listę zaufanych aplikacji do pliku XML.



Lista zaufanych aplikacji

5. W celu zaimportowania listy wykluczeń:

   a. W sekcji **Wykluczenia** kliknij odnośnik **Zarządzaj wykluczeniami**.

   b. Kliknij **Importuj**.

   c. W oknie, które zostanie otwarte, wybierz plik CSV, z którego chcesz zaimportować listę wykluczeń.

   d. Otwórz plik.

   Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku CSV.

6. W celu zaimportowania listy zaufanych aplikacji:

   a. W sekcji **Wykluczenia** kliknij odnośnik **Określ zaufane aplikacje**.

   b. Kliknij **Importuj**.

   c. Spowoduje to otwarcie okna; w tym oknie wybierz plik XML, z którego chcesz zaimportować listę zaufanych aplikacji.

d. Otwórz plik.

Jeśli komputer ma już listę zaufanych aplikacji, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

7. Zapisz swoje zmiany.

Obsługa aplikacji z zaufanym podpisem cyfrowym

Korzystanie z magazynu zaufanych certyfikatów systemowych umożliwia wykluczenie aplikacji posiadających zaufany podpis cyfrowy ze skanowań antywirusowych. Kaspersky Endpoint Security automatycznie przypisze takie aplikacje do grupy *Zaufane*.

Jak rozpocząć korzystanie z magazynu zaufanych certyfikatów systemowych w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Wykluczenia i typy obiektów**.
4. W sekcji **Magazyn zaufanych certyfikatów systemowych** zaznacz pole **Użyj magazynu zaufanych certyfikatów systemowych**.
5. Z listy rozwijalnej wybierz, który magazyn systemowy ma być uznawany za zaufany przez Kaspersky Endpoint Security.
6. Zapisz swoje zmiany.

Jak rozpocząć korzystanie z magazynu zaufanych certyfikatów systemowych w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do sekcji **Strefa zaufana**.
5. W otwartym oknie kliknij odnośnik **Zaufane certyfikaty**.
6. W otwartym oknie zaznacz pole **Użyj magazynu zaufanych certyfikatów systemowych**.
7. Wybierz, który magazyn systemowy ma być uważany za zaufany przez Kaspersky Endpoint Security.
8. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak rozpocząć korzystanie z magazynu zaufanych certyfikatów systemowych w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Wykluczenia i typy wykrytych obiektów**.

3. Z listy rozwijalnej **Magazyn zaufanych certyfikatów systemowych** wybierz, który magazyn systemowy ma być uznawany za zaufany przez Kaspersky Endpoint Security.

4. Zapisz swoje zmiany.

Dodatek. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje

Począwszy od Kaspersky Endpoint Security 12.6 for Windows, wykluczenia skanowania I zaufane aplikacje są dodawane do strefy zaufanej. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach. Począwszy od Kaspersky Endpoint Security 12.8 for Windows można instalować aplikację w trybie Light Agent w celu ochrony środowisk wirtualnych. Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje mogą pomóc w szybkiej konfiguracji Kaspersky Endpoint Security w środowiskach wirtualnych Citrix i VMware.

Predefiniowane wykluczenia i zaufane aplikacje możesz wybrać w następujący sposób:

- Instalowanie aplikacji.
  - Instalowanie aplikacji lokalnie przy użyciu kreatora
  - Właściwości pakietu instalacyjnego
- Ustawianie zasad.
  - Kreator nowej zasady
  - Właściwości zasady: wykluczenia ze skanowania i zaufane aplikacje

Serwer SQL

Podczas instalowania Kaspersky Endpoint Security na serwerze SQL należy utworzyć strefę zaufaną z predefiniowanych wykluczeń i zaufanych aplikacji, aby mieć pewność, że praca serwera nie zostanie zakłócona.

Predefiniowane wykluczenia ze skanowania

Ścieżka	Wersja SQL
`%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA\*.mdf`	2012 2014 2016 2017 2019 2022
`%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?\*\Data\*.mdf`	2012
`%ProgramFiles%\Microsoft SQL Server\MSSQL.?\*\Data\*.mdf`	2012

Ścieżka	Wersja SQL
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Serwer Microsoft Exchange

Podczas instalowania Kaspersky Endpoint Security na serwerze Microsoft Exchange należy utworzyć strefę zaufaną z predefiniowanych wykluczeń i zaufanych aplikacji, aby mieć pewność, że praca serwera nie zostanie zakłócona.

Predefiniowane wykluczenia ze skanowania

Ścieżka	Wersja Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019

Ścieżka	Wersja Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

Predefiniowane zaufane aplikacje

Ścieżka	Wersja Microsoft Exchange
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

System Center Configuration Manager

Predefiniowane wykluczenia ze skanowania

Ścieżka	Wersja programu System Center Configuration Manager
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Podczas instalowania Kaspersky Endpoint Security w środowisku wirtualnym Citrix należy utworzyć strefę zaufaną z predefiniowanych wykluczeń i zaufanych aplikacji, aby mieć pewność, że praca serwera nie zostanie zakłócona.

Predefiniowane wykluczenia ze skanowania

Ścieżka
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys

Ścieżka
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

Predefiniowane zaufane aplikacje

Ścieżka	Rozwiązanie Citrix
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Aplikacje i pulpity wirtualne

Ścieżka	Rozwiązanie Citrix
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Aplikacje i pulpity wirtualne
%SystemRoot%\System32\drivers\CVhdFilter.sys	Aplikacje i pulpity wirtualne
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Aplikacje i pulpity wirtualne
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Aplikacje i pulpity wirtualne
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Aplikacje i pulpity wirtualne
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Aplikacje i pulpity wirtualne
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Aplikacje i pulpity wirtualne
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Aplikacje i pulpity wirtualne
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Aplikacje i pulpity wirtualne
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Aplikacja Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Aplikacja Workspace

Ścieżka	Rozwiązanie Citrix
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Aplikacja Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Aplikacja Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Aplikacja Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Aplikacja Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Aplikacja Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Aplikacja Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Aplikacja Workspace
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Aplikacja Workspace
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Provisioning
%SystemRoot%\System32\drivers\bnistack6.sys	Provisioning
%SystemRoot%\System32\drivers\CfsDep2.sys	Provisioning
%SystemRoot%\System32\drivers\cnicteam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Provisioning
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

Podczas instalowania Kaspersky Endpoint Security w środowisku wirtualnym VMware należy utworzyć strefę zaufaną z predefiniowanych zaufanych aplikacji, aby mieć pewność, że praca serwera nie zostanie zakłócona.

Ścieżka	Rozwiązanie VMware
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon

Ścieżka	Rozwiązanie VMware
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

Zarządzanie Kopią zapasową

Kopia zapasowa przechowuje zapasowe kopie plików, które zostały usunięte lub zmodyfikowane podczas leczenia. *Kopia zapasowa* to kopia pliku utworzona przed wyleczeniem lub usunięciem pliku. Kopie zapasowe plików są przechowywane w specjalnym formacie i nie stanowią zagrożenia.

Kopie zapasowe plików są przechowywane w folderze `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

Użytkownicy należący do grupy Administratorzy mają nadane pełne uprawnienie dostępu do tego folderu. Ograniczone uprawnienia dostępu do tego folderu są nadawane użytkownikom, których konto zostało użyte do zainstalowania Kaspersky Endpoint Security.

Kaspersky Endpoint Security nie oferuje możliwości skonfigurowania uprawnień dostępu użytkownika do kopii zapasowych plików.

Czasami niemożliwe jest zachowanie integralności plików w trakcie leczenia. W przypadku częściowej lub całkowitej utraty dostępu do istotnych informacji wyleczonego pliku, można spróbować przywrócić plik z jego kopii zapasowej do jego oryginalnego folderu.

Jeśli Kaspersky Endpoint Security działa pod kontrolą Kaspersky Security Center, kopie zapasowe plików mogą być przesyłane do Serwera administracyjnego Kaspersky Security Center. Aby uzyskać więcej informacji na temat zarządzania kopiami zapasowymi plików w Kaspersky Security Center, zapoznaj się z systemem pomocy Kaspersky Security Center.

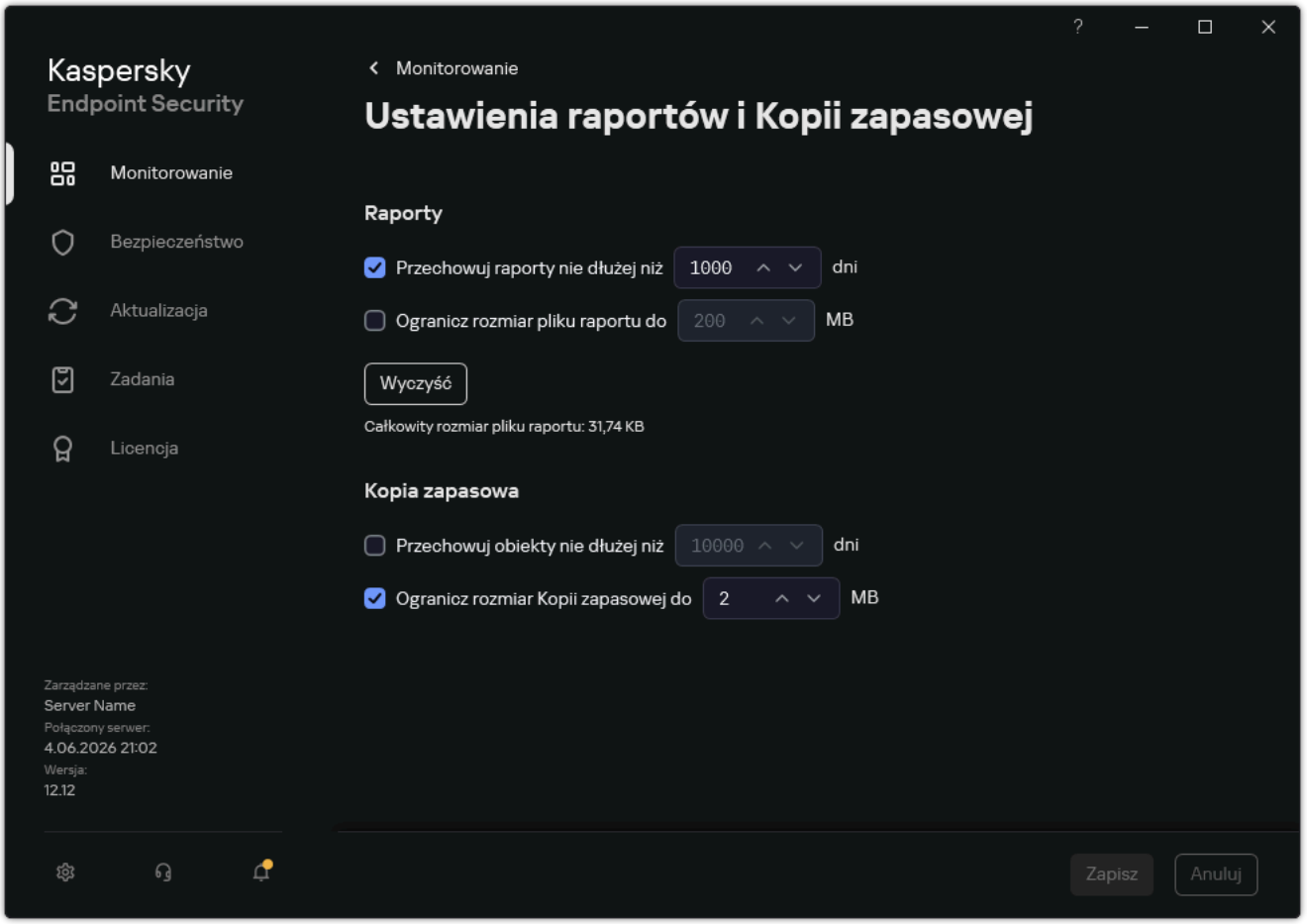
Konfigurowanie maksymalnego okresu przechowywania plików w Kopii zapasowej

Domyślnie maksymalny czas przechowywania kopii plików w Kopii zapasowej wynosi 30 dni. Po minięciu zdefiniowanego czasu, Kaspersky Endpoint Security usunie najstarsze pliki z Kopii zapasowej.

W celu skonfigurowania maksymalnego okresu przechowywania plików w Kopii zapasowej:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji kliknij kafelek **Raporty i Kopia zapasowa** w obszarze **Ustawienia ogólne**.



Ustawienia kopii zapasowej

3. Jeśli chcesz ograniczyć czas przechowywania kopii plików w Kopii zapasowej, w sekcji **Kopia zapasowa** zaznacz pole **Przechowuj obiekty nie dłużej niż N dni**. Wprowadź maksymalny czas przechowywania kopii plików w Kopii zapasowej.

4. Zapisz swoje zmiany.

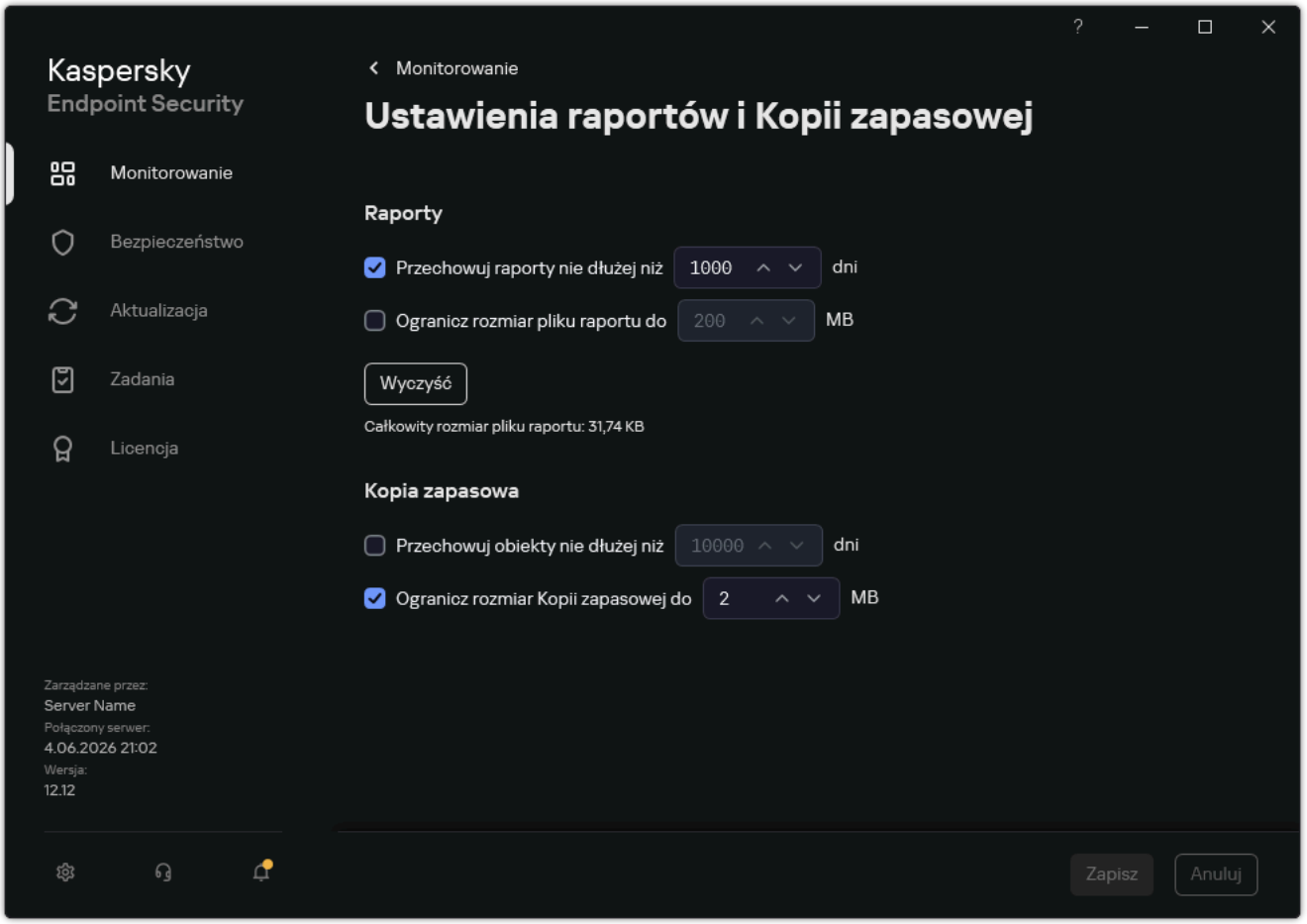
Konfigurowanie maksymalnego rozmiaru Kopii zapasowej

Możesz określić maksymalny rozmiar Kopii zapasowej. Domyślnie rozmiar Kopii zapasowej jest nieograniczony. Jeśli maksymalny rozmiar zostanie osiągnięty, Kaspersky Endpoint Security automatycznie usunie najstarsze pliki z Kopii zapasowej.

W celu skonfigurowania maksymalnego rozmiaru Kopii zapasowej:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji kliknij kafelek **Raporty i Kopia zapasowa** w obszarze **Ustawienia ogólne**.



Ustawienia kopii zapasowej

3. W sekcji **Kopia zapasowa** zaznacz pole **Ogranicz rozmiar Kopii zapasowej do N MB**. Jeśli pole jest zaznaczone, maksymalny rozmiar magazynu jest ograniczony do zdefiniowanej wartości. Domyślnie wynosi on 1024 MB. Aby uniknąć przekroczenia maksymalnego rozmiaru magazynu, Kaspersky Endpoint Security automatycznie usuwa najstarsze piki z magazynu po osiągnięciu maksymalnego rozmiaru magazynu.

4. Zapisz swoje zmiany.

Przywracanie plików z Kopii zapasowej

Jeżeli w pliku zostanie wykryty szkodliwy kod, Kaspersky Endpoint Security zablokuje plik, przypisze do niego stan *Niewyleczony*, umieści jego kopię w folderze Kopii zapasowej i spróbuje go wyleczyć. Po pomyślnym wyleczeniu stan kopii zapasowej pliku zmieni się na *Wyleczony*. Plik stanie się dostępny w oryginalnym folderze. Jeśli plik nie może zostać wyleczony, Kaspersky Endpoint Security usunie go z jego oryginalnego folderu. Możliwe jest przywrócenie pliku z jego kopii zapasowej do jego oryginalnego folderu.

Pliki ze stanem *Zostanie usunięty po ponownym uruchomieniu komputera* nie mogą zostać przywrócone. Uruchom komputer ponownie, a stan pliku zmieni się na *Wyleczony* lub *Usunięty*. Możliwe jest także przywrócenie pliku z jego kopii zapasowej do jego oryginalnego folderu.

Po wykryciu szkodliwego kodu w pliku aplikacji ze Sklepu Windows, Kaspersky Endpoint Security natychmiast usunie plik bez przenoszenia jego kopii do Kopii zapasowej. Możesz przywrócić integralność aplikacji ze Sklepu Windows, korzystając z odpowiednich narzędzi systemu operacyjnego (zobacz pliki pomocy dla Microsoft Windows, aby uzyskać szczegółowe informacje dotyczące przywracania aplikacji ze Sklepu Windows).

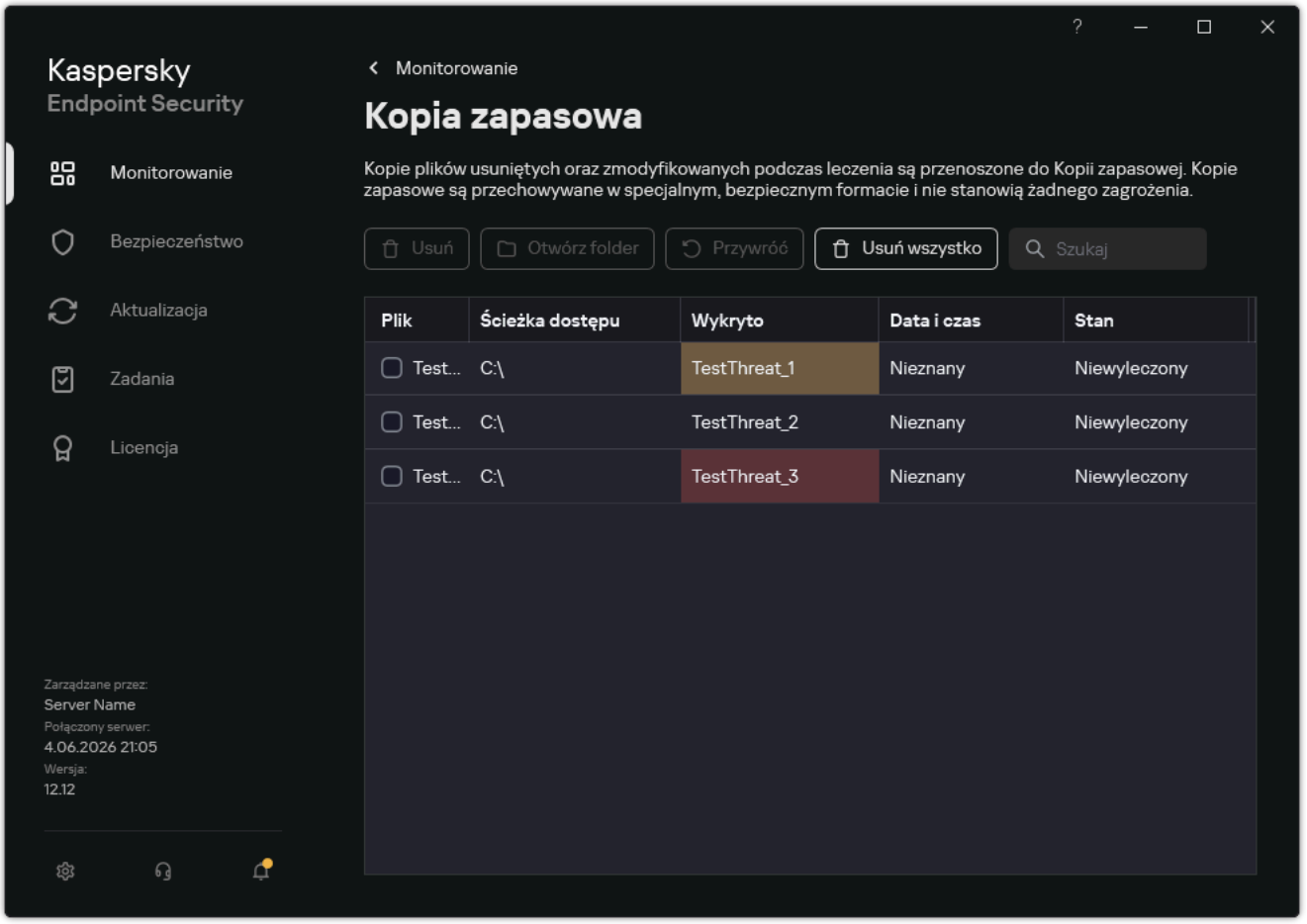
Zestaw kopii zapasowych plików jest przedstawiony w postaci tabeli. Dla kopii zapasowej pliku wyświetlana jest ścieżka dostępu do oryginalnego folderu pliku. Ścieżka do oryginalnego folderu pliku może zawierać dane osobowe.

Jeśli kilka plików o identycznych nazwach i różnej zawartości zostanie przeniesionych z tego samego folderu do folderu Kopii zapasowej, zostanie przywrócony tylko ten plik, który został ostatnio umieszczony w Kopii zapasowej.

W celu przywrócenia plików z Kopii zapasowej:

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Kopia zapasowa**.
2. To spowoduje otwarcie listy plików w Kopii zapasowej; na tej liście wybierz pliki, które chcesz przywrócić, i kliknij **Przywróć**.

   Kaspersky Endpoint Security przywróci wszystkie pliki z wybranych kopii zapasowych do ich oryginalnych folderów.



Kopia zapasowa

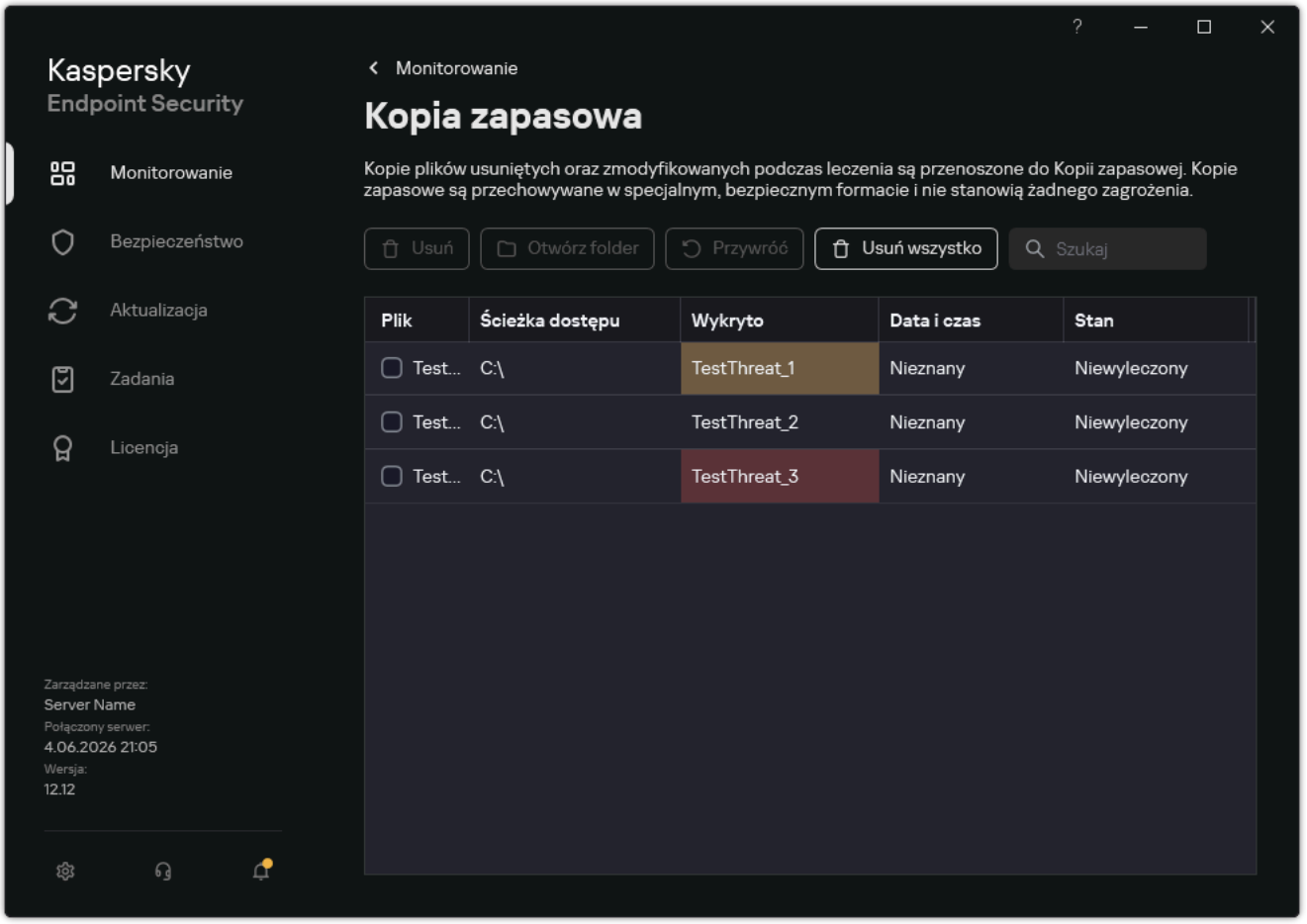
Usuwanie kopii zapasowych plików z Kopii zapasowej

Kaspersky Endpoint Security automatycznie usuwa kopie zapasowe plików posiadające dowolny stan z Kopii zapasowej po upłynięciu czasu przechowywania, zdefiniowanego w ustawieniach aplikacji. Możesz także ręcznie usunąć dowolną kopię pliku z folderu Kopii zapasowej.

W celu usunięcia kopii zapasowej pliku z Kopii zapasowej:

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Kopia zapasowa**.
2. To spowoduje otwarcie listy plików w Kopii zapasowej; na tej liście wybierz pliki, które chcesz usunąć z Kopii zapasowej, i kliknij **Usuń**.

Kaspersky Endpoint Security usunie wybrane kopie zapasowe plików z Kopii zapasowej.



Kopia zapasowa

Usługa powiadomień

Podczas działania programu Kaspersky Endpoint Security pojawiają się różnego rodzaju zdarzenia. Powiadomienia o tych zdarzeniach mogą być czysto informacyjne lub zawierać krytyczne informacje. Na przykład, powiadomienia mogą informować o pomyślnej aktualizacji baz danych i modułów aplikacji lub rejestracji błędów komponentów, które muszą być rozwiązane.

Kaspersky Endpoint Security obsługuje rejestrowanie informacji o zdarzeniach w dzienniku aplikacji Microsoft Windows i / lub raporcie zdarzeń Kaspersky Endpoint Security.

Kaspersky Endpoint Security dostarcza powiadomienia w jeden z następujących sposobów:

- Pod postacią komunikatów wyskakujących w obszarze powiadomień paska zadań Microsoft Windows;
- W wiadomości e-mail.

Możliwe jest skonfigurowanie dostarczania powiadomień o zdarzeniach. Metoda dostarczania powiadomień jest konfigurowana dla każdego typu zdarzenia.

Podczas korzystania z tabeli zdarzeń w celu skonfigurowania usługi powiadamiania można:

- Filtrować zdarzenia według wartości kolumny lub według warunków filtra niestandardowego.
- Użyć funkcji wyszukiwania zdarzeń usługi powiadamiania.
- Sortować zdarzenia usługi powiadamiania.
- Zmienić kolejność i zestaw kolumn wyświetlanych na liście zdarzeń usługi powiadamiania.

Konfigurowanie ustawień dziennika zdarzeń

W celu skonfigurowania ustawień dziennika zdarzeń:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Interfejs**.
3. W sekcji **Powiadomienia** kliknij przycisk **Skonfiguruj powiadomienia**.

   Moduły i zadania programu Kaspersky Endpoint Security są wyświetlane w lewej części okna. W prawej części okna wyświetlone są zdarzenia wygenerowane dla wybranego komponentu lub zadania.

   Zdarzenia mogą zawierać następujące dane użytkownika:

   - Ścieżki do plików przeskanowanych przez Kaspersky Endpoint Security.
   - Ścieżki do kluczy rejestru zmodyfikowane podczas działania Kaspersky Endpoint Security.
   - Nazwę użytkownika Microsoft Windows.
   - Adresy stron internetowych otwieranych przez użytkownika.

4. W lewej części okna wybierz komponent lub zadanie, dla którego chcesz skonfigurować ustawienia dziennika zdarzeń.

5. Zaznacz pola obok odpowiednich zdarzeń w kolumnach **Zapisz w raporcie lokalnym** i **Zapisz w dzienniku zdarzeń Windows**.

   Zdarzenia, dla których zaznaczono pola w kolumnie **Zapisz w raporcie lokalnym**, są wyświetlane w raportach aplikacji. Zdarzenia, dla których zaznaczono pola w kolumnie **Zapisz w dzienniku zdarzeń Windows**, są wyświetlane w Dziennikach systemu Windows, w kanale `Application`.

6. Zapisz swoje zmiany.

Konfigurowanie wyświetlania i dostarczania powiadomień

W celu skonfigurowania wyświetlania i dostarczania powiadomień:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Interfejs**.

3. W sekcji **Powiadomienia** kliknij przycisk **Skonfiguruj powiadomienia**.

   Moduły i zadania programu Kaspersky Endpoint Security są wyświetlane w lewej części okna. W prawej części okna wyświetlone są zdarzenia wygenerowane dla wybranego komponentu lub zadania.

   Zdarzenia mogą zawierać następujące dane użytkownika:

   - Ścieżki do plików przeskanowanych przez Kaspersky Endpoint Security.
   - Ścieżki do kluczy rejestru zmodyfikowane podczas działania Kaspersky Endpoint Security.
   - Nazwę użytkownika Microsoft Windows.
   - Adresy stron internetowych otwieranych przez użytkownika.

4. W lewej części okna wybierz komponent lub zadanie, dla którego chcesz skonfigurować dostarczanie powiadomień.

5. W kolumnie **Powiadom na ekranie** zaznacz pola obok żądanych zdarzeń.

   Informacje o wybranych zdarzeniach są wyświetlane w postaci wiadomości wyskakujących w obszarze powiadomień paska zadań Microsoft Windows.

6. W kolumnie **Powiadom na e-mail** zaznacz pola obok żądanych zdarzeń.

   Informacje o wybranych zdarzeniach są dostarczane za pośrednictwem poczty elektronicznej, jeśli skonfigurowano ustawienia dostarczania powiadomień e-mail.

7. Kliknij **OK**.

8. Jeśli włączyłeś powiadomienia e-mail, skonfiguruj ustawienia dostarczania poczty elektronicznej:

   a. Kliknij **Skonfiguruj powiadomienia e-mail**.

   b. Zaznacz pole **Powiadamiaj o zdarzeniach**, aby włączyć dostarczanie informacji o zdarzeniach Kaspersky Endpoint Security wybranych w kolumnie **Powiadom na e-mail**.

c. Określ ustawienia dostarczania powiadomień e-mail.

d. Kliknij **OK**.

9. Zapisz swoje zmiany.

Konfigurowanie wyświetlania komunikatów o stanie aplikacji w obszarze powiadomień

W celu skonfigurowania wyświetlania komunikatów o stanie aplikacji w obszarze powiadomień:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Interfejs**.
3. W sekcji **Pokaż stan aplikacji w obszarze powiadomień** zaznacz pola obok tych kategorii zdarzeń, o których chcesz być informowany w obszarze powiadomień systemu Microsoft Windows.
4. Zapisz swoje zmiany.

Jeśli wystąpią zdarzenia skojarzone z wybraną kategorią, ikon aplikacji w obszarze powiadomień paska zadań zmieni się na lub (w zależności od powagi komunikatu).

Przesyłanie wiadomości między użytkownikami a administratorem

Komponenty Kontrola aplikacji, Kontrola urządzeń, Kontrola sieci i Adaptacyjna kontrola anomalii umożliwiają użytkownikom sieci LAN, którzy mają zainstalowany program Kaspersky Endpoint Security, wysyłanie wiadomości do administratora.

Użytkownik może chcieć wysłać wiadomość do administratora lokalnej sieci firmowej w następujących przypadkach:

- Kontrola urządzeń zablokowała dostęp do urządzenia.

  Szablon wiadomości z prośbą o dostęp do zablokowanego urządzenia jest dostępny w interfejsie Kaspersky Endpoint Security, w sekcji Kontrola urządzeń.

- Kontrola aplikacji zablokowała uruchomienie aplikacji.

  Szablon wiadomości z prośbą o zezwolenie na uruchomienie zablokowanej aplikacji jest dostępny w interfejsie Kaspersky Endpoint Security, w sekcji Kontrola aplikacji.

- Kontrola sieci zablokowała dostęp do zasobu sieciowego.

  Szablon wiadomości z prośbą o dostęp do zablokowanego zasobu sieciowego jest dostępny w interfejsie Kaspersky Endpoint Security, w sekcji Kontrola sieci.

Metoda używana do wysyłania wiadomości oraz wykorzystanie szablonu zależą od tego, czy na komputerze z zainstalowanym programem Kaspersky Endpoint Security działa profil Kaspersky Security Center oraz czy jest połączenie z Serwerem administracyjnym Kaspersky Security Center. Możliwe są następujące scenariusze:

- Jeśli profil Kaspersky Security Center nie działa na komputerze, na którym jest zainstalowany Kaspersky Endpoint Security, komunikat użytkownika zostanie wysłany do administratora sieci lokalnej za pośrednictwem poczty elektronicznej.

  Pola wiadomości są uzupełniane wartościami z pól szablonu, zdefiniowanego w lokalnym interfejsie Kaspersky Endpoint Security.

- Jeśli profil Kaspersky Security Center działa na komputerze, na którym jest zainstalowany Kaspersky Endpoint Security, standardowa wiadomość zostanie wysłana na Serwer administracyjny Kaspersky Security Center.

  W tym przypadku wiadomości użytkownika można sprawdzić w miejscu przechowywania zdarzeń programu Kaspersky Security Center (patrz instrukcja poniżej). Pola wiadomości są uzupełniane wartościami z szablonu zdefiniowanego w profilu Kaspersky Security Center.

- Jeśli na komputerze z zainstalowanym produktem Kaspersky Endpoint Security działa profil użytkownika mobilnego z Kaspersky Security Center, metoda używana do wysyłania wiadomości zależy od tego, czy jest połączenie z Kaspersky Security Center.

  - Jeśli zostało nawiązane połączenie z Kaspersky Security Center, Kaspersky Endpoint Security wysyła standardowa wiadomość na Serwer administracyjny Kaspersky Security Center.

  - Jeśli nie zostało nawiązane połączenie z Kaspersky Security Center, komunikat użytkownika jest wysyłany do administratora sieci lokalnej za pośrednictwem poczty elektronicznej.

  W obu przypadkach pola wiadomości są uzupełniane wartościami z szablonu zdefiniowanego w profilu Kaspersky Security Center.

W celu przejrzenia wiadomości użytkownika w miejscu przechowywania zdarzeń programu Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Zdarzenia**.

   Obszar roboczy Kaspersky Security Center wyświetla wszystkie zdarzenia występujące podczas działania Kaspersky Endpoint Security, w tym wiadomości wysyłane do administratora, które są odbierane przez użytkowników sieci LAN.

3. Aby skonfigurować filtrowanie zdarzeń, na liście rozwijalnej **Wybory zdarzeń** wybierz **Żądania użytkownika**.

4. Wybierz wiadomość, która ma zostać wysłana do administratora.

5. W prawej części obszaru roboczego Konsoli administracyjnej kliknij przycisk **Otwórz okno właściwości zdarzenia**.

Zarządzanie raportami

W raportach zapisywane są informacje o działaniu każdego modułu programu Kaspersky Endpoint Security, zdarzeniach szyfrowania danych, wykonaniu każdego zadania skanowania, zadania aktualizacji oraz zadania sprawdzania integralności, a także o ogólnym działaniu aplikacji.

Raporty są przechowywane w folderze `C:\ProgramData\Kaspersky Lab\KES.14.1\Report`.

Raporty mogą zawierać następujące dane użytkownika:

- Ścieżki do plików przeskanowanych przez Kaspersky Endpoint Security.
- Ścieżki do kluczy rejestru zmodyfikowane podczas działania Kaspersky Endpoint Security.
- Nazwę użytkownika Microsoft Windows.
- Adresy stron internetowych otwieranych przez użytkownika.

Dane w raporcie są przedstawione w formie tabelarycznej. Każdy wiersz tabeli zawiera informacje o oddzielnym zdarzeniu. Atrybuty zdarzenia są zlokalizowane w kolumnach tabeli. Niektóre kolumny zawierają zagnieżdżone kolumny z dodatkowymi atrybutami. Aby wyświetlić dodatkowe atrybuty, należy kliknąć przycisk ⊞ znajdujący się obok nazwy kolumny. Zdarzenia zapisywane podczas działania różnych komponentów lub podczas wykonywania różnych zadań posiadają różne zestawy atrybutów.

Dostępne są następujące raporty:

- Raport **Audyt systemu**. Zawiera informacje o zdarzeniach występujących podczas interakcji pomiędzy użytkownikiem i aplikacją oraz o zdarzeniach występujących w trakcie działania aplikacji w ogóle, gdy nie są związane z żadnym konkretnym modułem lub zadaniem Kaspersky Endpoint Security.
- Raporty dotyczące działania komponentów Kaspersky Endpoint Security.
- Raporty zadań Kaspersky Endpoint Security.
- Raport **Szyfrowanie danych**. Zawiera informacje o zdarzeniach występujących podczas szyfrowania i deszyfrowania danych.

W raportach używane są następujące priorytety zdarzeń:

ⓘ **Zdarzenia informacyjne**. Odpowiednie zdarzenia nie zawierające istotnych informacji.

⚠ **Ostrzeżenia**. Zdarzenia wymagające uwagi użytkownika, ponieważ odzwierciedlają istotne sytuacje związane z działaniem Kaspersky Endpoint Security.

⊘ **Zdarzenia krytyczne**. Zdarzenia posiadające charakter krytyczny i wskazujące na problemy z działaniem Kaspersky Endpoint Security lub luki w ochronie komputera użytkownika.

W celu wygodnego zarządzania raportami możesz zmodyfikować wyświetlanie danych na ekranie w następujące sposoby:

- Filtrować listę zdarzeń według różnych kryteriów.
- Użyć opcji wyszukiwania określonych zdarzeń.
- Przejrzeć wybrane zdarzenie w oddzielnej sekcji.
- Sortować listę zdarzeń według każdej kolumny raportu.
- Wyświetlać i ukrywać zdarzenia grupowane przez filtr zdarzeń przy użyciu przycisku ⊞.
- Zmienić kolejność i rozmieszczenie kolumn wyświetlanych w raporcie.

W razie konieczności możesz zapisać wygenerowany raport do pliku. Możesz również usunąć raport z informacjami z działania komponentów i zadań programu Kaspersky Endpoint Security, które są połączone w grupy.

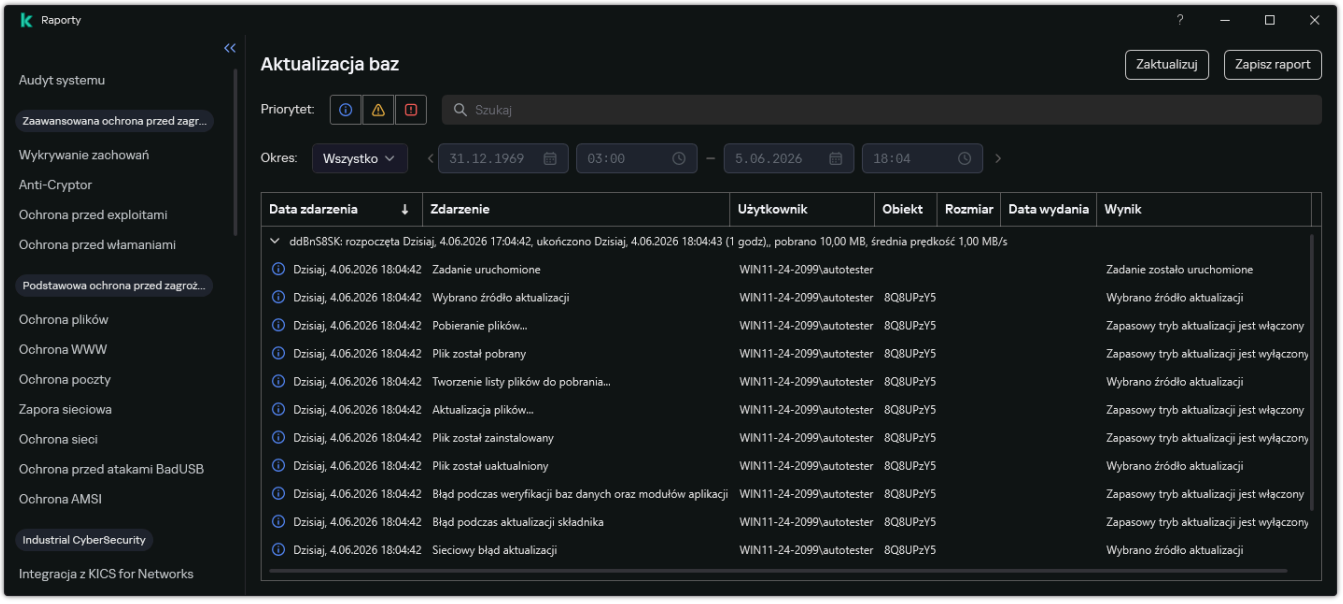
Jeśli Kaspersky Endpoint Security działa pod zarządzaniem Kaspersky Security Center, informacje o zdarzeniach mogą być przekazywane do Serwera administracyjnego Kaspersky Security Center (więcej informacji znajduje się w pomocy Kaspersky Security Center).

Wyświetlanie raportów

Jeśli użytkownik może przeglądać raporty, może także przeglądać wszystkie zdarzenia odzwierciedlone w raportach.

W celu wyświetlenia raportów:

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Raporty**.



Raporty

2. Na liście składników i zadań wybierz komponent lub zadanie.

   W prawej części okna zostanie wyświetlony raport zawierający listę zdarzeń będących wynikiem działania wybranego komponentu lub wybranego zadania Kaspersky Endpoint Security. Możesz posortować zdarzenia w raporcie w oparciu o wartości w komórkach jednej z kolumn.

3. Aby wyświetlić szczegółowe informacje o zdarzeniu, wybierz zdarzenie w raporcie.

W dolnej części okna zostaną wyświetlone informacje podsumowujące zdarzenie.

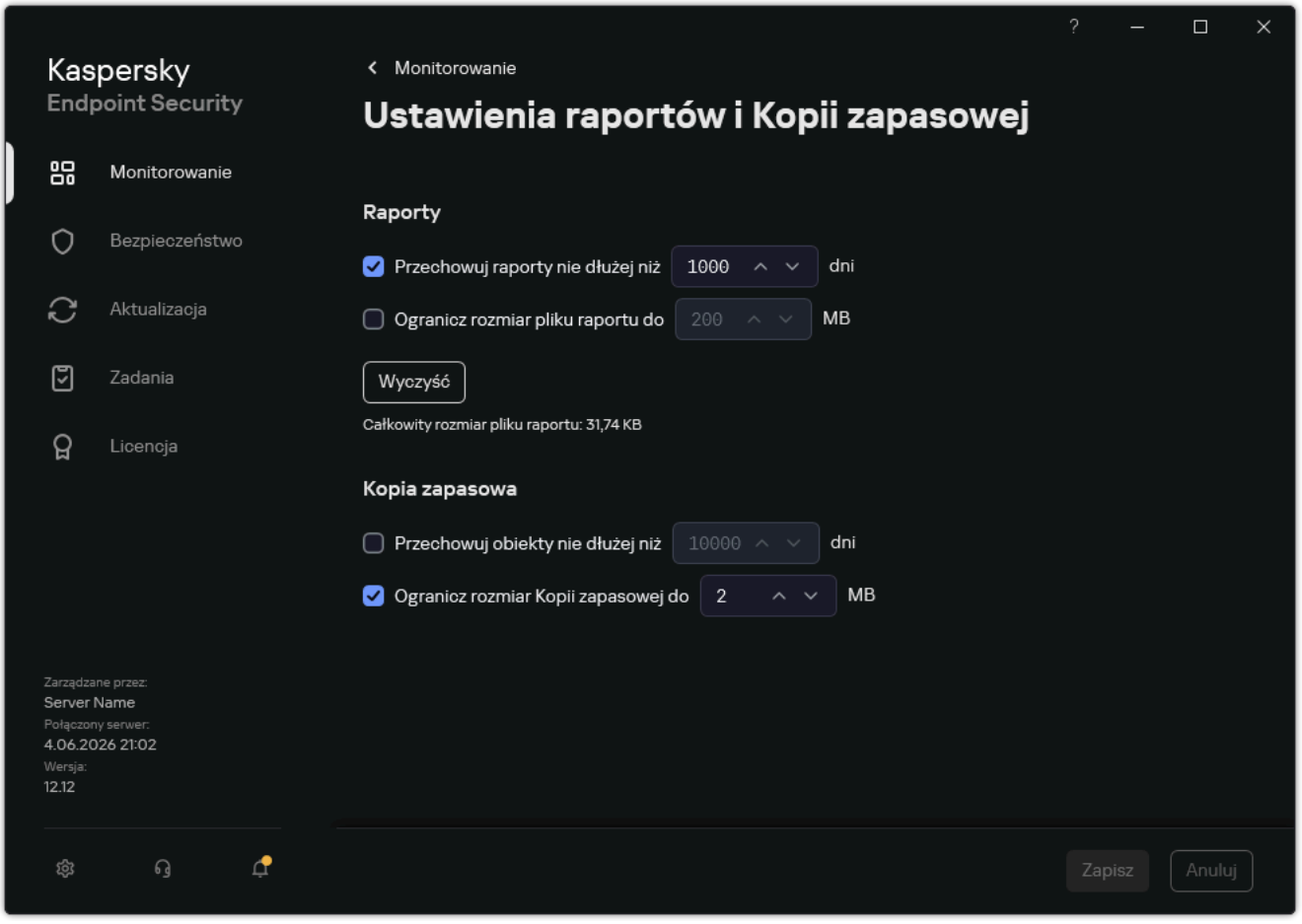
Konfigurowanie maksymalnego czasu przechowywania raportu

Maksymalny czas przechowywania dla raportów zapisywanych przez Kaspersky Endpoint Security wynosi 30 dni. Po tym czasie Kaspersky Endpoint Security automatycznie usuwa najstarsze wpisy z pliku raportu.

W celu zmiany maksymalnego czasu przechowywania raportów:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji kliknij kafelek **Raporty i Kopia zapasowa** w obszarze **Ustawienia ogólne**.



Ustawienia raportu

3. Jeśli chcesz ograniczyć czas przechowywania raportu, w sekcji **Raporty** zaznacz pole **Przechowuj raporty nie dłużej niż N dni**. Zdefiniuj maksymalny czas przechowywania raportu.

4. Zapisz swoje zmiany.

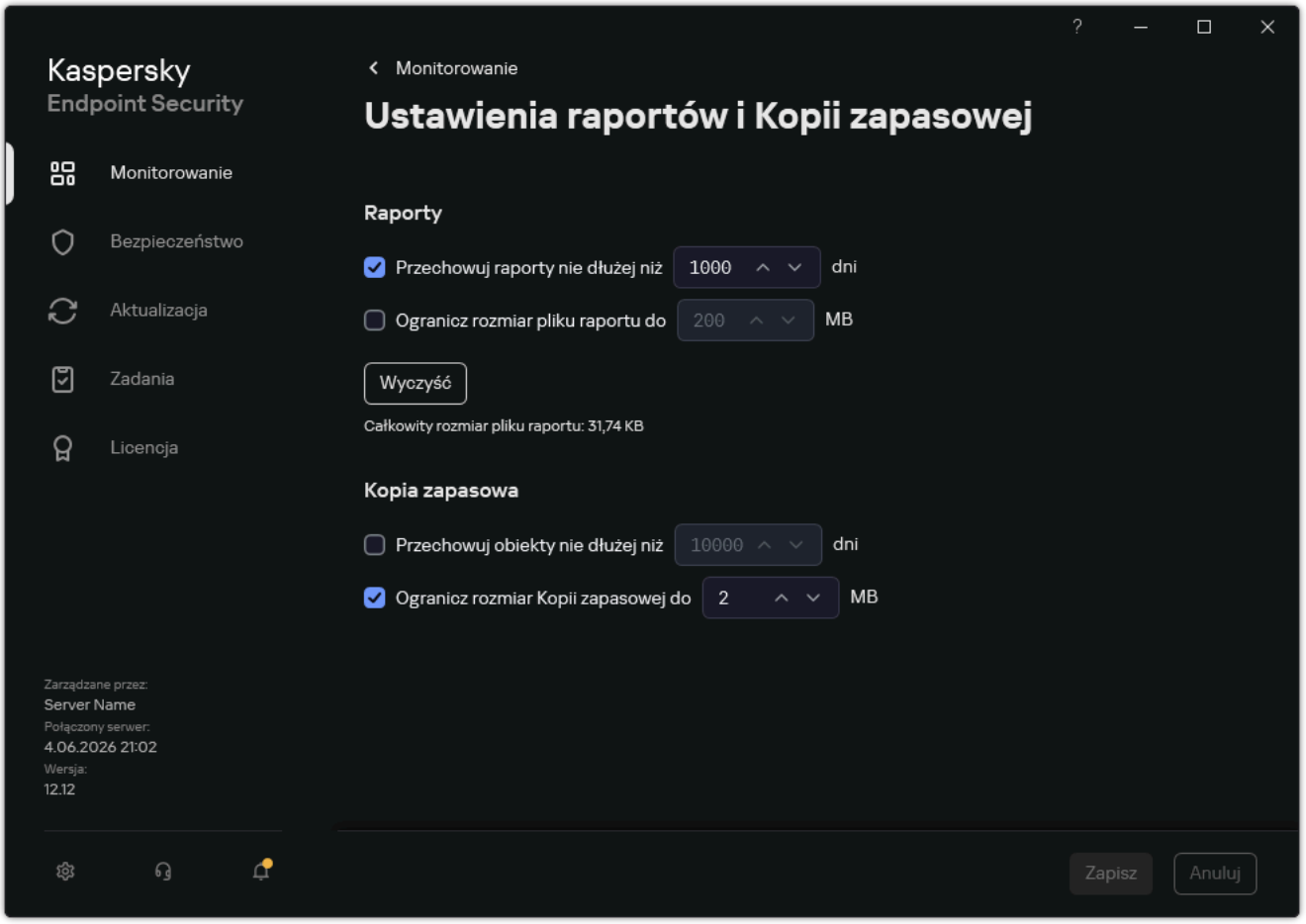
Konfigurowanie maksymalnego rozmiaru pliku raportu

Możesz określić maksymalny rozmiar pliku zawierającego raport. Domyślnie maksymalny rozmiar pliku raportu wynosi 1024 MB. Aby uniknąć przekroczenia maksymalnego rozmiaru pliku raportu, Kaspersky Endpoint Security automatycznie usuwa najstarsze wpisy z pliku raportu po osiągnięciu maksymalnego rozmiaru pliku raportu.

W celu skonfigurowania maksymalnego rozmiaru pliku raportu:

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji kliknij kafelek **Raporty i Kopia zapasowa** w obszarze **Ustawienia ogólne**.



Ustawienia raportu

3. W sekcji **Raporty** zaznacz pole **Ogranicz rozmiar pliku raportu do N MB**, jeśli chcesz ograniczyć rozmiar pliku raportu. Zdefiniuj maksymalny rozmiar pliku raportu.

4. Zapisz swoje zmiany.

Zapisywanie raportu do pliku

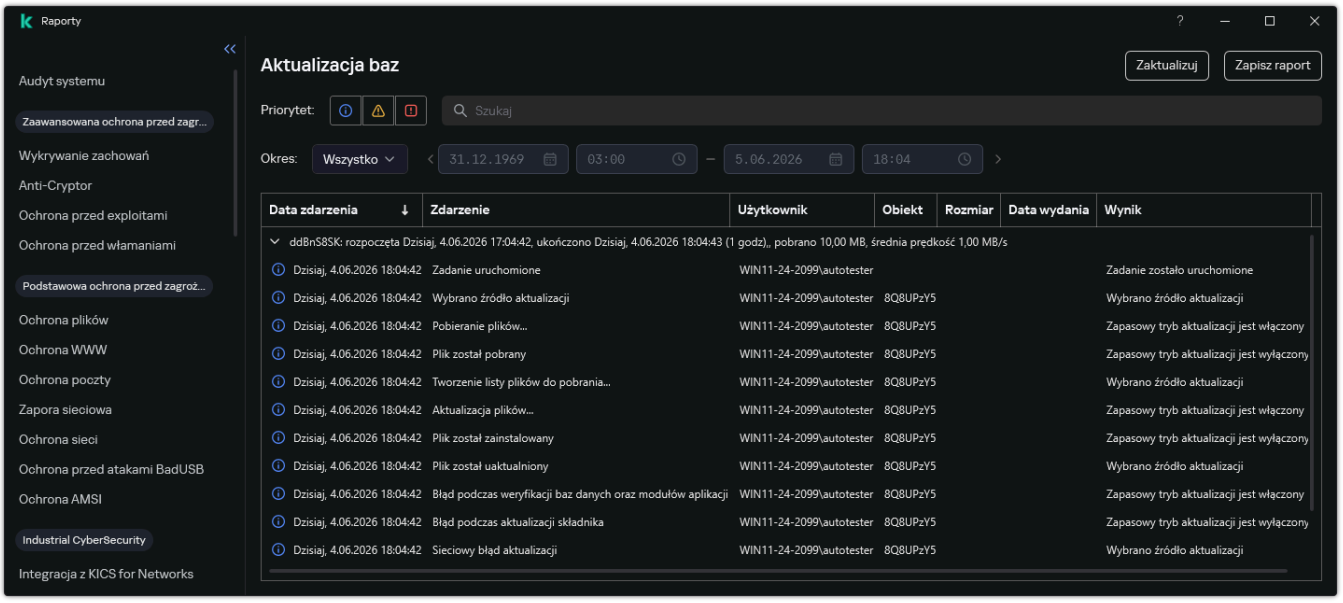
Użytkownik jest osobiście odpowiedzialny z zapewnienie bezpieczeństwa informacji z raportu zapisywanego do pliku i częściowo za kontrolowanie i ograniczanie dostępu do tych informacji.

Wygenerowany raport można zapisać do pliku w formacie tekstowym (TXT) lub pliku CSV.

Kaspersky Endpoint Security zapisuje zdarzenia w raporcie w takiej formie, w jakiej są wyświetlane na ekranie: innymi słowy, z takim samym zestawem i sekwencją atrybutów.

W celu zapisania raportu do pliku:

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Raporty**.



Raporty

2. To spowoduje otwarcie okna; w tym oknie wybierz komponent lub zadanie.

   Raport jest wyświetlany w prawej części okna i zawiera listę zdarzeń dotyczących działania wybranego modułu lub zadania Kaspersky Endpoint Security.

3. W razie konieczności możesz zmodyfikować wyświetlanie danych w raporcie poprzez:

   - Filtrowanie zdarzeń
   - Wyszukiwanie zdarzeń
   - Zmienianie kolejności kolumn
   - Sortowanie zdarzeń

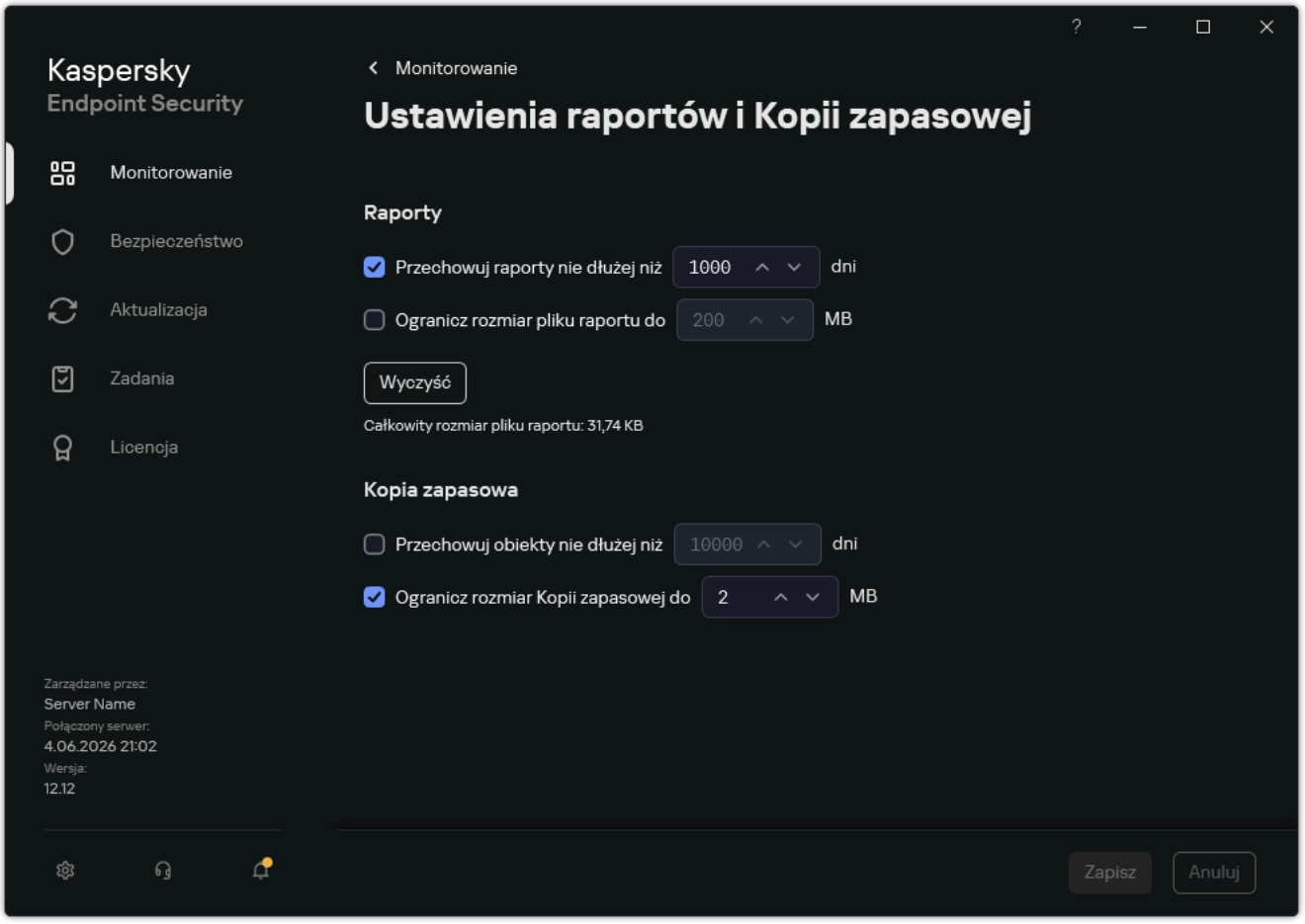
4. Kliknij przycisk **Zapisz raport** znajdujący się w prawej górnej części okna.

5. W otwartym oknie określ folder docelowy dla pliku raportu.
6. Wprowadź nazwę pliku raportu.
7. Wybierz odpowiedni format pliku raportu: TXT lub CSV.
8. Zapisz swoje zmiany.

Czyszczenie raportów

W celu usunięcia informacji z raportów:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji kliknij kafelek **Raporty i Kopia zapasowa** w obszarze **Ustawienia ogólne**.



Ustawienia raportu

3. W sekcji **Raporty** kliknij przycisk **Wyczyść**.
4. Jeśli Ochrona hasłem jest włączona, Kaspersky Endpoint Security może wyświetlić monit o podanie danych uwierzytelniających do konta użytkownika. Aplikacja wyświetla monit o podanie danych uwierzytelniających do konta, jeśli użytkownik nie ma żądanego uprawnienia.

Kaspersky Endpoint Security usunie wszystkie raporty dla wszystkich komponentów i zadań aplikacji.

Autoochrona Kaspersky Endpoint Security

Autoochrona uniemożliwia innym aplikacjom wykonanie działań, które mogą przeszkadzać w działaniu Kaspersky Endpoint Security i, na przykład, usunąć Kaspersky Endpoint Security z komputera. Zestaw dostępnych technologii autoochrony dla Kaspersky Endpoint Security zależy od tego, czy system operacyjny jest 32-bitowy, czy 64-bitowy (patrz tabela poniżej). Autoochrona obejmuje również ochronę hasłem i ochronę połączenia z Serwerem administracyjnym.

Ochrona hasłem umożliwia ograniczenie dostępu użytkowników do Kaspersky Endpoint Security zgodnie z uprawnieniami im nadanymi (na przykład, uprawnienie do zakończenia działania aplikacji).

Ochrona połączenia z Serwerem administracyjnym zapobiega nieautoryzowanemu ponownemu podłączeniu komputera do niezaufanego serwera.

Technologie autoochrony Kaspersky Endpoint Security

Technologia	Opis	Komputer z architekturą x86	Komputer z architekturą x64
Mechanizm autoochrony	Technologia blokuje dostęp do następujących komponentów aplikacji: • pliki w folderze instalacyjnym Kaspersky Endpoint Security i inne pliki aplikacji; • klucze rejestru z wpisami należącymi do aplikacji; • procesy, które aplikacja uruchamia.	✓	✓
AM-PPL (Antimalware Protected Process Light)	Technologia chroni procesy Kaspersky Endpoint Security przed szkodliwymi działaniami. Więcej informacji na temat technologii AM-PPL znajdziesz na stronie internetowej firmy Microsoft. Technologia AM-PPL jest dostępna dla systemu Windows 10 w wersji 1703 (RS2) lub nowszej oraz systemów operacyjnych Windows Server 2019.	✓	✓
Mechanizm ochrony przed zewnętrznym zarządzaniem	Ta technologia uniemożliwia innym aplikacjom (np. TeamViewer lub RemotelyAnywhere) uzyskanie dostępu do Kaspersky Endpoint Security.	✓	– (za wyjątkiem Windows 7)

Włączanie i wyłączanie Autoochrony

Kaspersky Endpoint Security uniemożliwia modyfikowanie i usuwanie plików aplikacji, procesów pamięci i wpisów w rejestrze systemowym.

Technologia blokuje dostęp do następujących komponentów aplikacji:

- pliki w folderze instalacyjnym Kaspersky Endpoint Security i inne pliki aplikacji;
- klucze rejestru z wpisami należącymi do aplikacji;
- procesy, które aplikacja uruchamia.

Domyślnie Autoochrona programu Kaspersky Endpoint Security jest włączona.

Jak w Konsoli administracyjnej (MMC) włączyć lub wyłączyć Autoochronę?

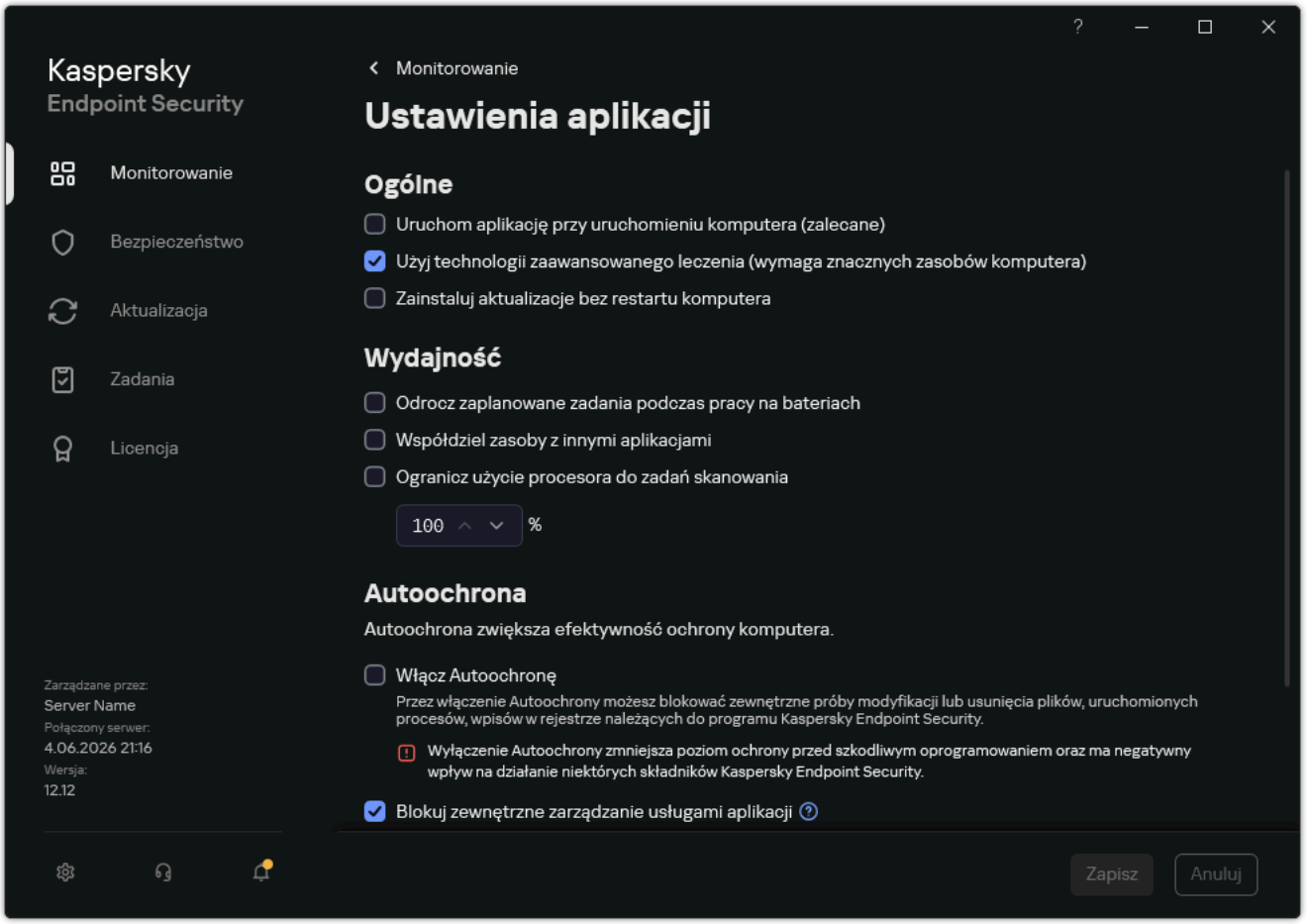
1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.
4. Użyj pola **Włącz autoochronę**, aby włączyć lub wyłączyć mechanizm autoochrony.
5. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć Autoochronę w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Autoochrona**.
5. Użyj przełącznika **Autoochrona WŁĄCZONA**, aby włączyć lub wyłączyć mechanizm Autoochrona.
6. Zapisz swoje zmiany.

Jak w interfejsie aplikacji włączyć lub wyłączyć Autoochronę?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.



Ustawienia Kaspersky Endpoint Security for Windows

3. Użyj pola **Włącz Autoochronę**, aby włączyć lub wyłączyć mechanizm autoochrony.
4. Zapisz swoje zmiany.

Włączanie i wyłączanie obsługi AM-PPL

Kaspersky Endpoint Security obsługuje technologię Antimalware Protected Process Light (zwana dalej „AM-PPL") firmy Microsoft. AM-PPL chroni procesy Kaspersky Endpoint Security przed szkodliwymi działaniami (na przykład, zakończeniem działania aplikacji). AM-PPL pozwala na uruchamianie tylko zaufanych procesów. Procesy Kaspersky Endpoint Security są podpisywane zgodnie z wymaganiami dotyczącymi zabezpieczeń systemu Windows, dlatego są zaufane. Więcej informacji na temat technologii AM-PPL znajdziesz na stronie internetowej firmy Microsoft. Domyślnie technologia AM-PPL jest włączona.

Kaspersky Endpoint Security ma również wbudowane mechanizmy ochrony procesów aplikacji. Obsługa AM-PPL pozwala delegować funkcje ochrony procesów do systemu operacyjnego. W ten sposób można zwiększyć szybkość aplikacji i zmniejszyć zużycie zasobów komputerowych.

Korzystaj z technologii AM-PPL w sposób ciągły. AM-PPL jest ważnym elementem ochrony systemu operacyjnego. Wyłączenie obsługi AM-PPL może spowodować nieprawidłowe działanie niektórych funkcji Kaspersky Endpoint Security (na przykład integrację aplikacji z Windows Security Center). Wyłączenie obsługi AM-PPL jest dozwolone wyłącznie w oddzielnym środowisku testowym w celu rozwiązywania problemów.

Technologia AM-PPL jest dostępna dla systemu Windows 10 w wersji 1703 (RS2) lub nowszej oraz systemów operacyjnych Windows Server 2019.

W celu włączenia lub wyłączenia technologii AM-PPL:

1. Wyłącz mechanizm autoochrony aplikacji.

   Mechanizm autoochrony zapobiega modyfikowaniu i usuwaniu procesów aplikacji w pamięci komputera, w tym zmianie stanu AM-PPL.

2. Uruchom wiersz poleceń (cmd.exe) jako administrator.

3. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

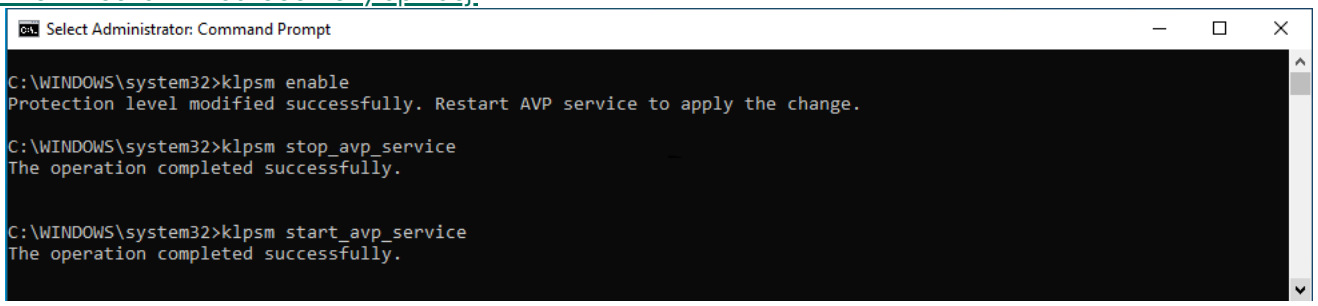
   Możesz dodać ścieżkę do pliku wykonywalnego do zmiennej systemowej %PATH% podczas instalacja aplikacji.

4. W wierszu poleceń wpisz następujące polecenie:

   - `klpsm.exe enable` - włącza obsługę technologii AM-PPL (patrz rysunek poniżej).
   - `klpsm.exe disable` - wyłącz aobsługę technologii AM-PPL.

5. Uruchom ponownie Kaspersky Endpoint Security.

6. Wznów mechanizm autoochrony aplikacji.



Włączanie obsługi technologii AM-PPL

Ochrona usług aplikacji przed zewnętrznym zarządzaniem

Ochrona usług aplikacji przed zewnętrznym zarządzaniem blokuje próby zatrzymania usług Kaspersky Endpoint Security przez użytkowników i inne aplikacje. Ochrona zapewnia działanie następujących usług:

- Usługa Kaspersky Endpoint Security (AVP.KES.14.1)
- Usługa Kaspersky Seamless Update Service (AVPSUS.KES.14.1)

Aby zakończyć działanie aplikacji z poziomu wiersza poleceń, wyłącz ochronę usług Kaspersky Endpoint Security przed zewnętrznym zarządzaniem.

Zezwalać na zewnętrzne zarządzanie usługami aplikacji można tylko na komputerach, które nie obsługują technologii AM-PPL lub na komputerach, na których wyłączono tę technologię.

Jak włączyć lub wyłączyć Ochronę usług aplikacji przed zewnętrznym zarządzaniem w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.
4. Użyj pola **Blokuj zewnętrzne zarządzanie usługami aplikacji**, aby włączyć lub wyłączyć ochronę usług Kaspersky Endpoint Security przed zewnętrznym zarządzaniem.
5. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć Ochronę usług aplikacji przed zewnętrznym zarządzaniem w Web Console i Cloud Console?

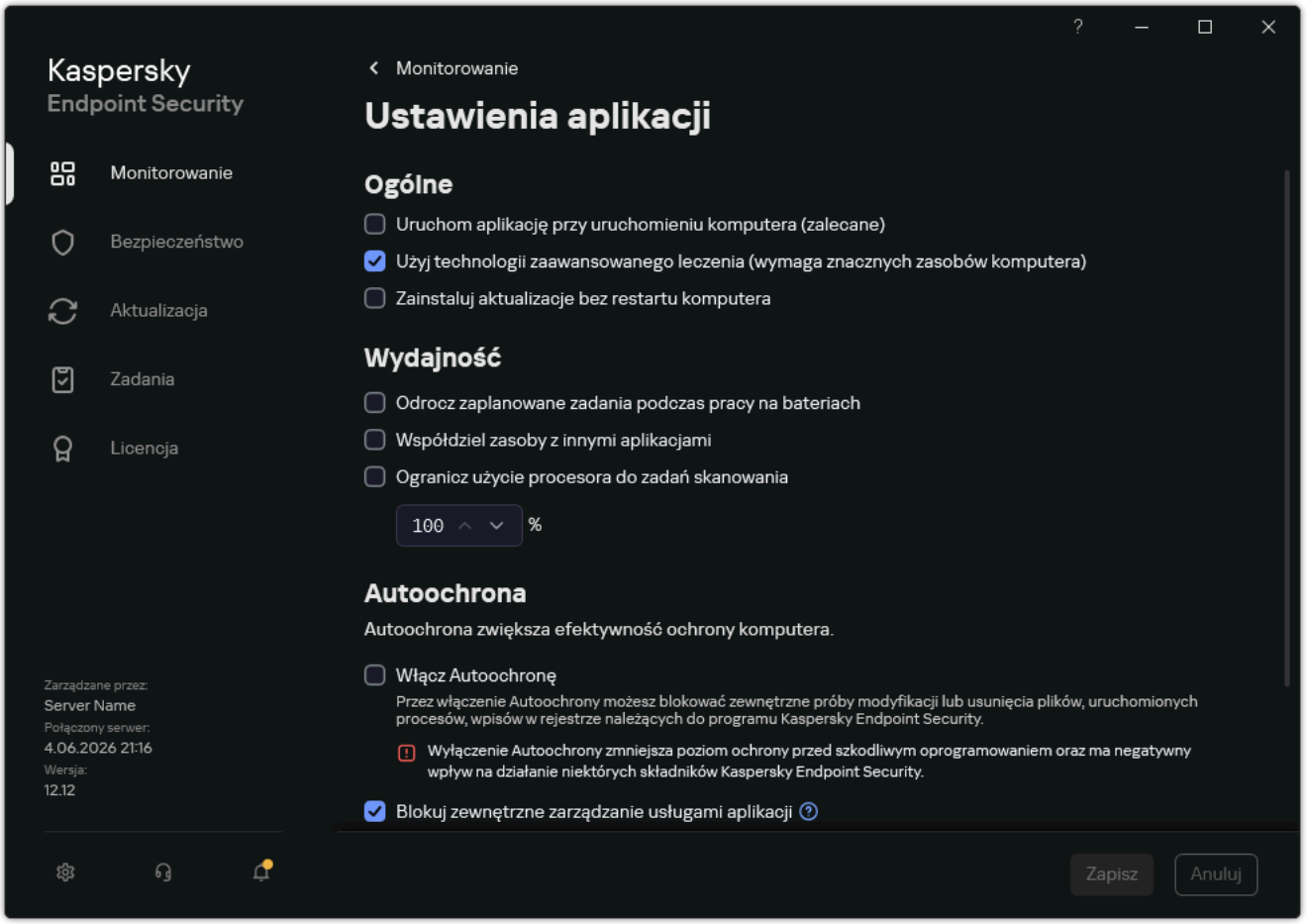
1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Autoochrona**.
5. Użyj pola **Blokuj zewnętrzne zarządzanie usługami aplikacji**, aby włączyć lub wyłączyć ochronę usług Kaspersky Endpoint Security przed zewnętrznym zarządzaniem.
6. Zapisz swoje zmiany.

Jak włączyć lub wyłączyć Ochronę usług aplikacji przed zewnętrznym zarządzaniem w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.

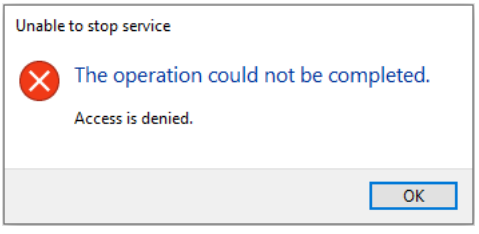


Ustawienia Kaspersky Endpoint Security for Windows

3. Użyj pola **Blokuj zewnętrzne zarządzanie usługami aplikacji**, aby włączyć lub wyłączyć ochronę usług Kaspersky Endpoint Security przed zewnętrznym zarządzaniem.

4. Zapisz swoje zmiany.

W rezultacie, gdy użytkownik próbuje zatrzymać usługi aplikacji, pojawia się okno systemowe z komunikatem o błędzie. Użytkownik może zarządzać usługami aplikacji tylko z poziomu interfejsu Kaspersky Endpoint Security.



Błąd dostępu do usług aplikacji

Obsługiwanie aplikacji do zdalnej administracji

Czasami możesz potrzebować aplikacji do zdalnej administracji, gdy włączona jest ochrona przed zewnętrznym zarządzaniem.

W celu włączenia działania aplikacji do zdalnej administracji:

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Wykluczenia i typy wykrytych obiektów**.
3. W sekcji **Wykluczenia** kliknij odnośnik **Określ zaufane aplikacje**.
4. W otwartym oknie kliknij przycisk **Dodaj**.
5. Wybierz plik wykonywalny aplikacji do zdalnej administracji.

   Możesz także wprowadzić ścieżkę ręczne. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.
6. Zaznacz pole **Zezwól na interakcję z interfejsem Kaspersky Endpoint Security**.
7. Zapisz swoje zmiany.

Ochrona hasłem

Zdarza się, że z jednego komputera korzysta wielu użytkowników o rożnej umiejętności jego obsługi. Jeżeli użytkownicy nie mają ograniczonego dostępu do Kaspersky Endpoint Security i jego ustawień, może to zmniejszyć ogólny poziom ochrony komputera. Ochrona hasłem umożliwia ograniczenie dostępu użytkowników do Kaspersky Endpoint Security zgodnie z uprawnieniami im nadanymi (na przykład, uprawnienie do zakończenia działania aplikacji).

Jeśli użytkownik, który rozpoczął sesję Windows (*użytkownik sesji*) ma uprawnienia do wykonania tej akcji, Kaspersky Endpoint Security nie prosi o nazwę użytkownika i hasło ani o hasło tymczasowe. Użytkownik uzyskuje dostęp do Kaspersky Endpoint Security zgodnie z udzielonymi uprawnieniami.

Jeśli użytkownik sesji nie ma uprawnień do wykonania akcji, może uzyskać dostęp do aplikacji w następujące sposoby:

- Wprowadź nazwę użytkownika i hasło.

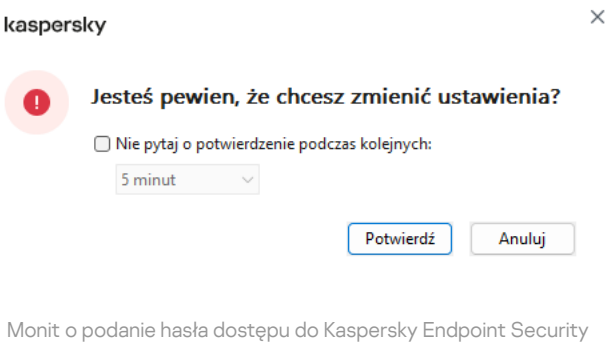
  Ta metoda jest odpowiednia dla codziennych działań. Aby wykonać działanie chronione hasłem, musisz wprowadzić poświadczenia konta domeny użytkownika z wymaganym uprawnieniem. W takim przypadku komputer musi należeć do tej domeny. Jeśli komputer nie znajduje się w domenie, możesz użyć konta KLAdmin lub konta dodanego ręcznie.

- Wprowadź hasło tymczasowe.

  Ta metoda jest odpowiednia do nadania uprawnień tymczasowych do wykonywania zablokowanych działań (na przykład, kończenia działania aplikacji) użytkownikom poza siecią firmową. Jeśli hasło tymczasowe wygaśnie lub sesja zakończy się, Kaspersky Endpoint Security przywróci ustawienia do poprzedniego stanu.

Jeśli użytkownik spróbuje wykonać działanie ochrony hasłem, Kaspersky Endpoint Security wyświetli prośbę o podanie nazwy użytkownika i hasła lub hasła tymczasowego (patrz rysunek poniżej).

W oknie do wprowadzenia hasła możesz zmienić język tylko poprzez wciśnięcie klawiszy **ALT+SHIFT**. Korzystając z innych skrótów, nawet wtedy, gdy są skonfigurowane w systemie operacyjnym, nie działają do zmiany języków.



Monit o podanie hasła dostępu do Kaspersky Endpoint Security

Nazwa użytkownika i hasło

Aby uzyskać dostęp do Kaspersky Endpoint Security, musisz wprowadzić dane uwierzytelniające konta. Ochrona hasłem obsługuje następujące konta:

- **KLAdmin**. Konto administratora z nieograniczonym dostępem do Kaspersky Endpoint Security. Konto KLAdmin posiada prawo do wykonania dowolnego działania, które jest chronione hasłem. Uprawnień dla konta KLAdmin nie można wycofać. Jeśli włączysz ochronę hasłem, Kaspersky Endpoint Security wyświetli monit o ustawienie hasła dla konta KLAdmin.

- **Konto dodane ręcznie**. Konto spoza domeny Active Directory. Możesz używać tego konta usługi zamiast konta KLAdmin, jeżeli nie chcesz udostępniać swojego hasła administratora. Możesz wybrać dowolną nazwę użytkownika i hasło oraz skonfigurować poszczególne uprawnienia.

- **Grupa Każda**. Wbudowana grupa Windows, która zawiera wszystkich użytkowników w obrębie sieci firmowej. Użytkownicy w grupie Każda mogą uzyskać dostęp do aplikacji zgodnie z uprawnieniami, które są im nadane.

- **Użytkownicy indywidualni lub grupy**. Konta użytkowników, dla których możesz skonfigurować uprawnienia indywidualne. Na przykład, jeśli działanie jest zablokowane dla grupy Każda, możesz zezwolić na to działanie dla użytkownika indywidualnego lub grupy.

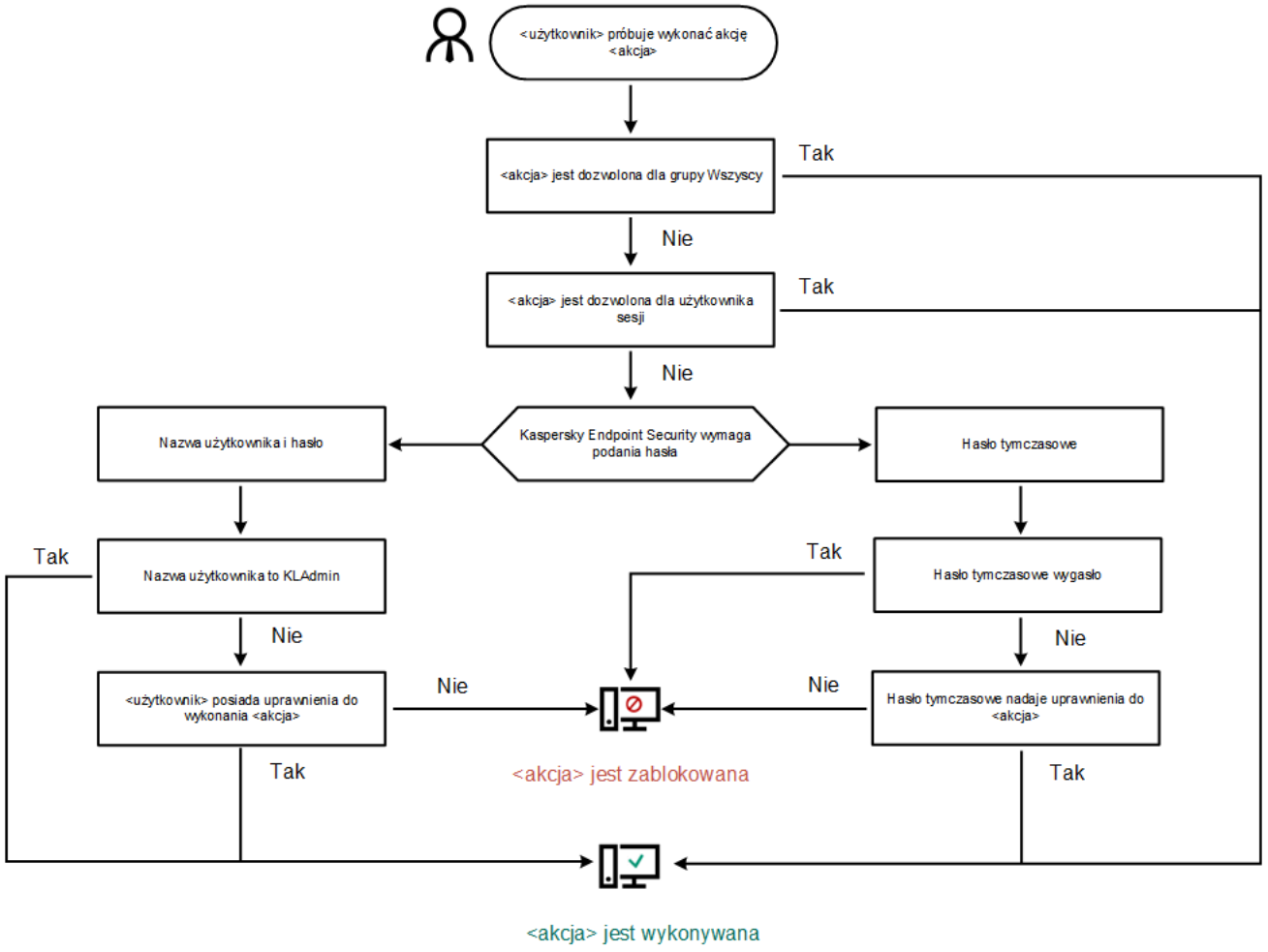
- **Użytkownik sesji**. Konto użytkownika, który uruchomił sesję systemu Windows. Po wyświetleniu monitu o podanie hasła, możesz przełączyć się do innego użytkownika sesji (pole **Zapisz hasło dla bieżącej sesji**). W tym przypadku Kaspersky Endpoint Security odnosi się do użytkownika, którego dane uwierzytelniające zostały wprowadzone jako użytkownika sesji zamiast użytkownika, który rozpoczął sesję systemu Windows.

Hasło tymczasowe

Hasło tymczasowe może zostać użyte do nadania tymczasowego dostępu do Kaspersky Endpoint Security dla pojedynczego komputera poza siecią firmową. Administrator generuje hasło tymczasowe dla indywidualnego komputera we właściwościach komputera w Kaspersky Security Center. Administrator wybierz działania, które będą chronione hasłem tymczasowym, i określa okres ważności hasła tymczasowego.

Algorytm działania ochrony hasłem

Kaspersky Endpoint Security decyduje, czy zezwolić na lub zablokować działanie ochrony hasłem w oparciu o następujący algorytm (patrz rysunek poniżej).



Algorytm działania ochrony hasłem

Włączanie ochrony hasłem

Ochrona hasłem umożliwia ograniczenie dostępu użytkowników do Kaspersky Endpoint Security zgodnie z uprawnieniami im nadanymi (na przykład, uprawnienie do zakończenia działania aplikacji).

Jak w Konsoli administracyjnej (MMC) włączyć Ochronę hasłem?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Interfejs**.
4. W sekcji **Ochrona hasłem** kliknij przycisk **Ustawienia**.

   Spowoduje to otwarcie okna z ustawieniami Ochrony hasłem.
5. Użyj pola **Włącz ochronę hasłem**, aby włączyć lub wyłączyć komponent.
6. W sekcji **Uprawnienia** wybierz konto KLAdmin.
7. Spowoduje to otwarcie okna; w tym oknie kliknij **Hasło** i ustaw hasło do konta KLAdmin.

   Konto KLAdmin posiada prawo do wykonania dowolnego działania, które jest chronione hasłem.

   > Jeśli nie pamiętasz hasła do konta KLAdmin, możesz zresetować hasło we właściwościach zasady.
8. Wróć do listy kont.
9. Ustaw uprawnienia dla wszystkich użytkowników w sieci firmowej:

   a. W sekcji **Uprawnienia** wybierz grupę „Wszyscy".

      Grupa Każda jest wbudowaną grupą Windows, która zawiera wszystkich użytkowników w obrębie sieci firmowej.

   b. W otwartym oknie zaznacz pola obok działań, które użytkownicy będą mogli wykonywać bez wprowadzenia hasła.

      Jeśli pole jest odznaczone, użytkownicy nie mogą wykonywać tego działania. Na przykład, jeśli pole obok uprawnienia **Zakończenie działania aplikacji** jest odznaczone, możesz zakończyć działanie aplikacji tylko wtedy, gdy jesteś zalogowany jako KLAdmin lub jako pojedynczy użytkownik, który posiada wymagane uprawnienie, lub jeśli wprowadzisz hasło tymczasowe.

      > Uprawnienia Ochrony hasłem obejmują pewne ważne aspekty, które należy rozważyć. Upewnij się, że wszystkie warunki dla uzyskania dostępu do Kaspersky Endpoint Security zostaną spełnione.
10. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console włączyć Ochronę hasłem?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Autoochrona**.

5. W sekcji **Ochrona hasłem** użyj przełącznika **Ochrona hasłem WŁĄCZONA**, aby włączyć lub wyłączyć komponent.

6. Określ hasło dla konta KLAdmin i potwierdź je.

   Konto KLAdmin posiada prawo do wykonania dowolnego działania, które jest chronione hasłem.

   > Jeśli nie pamiętasz hasła do konta KLAdmin, możesz zresetować hasło we właściwościach zasady.

7. Wróć do listy kont.

8. Ustaw uprawnienia dla wszystkich użytkowników w sieci firmowej:

   a. W tabeli kont wybierz grupę „Wszyscy".

      Grupa Każda jest wbudowaną grupą Windows, która zawiera wszystkich użytkowników w obrębie sieci firmowej.

   b. W otwartym oknie zaznacz pola obok działań, które użytkownicy będą mogli wykonywać bez wprowadzenia hasła.

      Jeśli pole jest odznaczone, użytkownicy nie mogą wykonywać tego działania. Na przykład, jeśli pole obok uprawnienia **Zakończenie działania aplikacji** jest odznaczone, możesz zakończyć działanie aplikacji tylko wtedy, gdy jesteś zalogowany jako KLAdmin lub jako pojedynczy użytkownik, który posiada wymagane uprawnienie, lub jeśli wprowadzisz hasło tymczasowe.

      > Uprawnienia Ochrony hasłem obejmują pewne ważne aspekty, które należy rozważyć. Upewnij się, że wszystkie warunki dla uzyskania dostępu do Kaspersky Endpoint Security zostaną spełnione.

9. Zapisz swoje zmiany.

Jak w interfejsie aplikacji włączyć Ochronę hasłem?

1. W oknie głównym aplikacji kliknij przycisk ⚙.

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Interfejs**.

3. Użyj przełącznika **Ochrona hasłem**, aby włączyć lub wyłączyć komponent.

4. Określ hasło dla konta KLAdmin i potwierdź je.

   Konto KLAdmin posiada prawo do wykonania dowolnego działania, które jest chronione hasłem.

   > Jeśli komputer działa pod kontrolą profilu, Administrator może zresetować hasło dla konta KLAdmin we właściwościach profilu. Jeśli komputer nie jest połączony z Kaspersky Security Center, a Ty zapomniałeś hasło do konta KLAdmin, nie ma możliwości odzyskania hasła.

5. Ustaw uprawnienia dla wszystkich użytkowników w sieci firmowej:

   a. W tabeli konta kliknij przycisk **Edytuj**, aby otworzyć listę uprawnień dla grupy Każdy.

      Grupa Każda jest wbudowaną grupą Windows, która zawiera wszystkich użytkowników w obrębie sieci firmowej.

   b. Zaznacz pola obok działań, które użytkownicy będą mogli wykonywać bez wprowadzenia hasła.

Jeśli pole jest odznaczone, użytkownicy nie mogą wykonywać tego działania. Na przykład, jeśli pole obok uprawnienia **Zakończenie działania aplikacji** jest odznaczone, możesz zakończyć działanie aplikacji tylko wtedy, gdy jesteś zalogowany jako KLAdmin lub jako pojedynczy użytkownik, który posiada wymagane uprawnienie, lub jeśli wprowadzisz hasło tymczasowe.

Uprawnienia Ochrony hasłem obejmują pewne ważne aspekty, które należy rozważyć. Upewnij się, że wszystkie warunki dla uzyskania dostępu do Kaspersky Endpoint Security zostaną spełnione.

6. Zapisz swoje zmiany.

Jeśli ochrona hasłem jest włączona, aplikacja ograniczy dostęp użytkowników do Kaspersky Endpoint Security zgodnie z uprawnieniami nadanymi grupie Każda. Możesz wykonać działania, które są zablokowane dla grupy Każda tylko wtedy, gdy korzystasz z konta KLAdmin, innego konta posiadającego wymagane uprawnienia, lub jeśli wprowadzasz hasło tymczasowe.

Możesz wyłączyć Ochronę hasłem tylko wtedy, gdy jesteś zalogowany jako KLAdmin. Nie można wyłączyć ochrony hasłem, jeśli używasz innego konta użytkownika lub hasła tymczasowego.

Podczas sprawdzania hasła możesz zaznaczyć pole **Zapisz hasło dla bieżącej sesji**. W tym przypadku Kaspersky Endpoint Security nie wyświetli monitu o podanie hasła, gdy użytkownik próbuje wykonać inne działanie ochrony hasłem na czas trwania sesji.

Nadawanie uprawnień pojedynczym użytkownikom lub grupom

Ochrona hasłem umożliwia przyznawanie dostępu do Kaspersky Endpoint Security poszczególnym kontom użytkownika Active Directory i ręczne dodawanie kont użytkownika.

Konta użytkownika Active Directory

Możesz przyznać dostęp do Kaspersky Endpoint Security poszczególnym użytkownikom lub grupom użytkowników w domenie Active Directory. Na przykład, jeśli istniejąca aplikacja jest zablokowana dla grupy Każda, możesz nadać uprawnienie **Zakończenie działania aplikacji** pojedynczemu użytkownikowi. W wyniku tego możesz zakończyć działanie aplikacji tylko wtedy, gdy jesteś zalogowany jako ten użytkownik lub jako KLAdmin.

Możesz użyć danych uwierzytelniających do konta, aby uzyskać dostęp do aplikacji tylko wtedy, gdy komputer jest w domenie. Jeśli komputer nie znajduje się w domenie, możesz użyć konta KLAdmin lub hasła tymczasowego.

Ręcznie dodane konta użytkownika

Możesz utworzyć konto użytkownika, którego nie ma w usłudze Active Directory i przydzielić osobne uprawnienia do tego konta użytkownika. Oznacza to, że możesz utworzyć *konto użytkownika usługi* i używać go zamiast konta KLAdmin. W ten sposób nie musisz udostępniać hasła KLAdmin innym użytkownikom ani tworzyć nowych kont użytkownika Active Directory. Możesz wprowadzić dowolną nazwę użytkownika i hasło. Na przykład, możesz przydzielić uprawnienie **Wyświetl raporty** do konta użytkownika usługi. W rezultacie, jeżeli grupa „Wszyscy" nie może wyświetlać raportów, możesz otwierać raporty za pomocą konta użytkownika usługi lub konta użytkownika KLAdmin.

Nadawanie uprawnień pojedynczym użytkownikom lub grupom

Jak nadawać uprawnienia użytkownikom indywidualnym lub grupom w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Interfejs**.
4. W sekcji **Ochrona hasłem** kliknij przycisk **Ustawienia**.

   Spowoduje to otwarcie okna z ustawieniami Ochrony hasłem.
5. W tabeli konta kliknij **Dodaj**.
6. Wybierz typ konta użytkownika, który chcesz dodać:

   - **Wybierz użytkownika/grupę z Active Directory** – konta użytkownika Active Directory.

     Aby wybrać konto użytkownika, kliknij przycisk **Wybierz**. Wybierz użytkownika lub grupę w Active Directory i potwierdź swój wybór.
   - **Dodaj użytkownika/grupę ręcznie** dla ręcznie dodanego konta użytkownika usługi.

     Aby dodać konto użytkownika usługi, wprowadź nazwę użytkownika i hasło (na przykład, SecureAdmin).

     > Możesz zresetować hasło do konta użytkownika usługi w ustawieniach zasad. Hasło konta użytkownika usługi resetuje się w ten sam sposób, co hasło konta KLAdmin. Jeśli edytowanie ustawień ochrony hasłem jest dozwolone („blokada" jest otwarta) lub na komputerze nie są stosowane żadne zasady, możesz zresetować hasło konta użytkownika usługi w interfejsie aplikacji. W tym celu potwierdź zmiany informacji o koncie użytkownika usługi za pomocą hasła KLAdmin.
7. Na liście **Uprawnienia** zaznacz pola obok działań, które wybrany użytkownik lub grupa będą mogli wykonywać bez pytania o podanie hasła.

   Jeśli pole jest odznaczone, użytkownicy nie mogą wykonywać tego działania. Na przykład, jeśli pole obok uprawnienia **Zakończenie działania aplikacji** jest odznaczone, możesz zakończyć działanie aplikacji tylko wtedy, gdy jesteś zalogowany jako KLAdmin lub jako pojedynczy użytkownik, który posiada wymagane uprawnienie, lub jeśli wprowadzisz hasło tymczasowe.

Uprawnienia Ochrony hasłem obejmują pewne ważne aspekty, które należy rozważyć. Upewnij się, że wszystkie warunki dla uzyskania dostępu do Kaspersky Endpoint Security zostaną spełnione.

8. Zapisz swoje zmiany.

Jak nadawać uprawnienia użytkownikom indywidualnym lub grupom w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Autoochrona**.
5. W sekcji **Ochrona hasłem** kliknij odnośnik **Uprawnienia użytkownika**.

   To powoduje otwarcie formularza umożliwiającego udzielenie uprawnień do włączania hasła.
6. Kliknij **Dodaj**.
7. Wybierz typ konta użytkownika, który chcesz dodać:

   - **Wybierz z usługi Active Directory** – konta użytkownika Active Directory.

     Aby wybrać konto użytkownika, kliknij przycisk **Edytuj**. Wybierz użytkownika lub grupę w Active Directory i potwierdź swój wybór.
   - **Dodaj ręcznie** dla ręcznie dodanego konta użytkownika usługi.

     Aby dodać konto użytkownika usługi, wprowadź nazwę użytkownika i hasło (na przykład, SecureAdmin).

     Możesz zresetować hasło do konta użytkownika usługi w ustawieniach zasad. Hasło konta użytkownika usługi resetuje się w ten sam sposób, co hasło konta KLAdmin. Jeśli edytowanie ustawień ochrony hasłem jest dozwolone („blokada" jest otwarta) lub na komputerze nie są stosowane żadne zasady, możesz zresetować hasło konta użytkownika usługi w interfejsie aplikacji. W tym celu potwierdź zmiany informacji o koncie użytkownika usługi za pomocą hasła KLAdmin.
8. Na liście **Uprawnienia** zaznacz pola obok działań, które wybrany użytkownik lub grupa będą mogli wykonywać bez pytania o podanie hasła.

   Jeśli pole jest odznaczone, użytkownicy nie mogą wykonywać tego działania. Na przykład, jeśli pole obok uprawnienia **Zakończenie działania aplikacji** jest odznaczone, możesz zakończyć działanie aplikacji tylko wtedy, gdy jesteś zalogowany jako KLAdmin lub jako pojedynczy użytkownik, który posiada wymagane uprawnienie, lub jeśli wprowadzisz hasło tymczasowe.

   Uprawnienia Ochrony hasłem obejmują pewne ważne aspekty, które należy rozważyć. Upewnij się, że wszystkie warunki dla uzyskania dostępu do Kaspersky Endpoint Security zostaną spełnione.
9. Kliknij **Dodaj**.
10. Zapisz swoje zmiany.

Jak nadawać uprawnienia użytkownikom indywidualnym lub grupom w interfejsie użytkownika aplikacji

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Interfejs**.
3. W tabeli konta kliknij **Dodaj**.
4. Wybierz typ konta użytkownika, który chcesz dodać:
   - **Wybierz użytkownika/grupę z Active Directory** – konta użytkownika Active Directory.

     Aby wybrać konto użytkownika, kliknij przycisk **Wybierz użytkownika lub grupę**. Wybierz użytkownika lub grupę w Active Directory i potwierdź swój wybór.
   - **Dodaj użytkownika ręcznie** dla ręcznie dodanego konta użytkownika usługi.

     Aby dodać konto użytkownika usługi, wprowadź nazwę użytkownika i hasło (na przykład, SecureAdmin).

     > Możesz zresetować hasło do konta użytkownika usługi w ustawieniach zasad. Hasło konta użytkownika usługi resetuje się w ten sam sposób, co hasło konta KLAdmin. Jeśli edytowanie ustawień ochrony hasłem jest dozwolone („blokada" jest otwarta) lub na komputerze nie są stosowane żadne zasady, możesz zresetować hasło konta użytkownika usługi w interfejsie aplikacji. W tym celu potwierdź zmiany informacji o koncie użytkownika usługi za pomocą hasła KLAdmin.
5. Na liście **Uprawnienia** zaznacz pola obok działań, które wybrany użytkownik lub grupa będą mogli wykonywać bez pytania o podanie hasła.

   Jeśli pole jest odznaczone, użytkownicy nie mogą wykonywać tego działania. Na przykład, jeśli pole obok uprawnienia **Zakończenie działania aplikacji** jest odznaczone, możesz zakończyć działanie aplikacji tylko wtedy, gdy jesteś zalogowany jako KLAdmin lub jako pojedynczy użytkownik, który posiada wymagane uprawnienie, lub jeśli wprowadzisz hasło tymczasowe.

   > Uprawnienia Ochrony hasłem obejmują pewne ważne aspekty, które należy rozważyć. Upewnij się, że wszystkie warunki dla uzyskania dostępu do Kaspersky Endpoint Security zostaną spełnione.
6. Zapisz swoje zmiany.

W wyniku tego działania, jeśli dostęp do aplikacji zostanie ograniczony dla grupy Każda, użytkownicy będą mieli uprawnienia dostępu do Kaspersky Endpoint Security zgodnie z pojedynczymi uprawnieniami użytkowników.

Używanie hasła tymczasowego do nadawania uprawnień

Hasło tymczasowe może zostać użyte do nadania tymczasowego dostępu do Kaspersky Endpoint Security dla pojedynczego komputera poza siecią firmową. Jest to konieczne do zezwolenia użytkownikowi na wykonanie zablokowanego działania bez uzyskania danych uwierzytelniających konta KLAdmin. Aby użyć hasła tymczasowego, komputer musi zostać dodany do Kaspersky Security Center.

Jak zezwolić użytkownikowi na wykonanie zablokowanego działania, korzystając z hasła tymczasowego w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Kliknij dwukrotnie komputer, aby otworzyć okno właściwości komputera.
5. W oknie ustawień komputera wybierz sekcję **Aplikacje**.
6. Na liście aplikacji Kaspersky zainstalowanych na komputerze wybierz **Kaspersky Endpoint Security for Windows (14.1)** i kliknij ją dwukrotnie, aby otworzyć właściwości aplikacji.
7. W oknie ustawień aplikacji wybierz **Ustawienia ogólne → Interfejs**.
8. W sekcji **Ochrona hasłem** kliknij przycisk **Ustawienia**.
9. W oknie, które się otworzy, w bloku **Hasło tymczasowe**, kliknij przycisk **Lista haseł tymczasowych**.

   Otwiera się okno zarządzania hasłami tymczasowymi.
10. Kliknij **Dodaj**.
11. W polu **Data wygaśnięcia** określ datę wygaśnięcia hasła tymczasowego.
12. W tabeli **Zakres hasła tymczasowego** zaznacz pola obok działań, które będą dostępne dla użytkownika po wprowadzeniu hasła tymczasowego.
13. Kliknij **Wygeneruj**.

    Zostanie otwarte okno zawierające hasło tymczasowe (patrz rysunek poniżej).
14. Skopiuj hasło i dostarcz je użytkownikowi.

Jak zezwolić użytkownikowi na wykonanie zablokowanego działania, korzystając z hasła tymczasowego w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasoby (urządzenia)**.
2. Kliknij nazwę komputera, na którym chcesz zezwolić użytkownikowi na wykonywanie zablokowanego działania.
3. Wybierz zakładkę **Aplikacje**.
4. Kliknij **Kaspersky Endpoint Security for Windows**.

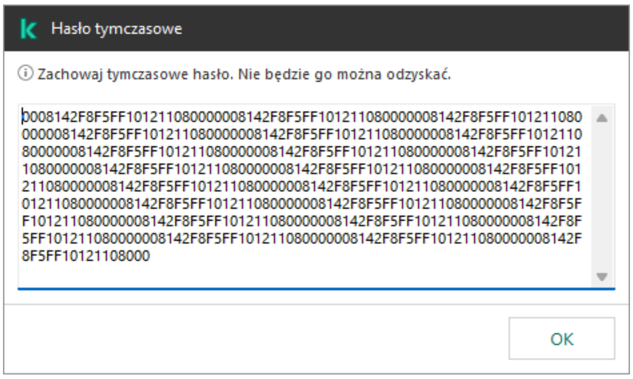
   Spowoduje to otwarcie lokalnych ustawień aplikacji.
5. Wybierz zakładkę **Ustawienia aplikacji**.
6. W oknie ustawień aplikacji wybierz **Ustawienia ogólne → Interfejs**.
7. W sekcji **Hasła tymczasowe** kliknij przycisk **Dodaj**.
8. W polu **Data wygaśnięcia** określ datę wygaśnięcia hasła tymczasowego.

9. W tabeli **Zakres hasła tymczasowego** zaznacz pola obok działań, które będą dostępne dla użytkownika po wprowadzeniu hasła tymczasowego.

10. Kliknij **Wygeneruj**.

    Zostanie otwarte okno zawierające hasło tymczasowe.

11. Skopiuj hasło i dostarcz je użytkownikowi.



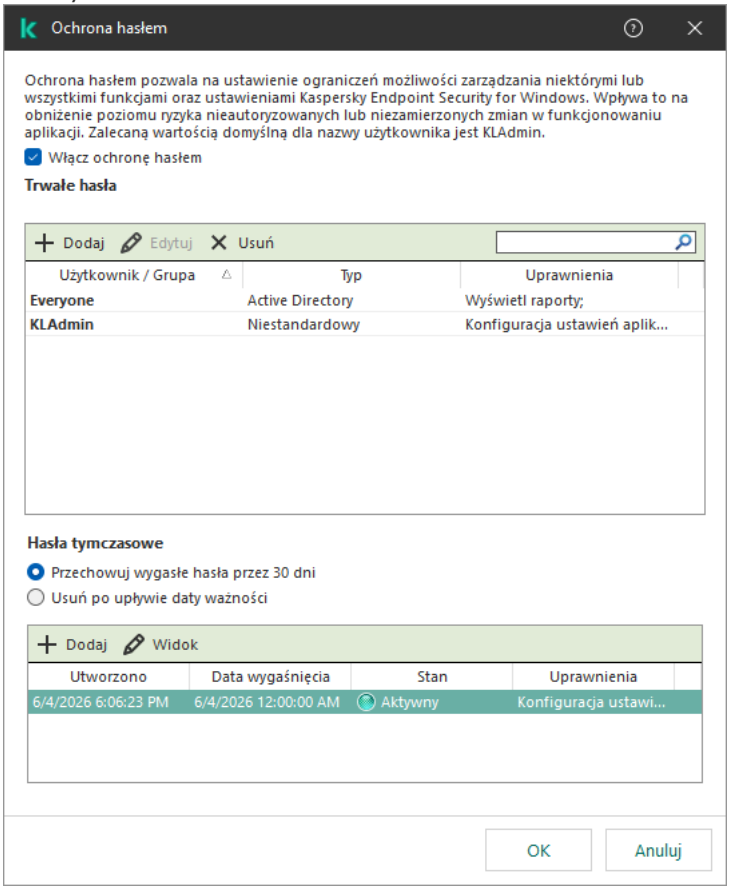
Hasło tymczasowe

Unieważnienie tymczasowego hasła

Począwszy od wersji 12.9 Kaspersky Endpoint Security for Windows obejmuje *Zarządzanie hasłami tymczasowymi*. Zarządzanie hasłami tymczasowymi umożliwia wykonywanie następujących czynności:

- Zapisywanie historii haseł (do 30 dni).
- Monitorowanie tymczasowego statusu hasła: *Aktywny*, *Utraciła ważność*, *Odwołany*.

- Unieważnianie haseł tymczasowych.



Zarządzanie hasłami tymczasowymi

Zarządzanie hasłami tymczasowymi umożliwia aktualizację statusu hasła i unieważnienie hasła wyłącznie po synchronizacji komputera z Kaspersky Security Center.

Jak unieważnić hasło tymczasowe za pomocą Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Kliknij dwukrotnie komputer, aby otworzyć okno właściwości komputera.
5. W oknie ustawień komputera wybierz sekcję **Aplikacje**.
6. Na liście aplikacji Kaspersky zainstalowanych na komputerze wybierz **Kaspersky Endpoint Security for Windows (14.1)** i kliknij ją dwukrotnie, aby otworzyć właściwości aplikacji.
7. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Interfejs**.
8. W sekcji **Ochrona hasłem** kliknij przycisk **Ustawienia**.
9. Otwiera się okno; w tym oknie pod **Hasło tymczasowe** skonfiguruj ustawienia przechowywania wygasłych haseł.
10. Kliknij **Lista haseł tymczasowych**.

    Otwiera się okno zarządzania hasłami tymczasowymi. Zarządzanie hasłami tymczasowymi wyświetla datę wygaśnięcia hasła, jego status i listę uprawnień.

11. Wybierz aktywne hasło tymczasowe, które chcesz unieważnić, i kliknij je dwukrotnie, aby otworzyć jego właściwości.

12. W otwartym oknie kliknij przycisk **Wycofaj**.

13. Zapisz swoje zmiany. Aby zastosować zasady na komputerach, zamknij kłódki .

Jak unieważnić hasło tymczasowe w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

2. Kliknij nazwę komputera, na którym chcesz zezwolić użytkownikowi na wykonywanie zablokowanego działania.

3. Wybierz zakładkę **Aplikacje**.

4. Kliknij **Kaspersky Endpoint Security for Windows**.

   Spowoduje to otwarcie lokalnych ustawień aplikacji.

5. Wybierz zakładkę **Ustawienia aplikacji**.

6. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Interfejs**.

7. Pod **Hasła tymczasowe** skonfiguruj przechowywanie wygasłych haseł.

8. Kliknij odnośnik **Hasło tymczasowe**.

   Otwiera się okno zarządzania hasłami tymczasowymi. Zarządzanie hasłami tymczasowymi wyświetla datę wygaśnięcia hasła, jego status i listę uprawnień.

9. Wybierz aktywne hasło tymczasowe, które chcesz unieważnić.

10. W otwartym oknie kliknij przycisk **Wycofaj hasło**.

11. Zapisz swoje zmiany. Aby zastosować zasady na komputerach, zamknij kłódki .

Zarządzanie hasłami tymczasowymi ustawia status hasła na *Wycofywanie (synchronizacja z hostem)*. Po zsynchronizowaniu komputera z Kaspersky Security Center aplikacja natychmiast unieważnia tymczasowe hasło i blokuje przyznane uprawnienia.

Specjalne kwestie dotyczące uprawnień Ochrony hasłem

Uprawnienia Ochrony hasłem obejmują pewne ważne aspekty i ograniczenia, które należy rozważyć.

Konfiguracja ustawień aplikacji

Jeśli komputer użytkownika działa pod kontrolą profilu, upewnij się, że wszystkie wymagane ustawienia w profilu są dostępne do edycji (atrybuty są otwarte).

Zakończenie działania aplikacji

Nie ma żadnych specjalnych kwestii ani ograniczeń.

Wyłączenie składników ochrony

- Nie można przyznać uprawnienia do wyłączenia składników ochrony dla grupy Wszyscy. Aby zezwolić użytkownikom innym niż KLAdmin na wyłączenie składników kontroli, dodaj użytkownika lub grupę, który/która posiada uprawnienie **Wyłączenie składników ochrony** w ustawieniach Ochrony hasłem.
- Jeśli komputer użytkownika działa pod kontrolą profilu, upewnij się, że wszystkie wymagane ustawienia w profilu są dostępne do edycji (atrybuty są otwarte).
- Aby wyłączyć składniki ochrony w ustawieniach aplikacji, użytkownik musi mieć uprawnienie **Konfiguracja ustawień aplikacji**.
- Aby wyłączyć składniki ochrony z poziomu menu kontekstowego (korzystając z elementu menu **Wstrzymaj ochronę**), użytkownik musi mieć uprawnienie **Wyłączenie składników ochrony** jako dodatek do uprawnienia **Wyłączenie składników kontroli**.

Wyłączenie składników kontroli

- Nie można przyznać uprawnienia do wyłączenia składników kontroli dla grupy Wszyscy. Aby zezwolić użytkownikom innym niż KLAdmin na wyłączenie składników kontroli, dodaj użytkownika lub grupę, który/która posiada uprawnienie **Wyłączenie składników kontroli** w ustawieniach Ochrony hasłem.
- Jeśli komputer użytkownika działa pod kontrolą profilu, upewnij się, że wszystkie wymagane ustawienia w profilu są dostępne do edycji (atrybuty są otwarte).
- Aby wyłączyć składniki kontroli w ustawieniach aplikacji, użytkownik musi mieć uprawnienie **Konfiguracja ustawień aplikacji**.
- Aby wyłączyć składniki kontroli z poziomu menu kontekstowego (korzystając z elementu menu **Wstrzymaj ochronę**), użytkownik musi mieć uprawnienie **Wyłączenie składników kontroli** jako dodatek do uprawnienia **Wyłączenie składników ochrony**.

Wyłącz zasadę Kaspersky Security Center

Nie możesz udzielić grupie „Wszyscy” uprawnienia do wyłączenia profilu Kaspersky Security Center. Aby zezwolić użytkownikom innym niż KLAdmin na wyłączenie zasady, dodaj użytkownika lub grupę, który/która posiada uprawnienie **Wyłącz zasadę Kaspersky Security Center** w ustawieniach Ochrony hasłem.

Usuwanie klucza

Nie ma żadnych specjalnych kwestii ani ograniczeń.

Dezinstalacja / modyfikacja / przywracanie aplikacji

Jeśli posiadasz dozwolone usuwanie, modyfikowanie i przywracanie aplikacji dla grupy „Wszystkie", Kaspersky Endpoint Security nie wymaga podania hasła podczas próby wykonania tych działań przez użytkownika. Dlatego każdy użytkownik, także użytkownicy spoza domeny, może zainstalować, zmodyfikować lub przywrócić aplikację.

Przywracanie dostępu do danych na zaszyfrowanych dyskach

Możesz odzyskać dostęp do danych na zaszyfrowanych dyskach tylko wtedy, gdy jesteś zalogowany jako KLAdmin. Uprawnienie do wykonywania tego działania nie może zostać nadane żadnemu innemu użytkownikowi.

Wyświetl raporty

Nie ma żadnych specjalnych kwestii ani ograniczeń.

Przywróć z Kopii zapasowej

Nie ma żadnych specjalnych kwestii ani ograniczeń.

Eksportuj ustawienia

Domyślnie eksportowanie ustawień aplikacji jest zabronione dla grupy „Wszyscy". Ustawienia aplikacji można eksportować, korzystając z konta użytkownika KLAdmin. Eksportowanie ustawień aplikacji obejmuje tylko tworzenie pliku konfiguracyjnego z ustawieniami Kaspersky Endpoint Security w interfejsie aplikacji. Uprawnienie to nie ogranicza eksportowania list wykluczeń ze skanowania, zaufanych adresów internetowych, zaufanych urządzeń ani innych list obsługiwanych przez składniki aplikacji.

Resetowanie hasła KLAdmin

Jeśli nie pamiętasz hasła do konta KLAdmin, możesz zresetować hasło we właściwościach zasady. Nie możesz zresetować hasła w interfejsie aplikacji.

Możesz przeprowadzić działania mające na celu ochronę hasłem, korzystając z hasła tymczasowego. W tym przypadku nie musisz wprowadzać poświadczeń konta KLAdmin.

Jeśli komputer nie jest połączony z Kaspersky Security Center, a Ty zapomniałeś hasło do konta KLAdmin, nie ma możliwości odzyskania hasła.

Jak zresetować hasło do konta KLAdmin przy użyciu Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Interfejs**.
4. W sekcji **Ochrona hasłem** kliknij przycisk **Ustawienia**.
5. W otwartym oknie odznacz pole **Włącz ochronę hasłem**.
6. Zapisz swoje zmiany.
7. Zaznacz ponownie pole **Włącz ochronę hasłem**.
8. Kliknij **OK**.
   To spowoduje otwarcie okna dla hasła administratora.
9. Określ nowe hasło dla konta KLAdmin i potwierdź je.
10. Zapisz swoje zmiany.

Jak zresetować hasło do konta KLAdmin w konsoli Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Wybierz komputer, dla którego chcesz skonfigurować lokalne ustawienia aplikacji.
   Spowoduje to otwarcie właściwości komputera.
3. Wybierz zakładkę **Aplikacje**.
4. Kliknij **Kaspersky Endpoint Security for Windows**.
   Spowoduje to otwarcie lokalnych ustawień aplikacji.
5. Wybierz zakładkę **Ustawienia aplikacji**.
6. Wybierz **Ustawienia ogólne** → **Autoochrona**.
7. W menu **Ochrona hasłem**, Wyłącz przełącznik **Ochrona hasłem**.
8. Zapisz swoje zmiany.
9. Ponownie ustaw przełącznik **Ochrona hasłem** na pozycję włączenia.

10. Określ nowe hasło dla konta KLAdmin i potwierdź je.

11. Zapisz swoje zmiany.

W wyniku tego działania, hasło do Twojego konta KLAdmin zostanie zaktualizowane po zastosowaniu zasady.

Ochrona połączenia z Serwerem administracyjnym

Połączenie między komputerem a Serwerem administracyjnym jest realizowane przez składnik *Agenta sieciowego* oprogramowania Kaspersky Security Center. Jeżeli przestępca będzie mieć uprawnienia pozwalające mu na zmianę ustawień połączenia z serwerem, komputer użytkownika będzie narażony na niebezpieczeństwo połączenia z niezaufanym serwerem. Dzięki temu przestępca mógłby zastosować własne zasady grupowe, na przykład aby wyłączyć mechanizmy autoochrony aplikacji. Program Kaspersky Endpoint Security może zapobiegać nieautoryzowanemu połączeniu komputera z innym serwerem. Aby chronić połączenie z serwerem, aplikacja zaleca ustawienie hasła i używanie funkcji Password-Based key Derivation Function (PBKDF2). W rezultacie dostęp do aplikacji bez hasła jest niemożliwy.

Aby zapewnić kompleksową ochronę Kaspersky Endpoint Security i Agenta sieciowego przed nieautoryzowanym dostępem, zalecamy włączenie dodatkowej ochrony. W przypadku Kaspersky Endpoint Security zalecamy włączenie ochrony hasłem. W celu ochrony Agenta sieciowego zalecamy ustawienie hasła do dezinstalacji. Szczegółowe informacje na temat ochrony przed usunięciem Agenta sieciowego można znaleźć w pomocy do Kaspersky Security Center.

Połączeniem komputera z Serwerem administracyjnym zarządza się za pomocą zadania *Ochrona połączenia z Serwerem administracyjnym*. Zadanie umożliwia wykonywanie następujących działań:

- Ustawienie hasła do ochrony połączenia z serwerem.
- Zmiana hasła.
- Ponowne łączenie komputera z innym serwerem.
- Wyłączanie ochrony połączenia z serwerem.

Uwierzytelnianie komputera podczas nawiązywania połączenia z Serwerem administracyjnym

Po ustawieniu hasła aplikacja tworzy tablicę danych, wykorzystując funkcję PBKDF2 do przekształcenia hasła. Tablica jest następnie szyfrowana za pomocą klucza Agenta sieciowego. Aplikacja wykorzystuje zaszyfrowaną tablicę danych do sprawdzania praw i uprawnień Serwera administracyjnego do nawiązywania kolejnych połączeń.

Przy kolejnych próbach połączenia komputera z Serwerem administracyjnym aplikacja odszyfrowuje tablicę danych przy użyciu klucza Agenta sieciowego i porównuje ją z lokalną kopią. Jeśli nie są zgodne, dostęp do aplikacji jest ograniczony.

Ochrona połączenia z Serwerem administracyjnym

Jak ustawić hasło do ochrony połączenia z serwerem w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Ochrona połączenia z Serwerem administracyjnym**.

Krok 2. Ochrona połączenia z Serwerem administracyjnym

Ustaw hasło, które będzie zabezpieczać połączenie z Serwerem administracyjnym:

1. W obszarze **Ochrona połączenia z Serwerem administracyjnym** wybierz **Chroń za pomocą hasła**.

2. Z listy rozwijalnej **Serwer administracyjny** wybierz **Nowy serwer**.

3. W polu **Hasło do połączenia z Serwerem administracyjnym** wprowadź hasło do połączenia z Serwerem administracyjnym i potwierdź je.

   Jeżeli zapomnisz hasła, możesz je zmienić za pomocą odpowiedniego zadania.

4. Jeśli masz wdrożoną aplikację Kaspersky Endpoint Security 12.7 lub jej starszą wersję, zaznacz pole wyboru **Włącz zgodność szyfrowania hasła dla poprzednich wersji aplikacji (12.7 i starszych)**.

   Począwszy od wersji Kaspersky Endpoint Security for Windows 12.8, aplikacja stosuje silniejsze szyfrowanie haseł. Jeśli masz wdrożoną wersję Kaspersky Endpoint Security 12.8 lub nowszą, zaleca się usunięcie zaznaczenia tego pola i użycie silniejszego szyfrowania haseł. Wcześniejsze wersje aplikacji nie obsługują silnego szyfrowania haseł. Aby uruchomić zadanie, musisz zaznaczyć pole wyboru.

Krok 3. Wybieranie konta do uruchomienia zadania

Wybierz **Konto domyślne**. Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

Krok 4. Konfigurowanie terminarza uruchamiania zadania

W obszarze **Zaplanowane uruchomienie** wybierz **Ręcznie**.

Krok 5. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład *Hasło do połączenia z serwerem głównym*.

Krok 6. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora** lub uruchom zadanie ręcznie. Możesz monitorować postęp zadania we właściwościach zadania.

Jak ustawić hasło do ochrony połączenia z serwerem w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Ochrona połączenia z Serwerem administracyjnym**.

   c. W polu **Nazwa zadania** wpisz krótki opis, na przykład *Hasło do połączenia z serwerem głównym*.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.

5. Wybierz domyślne konto użytkownika. Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

6. Zakończ działanie Kreatora.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij zadanie **Ochrona połączenia z Serwerem administracyjnym** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

8. Wybierz zakładkę **Ustawienia aplikacji**.

9. W obszarze **Ochrona połączenia z Serwerem administracyjnym** wybierz **Chroń za pomocą hasła**.

10. Z listy rozwijalnej **Połączenie z Serwerem administracyjnym** wybierz **Nowe hasło**.

11. W polu **Hasło** wprowadź hasło do połączenia z Serwerem administracyjnym i potwierdź je.

    Jeżeli zapomnisz hasła, możesz je zmienić za pomocą odpowiedniego zadania.

12. Jeśli masz wdrożoną aplikację Kaspersky Endpoint Security 12.7 lub jej starszą wersję, zaznacz pole wyboru **Włącz zgodność szyfrowania hasła dla poprzednich wersji aplikacji (12.7 i starszych)**.

    Począwszy od wersji Kaspersky Endpoint Security for Windows 12.8, aplikacja stosuje silniejsze szyfrowanie haseł. Jeśli masz wdrożoną wersję Kaspersky Endpoint Security 12.8 lub nowszą, zaleca się usunięcie zaznaczenia tego pola i użycie silniejszego szyfrowania haseł. Wcześniejsze wersje aplikacji nie obsługują silnego szyfrowania haseł. Aby uruchomić zadanie, musisz zaznaczyć pole wyboru.

13. Zapisz swoje zmiany.

14. Zaznacz pole obok zadania.

15. Kliknij **Uruchom**.

Możesz monitorować stan zadania oraz liczbę urządzeń, na których to zadanie zostało wykonane pomyślnie lub zakończyło się błędem.

Ponowne łączenie komputera z Serwerem administracyjnym

Ponowne podłączenie komputera do innego Serwera administracyjnego obejmuje następujące kroki:

1. W konsoli bieżącego serwera `[KSC1]` uruchom zadanie *Zmiana Serwera administracyjnego* dla Agenta sieciowego.

   Po uruchomieniu zadania komputer zostanie ponownie podłączony do nowego serwera `[KSC2]`.

   Komputer będzie wyświetlany na konsoli serwera `[KSC1]` ze stanem *Krytyczny* 🖥️. Konfiguracja aplikacji przy użyciu zasad lub zdalne uruchamianie zadań na komputerze jest niemożliwe.

2. W konsoli nowego serwera `[KSC2]` utwórz nowe zadanie *Ochrona połączenia z Serwerem administracyjnym* dla Kaspersky Endpoint Security. We właściwościach zadania wprowadź hasło poprzedniego serwera i ustaw hasło dla nowego serwera.

   Jak ustawić nowe hasło do połączenia z nowym serwerem w Konsoli administracyjnej (MMC)?

   1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

      Zostanie otwarta lista zadań.

   2. Kliknij **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1) → Ochrona połączenia z Serwerem administracyjnym**.

Krok 2. Ochrona połączenia z Serwerem administracyjnym

Ustaw hasło w celu ochrony połączenia z nowym serwerem administracyjnym:

1. W obszarze **Ochrona połączenia z Serwerem administracyjnym** wybierz **Chroń za pomocą hasła**.
2. Z listy rozwijalnej **Serwer administracyjny** wybierz **Połącz się ponownie z innego serwera**.
3. W polu **Bieżące hasło** wprowadź hasło ustawione dla połączenia z poprzednio używanym zaufanym serwerem.
4. W polu **Nowe hasło** wprowadź hasło do połączenia z nowym Serwerem administracyjnym i potwierdź je.

   Jeżeli zapomnisz hasła, możesz je zmienić za pomocą odpowiedniego zadania.
5. Jeśli masz wdrożoną aplikację Kaspersky Endpoint Security 12.7 lub jej starszą wersję, zaznacz pole wyboru **Włącz zgodność szyfrowania hasła dla poprzednich wersji aplikacji (12.7 i starszych)**.

   Począwszy od wersji Kaspersky Endpoint Security for Windows 12.8, aplikacja stosuje silniejsze szyfrowanie haseł. Jeśli masz wdrożoną wersję Kaspersky Endpoint Security 12.8 lub nowszą, zaleca się usunięcie zaznaczenia tego pola i użycie silniejszego szyfrowania haseł. Wcześniejsze wersje aplikacji nie obsługują silnego szyfrowania haseł. Aby uruchomić zadanie, musisz zaznaczyć pole wyboru.

Krok 3. Wybieranie konta do uruchomienia zadania

Wybierz **Konto domyślne**. Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

Krok 4. Konfigurowanie terminarza uruchamiania zadania

W obszarze **Zaplanowane uruchomienie** wybierz **Ręcznie**.

Krok 5. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład *Hasło do połączenia z serwerem głównym*.

Krok 6. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora** lub uruchom zadanie ręcznie. Możesz monitorować postęp zadania we właściwościach zadania.

Jak ustawić nowe hasło do połączenia z nowym serwerem w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Ochrona połączenia z Serwerem administracyjnym**.

   c. W polu **Nazwa zadania** wpisz krótki opis, na przykład *Hasło do połączenia z serwerem głównym*.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.

5. Wybierz domyślne konto użytkownika. Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

6. Zakończ działanie Kreatora.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij zadanie **Ochrona połączenia z Serwerem administracyjnym** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

8. Wybierz zakładkę **Ustawienia aplikacji**.

9. W obszarze **Ochrona połączenia z Serwerem administracyjnym** wybierz **Chroń za pomocą hasła**.

10. Z listy rozwijalnej **Połączenie z Serwerem administracyjnym** wybierz **Połącz się ponownie z innego serwera**.

11. W polu **Bieżące hasło** wprowadź hasło ustawione dla połączenia z poprzednio używanym zaufanym serwerem.

12. W polu **Nowe hasło** wprowadź hasło do połączenia z nowym Serwerem administracyjnym i potwierdź je.

    Jeżeli zapomnisz hasła, możesz je zmienić za pomocą odpowiedniego zadania.

13. Jeśli masz wdrożoną aplikację Kaspersky Endpoint Security 12.7 lub jej starszą wersję, zaznacz pole wyboru **Włącz zgodność szyfrowania hasła dla poprzednich wersji aplikacji (12.7 i starszych)**.

    Począwszy od wersji Kaspersky Endpoint Security for Windows 12.8, aplikacja stosuje silniejsze szyfrowanie haseł. Jeśli masz wdrożoną wersję Kaspersky Endpoint Security 12.8 lub nowszą, zaleca się usunięcie zaznaczenia tego pola i użycie silniejszego szyfrowania haseł. Wcześniejsze wersje aplikacji nie obsługują silnego szyfrowania haseł. Aby uruchomić zadanie, musisz zaznaczyć pole wyboru.

14. Zapisz swoje zmiany.

15. Zaznacz pole obok zadania.

16. Kliknij **Uruchom**.

    Możesz monitorować stan zadania oraz liczbę urządzeń, na których to zadanie zostało wykonane pomyślnie lub zakończyło się błędem.

Po wykonaniu zadania upewnij się, że w konsoli nowego serwera `[KSC2]` komputer ma status *OK*. Przetestuj, czy możesz zdalnie uruchamiać zadania i konfigurować aplikację za pomocą zasad.

Resetowanie hasła połączenia z Serwerem administracyjnym

Jeśli nie pamiętasz hasła do połączenia z Serwerem administracyjnym lub hasło zostało ujawnione, możesz zresetować hasło we właściwościach zadania. Możesz także zresetować hasło i ustawić nowe hasło dla grupy komputerów o różnych stanach ochrony połączenia z Serwerem administracyjnym. Oznacza to, że jeśli na niektórych komputerach ochrona jest włączona, a na innych wyłączona, zadanie ustawia hasło dla wszystkich komputerów.

Hasło połączenia z Serwerem administracyjnym można resetować tylko w konsoli zaufanego serwera, do którego podłączony jest komputer.

Jak zresetować połączenie z Serwerem administracyjnym przy użyciu Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zadania**.
3. Wybierz zadanie **Ochrona połączenia z Serwerem administracyjnym** i kliknij je dwukrotnie, aby otworzyć właściwości zadania.
4. W oknie właściwości zadania wybierz sekcję **Ustawienia**.
5. W obszarze **Ochrona połączenia z Serwerem administracyjnym** wybierz **Chroń i zmień hasło**.
6. W polu **Hasło do połączenia z Serwerem administracyjnym** ustaw nowe hasło do połączenia z obecnym zaufanym serwerem i potwierdź je.
7. Zapisz swoje zmiany.
8. Uruchom zadanie.

Jak zresetować hasło do połączenia z Serwerem administracyjnym w konsoli Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.
2. Kliknij zadanie **Ochrona połączenia z Serwerem administracyjnym** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. W obszarze **Ochrona połączenia z Serwerem administracyjnym** wybierz **Chroń i zmień hasło**.
5. W polu **Hasło** ustaw nowe hasło do połączenia z obecnym zaufanym serwerem i potwierdź je.

6. Zapisz swoje zmiany.
7. Zaznacz pole obok zadania.
8. Kliknij **Uruchom**.

W rezultacie hasło połączenia z Serwerem administracyjnym zostanie zresetowane po zakończeniu zadania.

Wyłączanie ochrony połączenia z Serwerem administracyjnym

Ochronę połączenia z Serwerem administracyjnym można wyłączyć zdalnie tylko w konsoli zaufanego serwera, do którego podłączony jest komputer. Możesz także wyłączyć ochronę lokalnie przy użyciu wiersza polecenia.

Jak wyłączyć ochronę połączenia z serwerem w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zadania**.
3. Wybierz zadanie **Ochrona połączenia z Serwerem administracyjnym** i kliknij je dwukrotnie, aby otworzyć właściwości zadania.
4. W oknie właściwości zadania wybierz sekcję **Ustawienia**.
5. W obszarze **Ochrona połączenia z Serwerem administracyjnym** wybierz **Nie chroń**.
6. Zapisz swoje zmiany.
7. Uruchom zadanie.

   Możesz monitorować stan zadania oraz liczbę urządzeń, na których to zadanie zostało wykonane pomyślnie lub zakończyło się błędem.

Jak wyłączyć ochronę połączenia z serwerem w Web Console i Cloud Console

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.
2. Kliknij zadanie **Ochrona połączenia z Serwerem administracyjnym** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. W obszarze **Ochrona połączenia z Serwerem administracyjnym** wybierz **Nie chroń**.
5. Zapisz swoje zmiany.
6. Zaznacz pole obok zadania.

7. Kliknij **Uruchom**.

   Możesz monitorować stan zadania oraz liczbę urządzeń, na których to zadanie zostało wykonane pomyślnie lub zakończyło się błędem.

Jak wyłączyć ochronę połączenia z serwerem w wierszu poleceń

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   gdzie `<password>` to hasło konta użytkownika KL Admin lub hasło z zadania *Ochrona połączenia z Serwerem administracyjnym*. Jeśli nie określono parametru, Kaspersky Endpoint Security wyświetli monit o wprowadzenie hasła w następnym wierszu.

   > Aby wykonać to polecenie, Ochrona hasłem musi być włączona.

Na przykład

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

Szyfrowanie danych

Kaspersky Endpoint Security umożliwia szyfrowanie plików i folderów przechowywanych na dyskach lokalnych i nośnikach wymiennych lub wszystkich nośnikach wymiennych i dyskach twardych. Szyfrowanie danych minimalizuje ryzyko wycieku informacji, co może mieć miejsce, gdy komputer przenośny, nośnik wymienny lub dysk twardy zostanie zgubiony bądź skradziony lub gdy dostęp do danych jest uzyskiwany przez nieautoryzowanych użytkowników lub aplikacje. Kaspersky Endpoint Security używa algorytmu szyfrowania Advanced Encryption Standard AES (Advanced Encryption Standard).

Jeśli licencja utraciła ważność, aplikacja nie szyfruje nowych danych, a stare zaszyfrowane dane pozostają zaszyfrowane i dostępne do użycia. W tej sytuacji szyfrowanie nowych danych wymaga aktywacji aplikacji z nową licencją zezwalającą na korzystanie z szyfrowania.

Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze opartym na architekturze Arm, dostępne jest tylko szyfrowanie dysków funkcją BitLocker. Aplikacja nie obsługuje innych komponentów szyfrowania danych.

Jeśli licencja utraciła ważność, postanowienia Umowy licencyjnej zostały naruszone lub klucz licencyjny, program Kaspersky Endpoint Security bądź moduły szyfrujące zostały usunięte, stan zaszyfrowany wcześniej zaszyfrowanych plików nie zostanie zagwarantowany. Dzieje się tak, ponieważ niektóre aplikacje, takie jak Microsoft Office Word, podczas modyfikacji tworzą tymczasowe kopie plików. Po zapisaniu oryginalnego pliku, tymczasowa kopia zastępuje oryginalny plik. W rezultacie, na komputerze, na którym nie ma żadnej lub dostępnej funkcji szyfrowania, plik pozostanie niezaszyfrowany.

Kaspersky Endpoint Security oferuje następujące aspekty ochrony danych:

- **Szyfrowanie na poziomie plików na lokalnych dyskach komputera**. Możesz tworzyć listy plików według rozszerzenia lub grup rozszerzeń oraz listy folderów przechowywanych na lokalnych dyskach komputera, a także tworzyć reguły szyfrowania plików, które są tworzone przez określone aplikacje. Po zastosowaniu zasady, Kaspersky Endpoint Security zaszyfruje i odszyfruje następujące pliki:
  - Pliki pojedynczo dodane do list elementów przeznaczonych do zaszyfrowania i odszyfrowania;
  - Pliki przechowywane w folderach dodanych do list elementów przeznaczonych do zaszyfrowania i odszyfrowania;
  - Pliki utworzone przez oddzielne aplikacje.
- **Szyfrowanie dysków wymiennych**. Możesz określić domyślną regułę szyfrowania, zgodnie z którą aplikacja stosuje tę samą akcję do wszystkich dysków wymiennych lub określić reguły szyfrowania dla pojedynczych dysków wymiennych.

  Domyślna reguła szyfrowania ma niższy priorytet niż reguły szyfrowania utworzone dla pojedynczych dysków wymiennych. Reguły szyfrowania utworzone dla dysków wymiennych z określonym modelem urządzenia mają niższy priorytet niż reguły szyfrowania, utworzone dla dysków wymiennych z określonym kodem ID urządzenia.

Aby wybrać regułę szyfrowania dla plików na nośniku wymiennym, Kaspersky Endpoint Security sprawdza, czy model i kod ID urządzenia są znane. Następnie aplikacja wykonuje jedną z poniższych czynności:

- Jeśli tylko model urządzenia jest znany, aplikacja używa reguły szyfrowania (jeśli istnieje), utworzonej dla dysków wymiennych o określonym modelu urządzenia.
- Jeśli tylko ID urządzenia jest znane, aplikacja używa reguły szyfrowania (jeśli istnieje), utworzonej dla dysków wymiennych o określonym ID urządzenia.
- Jeśli model i ID urządzenia są znane, aplikacja stosuje regułę szyfrowania (jeśli istnieje), utworzoną dla dysków wymiennych o określonym ID urządzenia. Jeśli nie istnieje taka reguła, ale istnieje reguła szyfrowania utworzona dla nośników wymiennych o określonym modelu urządzenia, aplikacja zastosuje tę regułę. Jeśli dla określonego ID urządzenia i określonego modelu urządzenia nie określono żadnej reguły szyfrowania, aplikacja zastosuje domyślną regułę szyfrowania.
- Jeśli nie jest znany model i kod ID urządzenia, aplikacja używa domyślnej reguły szyfrowania.

Aplikacja umożliwia przygotowanie dysku wymiennego do używania w trybie przenośnym przechowywanych na nim zaszyfrowanych danych. Po włączeniu trybu przenośnego, użytkownik może uzyskać dostęp do zaszyfrowanych plików na dyskach wymiennych podłączonych do komputera bez funkcji szyfrowania.

- **Zarządzanie regułami dostępu aplikacji do zaszyfrowanych plików**. Dla dowolnej aplikacji użytkownik może utworzyć regułę dostępu do zaszyfrowanego pliku, która zablokuje dostęp do zaszyfrowanych plików lub zezwoli na dostęp do zaszyfrowanych plików tylko jako tekst zaszyfrowany, który jest sekwencją znaków uzyskanych w momencie stosowania szyfrowania.
- **Tworzenie zaszyfrowanych pakietów**. Możesz utworzyć zaszyfrowane archiwa i chronić dostęp do takich archiwów przy pomocy hasła. Dostęp do zawartości zaszyfrowanych archiwów można uzyskać tylko poprzez wprowadzenie haseł, przy pomocy których chroniony jest dostęp do tych archiwów. Takie archiwa można bezpiecznie przesyłać poprzez sieci lub nośniki wymienne.
- **Szyfrowanie całego dysku**. Możesz wybrać technologię szyfrowania: Kaspersky Disk Encryption lub Szyfrowanie dysków funkcją BitLocker (zwana dalej również „BitLocker").

  BitLocker to technologia, która jest częścią systemu operacyjnego Windows. Jeśli komputer zawiera moduł Trusted Platform Module (TPM), BitLocker używa go do przechowywania kluczy dostępu, które umożliwiają uzyskanie dostępu do zaszyfrowanego dysku twardego. Po uruchomieniu komputera, BitLocker żąda od Trusted Platform Module kluczy odzyskiwania dysku twardego i odblokowuje dysk. Możesz skonfigurować korzystanie z hasła i/lub kodu PIN do uzyskania dostępu do kluczy odzyskiwania.

  Możesz określić domyślną regułę szyfrowania całego dysku oraz utworzyć listę dysków twardych wykluczonych z szyfrowania. Po zastosowaniu profilu Kaspersky Security Center, program Kaspersky Endpoint Security zaszyfruje cały dysk sektor po sektorze. Aplikacja szyfruje wszystkie logiczne partycje dysków twardych jednocześnie.

  Po zaszyfrowaniu dysków twardych, przy kolejnym uruchomieniu komputera użytkownik musi przejść proces autoryzacji przy użyciu Agenta autoryzacji przed uzyskaniem dostępu do dysków twardych i załadowaniem systemu operacyjnego. Wymaga to wprowadzenia hasła do tokena lub karty inteligentnej podłączonej do komputera, bądź wpisania nazwy użytkownika i hasła konta Agenta autoryzacji utworzonego przez administratora lokalnej sieci firmowej przy użyciu zadania *Zarządzanie kontami Agenta autoryzacji*. Konta te są oparte na kontach systemu Microsoft Windows, z poziomu których użytkownik loguje się do systemu operacyjnego. Możesz także użyć technologii Single Sign-On (SSO), która umożliwia automatyczne logowanie do systemu operacyjnego przy użyciu nazwy użytkownika i hasła dla konta Agenta autoryzacji.

Jeśli utworzysz kopie zapasowe danych komputera, a następnie zaszyfrujesz dane komputera, po czym przywrócisz kopie zapasowe danych komputera i ponownie zaszyfrujesz dane komputera, Kaspersky Endpoint Security utworzy kopie kont Agenta autoryzacji. Aby usunąć kopie kont, użyj narzędzia klmover z parametrem `dupfix`. Narzędzie klmover jest dostępne z programem Kaspersky Security Center. Więcej na temat działania tego narzędzia można znaleźć w systemie pomocy programu Kaspersky Security Center.

Dostęp do zaszyfrowanych dysków twardych jest możliwy tylko z poziomu komputerów, na których zainstalowany jest program Kaspersky Endpoint Security z funkcją szyfrowania całego dysku. Ten środek bezpieczeństwa minimalizuje ryzyko wycieku danych z zaszyfrowanego dysku twardego, gdy podjęta zostaje próba uzyskania dostępu do tego dysku spoza lokalnej sieci firmowej.

Aby zaszyfrować dyski twarde i nośniki wymienne, możesz użyć funkcji Zaszyfruj tylko używaną przestrzeń dyskową. Zalecane jest korzystanie z tej funkcji tylko w przypadku nowych urządzeń, które nie były wcześniej używane. Jeśli stosujesz szyfrowanie do urządzenia, które jest już w użyciu, zalecane jest zaszyfrowanie całego urządzenia. Zapewni to ochronę wszystkich danych, także tych usuniętych, gdyż mogą zawierać informacje, które można odzyskać.

Przed rozpoczęciem szyfrowania program Kaspersky Endpoint Security uzyskuje mapę sektorów systemu plików. Pierwszy etap szyfrowania obejmuje sektory zajmowane przez pliki w momencie rozpoczęcia szyfrowania. Drugi etap szyfrowania obejmuje sektory zapisane po rozpoczęciu szyfrowania. Po zakończeniu szyfrowania, wszystkie sektory zawierające dane zostają zaszyfrowane.

Po zakończeniu szyfrowania i usunięciu pliku przez użytkownika, sektory, w których był przechowywany usunięty plik, staną się niedostępne do przechowywania nowych informacji na poziomie systemu plików, ale pozostaną zaszyfrowane. Dlatego też, jeśli pliki są zapisywane na nowym urządzeniu, a urządzenie jest regularnie szyfrowane przy użyciu włączonej funkcji **Zaszyfruj tylko używaną przestrzeń dyskową**, wszystkie sektory zostaną zaszyfrowane po jakimś czasie.

Dane potrzebne do odszyfrowania plików są udostępniane przez Serwer administracyjny Kaspersky Security Center, który kontrolował komputer w momencie szyfrowania. Jeśli komputer z zaszyfrowanymi obiektami był z jakiegoś powodu zarządzany przez inny Serwer administracyjny, możesz uzyskać dostęp do zaszyfrowanych danych na jeden z następujących sposobów:

- Serwery administracyjne w tej samej hierarchii:
  - Nie musisz podejmować żadnych dodatkowych działań. Użytkownik zachowa dostęp do zaszyfrowanych obiektów. Klucze szyfrujące są dystrybuowane do wszystkich Serwerów administracyjnych.
- Oddzielne Serwery administracyjne:
  - Wyślij prośbę do administratora sieci LAN o dostęp do zaszyfrowanych obiektów.
  - Przywróć dane na zaszyfrowanych urządzeniach przy użyciu Narzędzia przywracania.
  - Przywróć z kopii zapasowej konfigurację Serwera administracyjnego Kaspersky Security Center kontrolującego komputer w momencie szyfrowania i użyj tej konfiguracji na Serwerze administracyjnym obecnie kontrolującym komputer z zaszyfrowanymi obiektami.

Jeśli nie ma dostępu do zaszyfrowanych danych, postępuj zgodnie ze specjalnymi instrukcjami dotyczącymi pracy z zaszyfrowanymi danymi (Przywracanie dostępu do zaszyfrowanych plików, Praca z zaszyfrowanymi urządzeniami, gdy nie ma do nich dostępu).

Ograniczenia funkcji szyfrowania

Szyfrowanie danych posiada następujące ograniczenia:

- Podczas szyfrowania aplikacja tworzy pliki usługi. Do ich przechowywania potrzeba około 0,5 % niepofragmentowanej, wolnej przestrzeni na dysku. Jeśli na dysku twardym nie ma wystarczającej ilości niepofragmentowanego, wolnego miejsca, szyfrowanie nie zostanie rozpoczęte, aż do zwolnienia wystarczającej ilości miejsca.

- Zarządzanie komponentami szyfrującymi wszystkie dane jest dostępne w Konsoli administracyjnej Kaspersky Security Center i w konsoli Kaspersky Security Center Web Console. W konsoli Kaspersky Security Center Cloud Console możesz tylko zarządzać BitLocker.

- Szyfrowanie danych jest dostępne tylko podczas używania Kaspersky Endpoint Security z systemem zarządzania Kaspersky Security Center lub Kaspersky Security Center Cloud Console (tylko BitLocker). Szyfrowanie danych podczas korzystania z Kaspersky Endpoint Security w trybie offline nie jest możliwe, ponieważ Kaspersky Endpoint Security przechowuje klucze szyfrowania w Kaspersky Security Center.

- Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Microsoft Windows dla serwerów, dostępne jest tylko szyfrowanie całego dysku przy użyciu technologii Szyfrowanie dysków funkcją BitLocker. Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych, funkcja szyfrowania danych jest w pełni dostępna.

- Jeśli Kaspersky Endpoint Security zainstalowano na komputerze z procesorem ARM, dostępne jest tylko pełne szyfrowanie dysku przy użyciu technologii szyfrowania dysków BitLocker. Inne komponenty szyfrowania nie są obsługiwane.

Szyfrowanie całego dysku przy użyciu technologii Kaspersky Disk Encryption jest niedostępne dla dysków twardych, które nie spełniają wymagań sprzętowych i programowych.

Kompatybilność funkcji szyfrowania całego dysku Kaspersky Endpoint Security z Kaspersky Anti-Virus dla UEFI nie jest obsługiwana. Kaspersky Anti-Virus dla UEFI uruchamia się przed załadowaniem systemu operacyjnego. Podczas korzystania z szyfrowania całego dysku aplikacja wykryje brak zainstalowanego systemu operacyjnego na komputerze. W rezultacie działanie Kaspersky Anti-Virus dla UEFI zakończy się błędem. Szyfrowanie na poziomie plików (FLE) nie wpływa na działanie programu Kaspersky Anti-Virus dla UEFI.

Kaspersky Endpoint Security obsługuje następujące konfiguracje:

- Dyski HDD, SSD i USB.

  Technologia Kaspersky Disk Encryption (FDE) obsługuje pracę z dyskami SSD, zapewniając działanie i okres użytkowania dysków SSD.

- Dyski podłączone poprzez magistralę: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.

- Dyski niewymienne podłączone poprzez magistralę SD lub MMC.

- Dyski z sektorami o pojemności 512 bajtów.

- Dyski z sektorami o pojemności 4096 bajtów, które emulują 512 bajtów.

- Dyski z następującym typem partycji: GPT, MBR i VBR (nośniki wymienne).
- Wbudowane oprogramowanie ze standardem UEFI 64 i Legacy BIOS.
- Wbudowane oprogramowanie ze standardem UEFI z obsługą Bezpiecznego rozruchu.

  Bezpieczny rozruch to technologia zaprojektowana do zweryfikowania podpisów cyfrowych dla sterowników i aplikacji UEFI loader. Bezpieczny rozruch blokuje uruchamianie sterowników i aplikacji w środowisku UEFI, które nie są podpisane lub są podpisane przez nieznanych wydawców. Kaspersky Disk Encryption (FDE) w pełni obsługuje Bezpieczny rozruch. Agent autoryzacji jest podpisany certyfikatem Microsoft Windows UEFI Driver Publisher.

  Na niektórych urządzeniach (na przykład: Microsoft Surface Pro i Microsoft Surface Pro 2), domyślnie zainstalowana może być przestarzała lista certyfikatów weryfikacji podpisów cyfrowych. Przed zaszyfrowaniem sterownika należy zaktualizować listę certyfikatów.
- Wbudowane oprogramowanie ze standardem UEFI z obsługą opcji Fast Boot.

  Fast Boot to technologia, która pomaga w szybszym uruchomieniu komputera. Jeśli technologia Fast Boot jest włączona, zazwyczaj komputer ładuje tylko minimalny zestaw sterowników UEFI wymaganych do uruchomienia systemu operacyjnego. Jeśli technologia Fast Boot jest włączona, klawiatury USB, mysz, tokeny USB, touchpady i ekrany dotykowe mogą nie działać, gdy uruchomiony jest Agent autoryzacji.

  > Aby użyć Kaspersky Disk Encryption (FDE), zalecane jest wyłączenie technologii Fast Boot. Aby sprawdzić działanie Kaspersky Disk Encryption (FDE), możesz użyć narzędzia FDE Test Utility.

Kaspersky Endpoint Security nie obsługuje następujących konfiguracji:

- Moduł ładujący rozruch znajduje się na jednym dysku, a system operacyjny na innym dysku.
- System zawiera oprogramowanie wbudowane w standardzie UEFI 32.
- System posiada technologię Intel® Rapid Start Technology i dyski, które posiadają partycję hibernacji nawet wtedy, gdy technologia Intel® Rapid Start Technology jest wyłączona.
- Dyski w formacie MBR z więcej niż 10 partycjami rozszerzonymi.
- System zawiera plik wymiany znajdujący się na dysku niesystemowym.
- Możliwość uruchamiania wielu systemów operacyjnych na komputerze z kilkoma jednocześnie zainstalowanymi systemami operacyjnymi.
- Partycje dynamiczne (obsługiwane są tylko główne partycje).
- Dyski posiadające mniej niż 0,5% wolnej niepofragmentowanej przestrzeni.
- Dyski posiadające sektor o rozmiarze innym niż 512 bajtów lub 4096 bajtów, który emuluje 512 bajtów.
- Dyski hybrydowe.
- System posiada moduły ładujące innych firm.
- Dyski ze skompresowanymi katalogami NTFS.
- Technologia Kaspersky Disk Encryption (FDE) jest niekompatybilna z innymi technologiami szyfrowania całego dysku (takimi, jak: BitLocker, McAfee Drive Encryption i WinMagic SecureDoc).

- Technologia Kaspersky Disk Encryption (FDE) jest niekompatybilna z technologią ExpressCache.
- Tworzenie, usuwanie i modyfikowanie partycji na dysku zaszyfrowanym nie jest obsługiwane. Mógłbyś utracić dane.
- Formatowanie systemu plików nie jest obsługiwane. Mógłbyś utracić dane.

  Jeśli chcesz sformatować dysk, który został zaszyfrowany przy pomocy technologii Kaspersky Disk Encryption (FDE), sformatuj dysk na komputerze, na którym nie ma programu Kaspersky Endpoint Security for Windows, i użyj tylko szyfrowania całego dysku.

  Zaszyfrowany dysk, który jest formatowany przy użyciu opcji szybkiego formatowania, przy następnym podłączeniu do komputera z zainstalowanym programem Kaspersky Endpoint Security for Windows może być błędne identyfikowany jako zaszyfrowany. Dane użytkownika będą niedostępne.
- Agent autoryzacji obsługuje nie więcej niż 100 kont.
- Technologia logowania jednokrotnego (SSO) jest niekompatybilna z innymi technologiami deweloperów innych firm.
- Technologia Kaspersky Disk Encryption (FDE) nie jest obsługiwana na następujących modelach urządzeń:
  - Dell Latitude E6410 (tryb UEFI)
  - HP Compaq nc8430 (tryb Legacy BIOS)
  - Lenovo ThinkCentre 8811 (tryb Legacy BIOS)
- Agent autoryzacji nie obsługuje pracy z tokenami USB po włączeniu obsługi starszych wersji USB. Na komputerze możliwe będzie tylko uwierzytelnianie przy użyciu hasła.
- Podczas szyfrowania dysku w trybie Legacy BIOS zalecane jest włączenie obsługi starszych wersji USB na następujących modelach urządzeń:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320

- Dell Vostro 1510
- Dell Vostro 1720
- Dell Vostro V13
- Dell XPS L502x
- Fujitsu Celsius W370
- Fujitsu LifeBook A555
- HP Compaq dx2450 Microtower PC
- Lenovo G550
- Lenovo ThinkPad L530
- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (płyta główna)

Zmiana długości klucza szyfrowania (AES56 / AES256)

Kaspersky Endpoint Security używa algorytmu szyfrowania AES (Advanced Encryption Standard). Kaspersky Endpoint Security obsługuje algorytm szyfrowania AES o efektywnej długości klucza 256 lub 56 bitów. Algorytm szyfrowania danych zależy od biblioteki szyfrowania AES zawartej w pakiecie dystrybucyjnym: *Silne szyfrowanie (AES256)* lub *Uproszczone szyfrowanie (AES56).* Biblioteka szyfrowania AES jest instalowana wraz z aplikacją.

Zmiana długości klucza szyfrowania jest dostępna tylko dla Kaspersky Endpoint Security 11.2.0 lub nowszego.

Zmiana długości klucza szyfrowania składa się z następujących kroków:

1. Przed zmianą długości klucza szyfrowania odszyfruj obiekty, które Kaspersky Endpoint Security zaszyfrował.

   a. Odszyfruj dyski twarde.

   b. Odszyfruj pliki na dyskach lokalnych.

   c. Odszyfruj nośniki wymienne.

   Po zmianie długości klucza szyfrowania, obiekty, które zostały wcześniej zaszyfrowane, staną się niedostępne.

2. Usuń Kaspersky Endpoint Security.

3. Zainstaluj Kaspersky Endpoint Security z pakietu dystrybucyjnego Kaspersky Endpoint Security zawierającego inną bibliotekę szyfrowania.

Możesz także zmienić długość klucza szyfrowania, aktualizując aplikację. Długość klucza można zmienić poprzez aktualizację aplikacji tylko wtedy, gdy spełnione są następujące warunki:

- Kaspersky Endpoint Security w wersji 10 z dodatkiem Service Pack 2 lub nowszym jest zainstalowany na komputerze.
- Komponenty szyfrowania danych (Szyfrowanie plików, Szyfrowanie całego dysku) nie są zainstalowane na komputerze.

  Domyślnie komponenty szyfrowania danych nie są zawarte w Kaspersky Endpoint Security. Komponent Zarządzanie BitLocker nie wpływa na zmianę długości klucza szyfrowania.

Aby zmienić długość klucza szyfrowania, uruchom plik kes_win.msi lub setup_kes.exe z pakietu dystrybucyjnego zawierającego niezbędną bibliotekę szyfrowania. Możesz także zdalnie zaktualizować aplikację za pomocą pakietu instalacyjnego.

Nie można zmienić długości klucza szyfrowania za pomocą pakietu dystrybucyjnego tej samej wersji aplikacji, która jest zainstalowana na komputerze bez uprzedniego odinstalowania aplikacji.

Kaspersky Disk Encryption

Rozwiązanie Kaspersky Disk Encryption nie jest obsługiwane na komputerach opartych na architekturze ARM.

Kaspersky Disk Encryption jest dostępny tylko dla komputerów z systemem operacyjnym Windows dla stacji roboczych. W przypadku komputerów z systemem operacyjnym Windows dla serwerów użyj technologii szyfrowania dysków funkcją BitLocker.

Kaspersky Endpoint Security obsługuje szyfrowanie całego dysku z systemami plików FAT32, NTFS i exFat.

Przed rozpoczęciem szyfrowania całego dysku aplikacja przeprowadza serie skanowań (np. sprawdza dysk twardy systemu na kompatybilność z Agentem autoryzacji i komponentami technologii BitLocker) w celu określenia, czy urządzenie może zostać zaszyfrowane. Aby sprawdzenie kompatybilności mogło się odbyć, należy uruchomić ponownie komputer. Po ponownym uruchomieniu komputera aplikacja automatycznie przeprowadzi wszystkie potrzebne skanowania. Jeśli sprawdzenie kompatybilności zostanie zakończone pomyślnie, szyfrowanie całego dysku rozpocznie się po załadowaniu systemu operacyjnego i uruchomieniu aplikacji. Jeśli skanowanie wykaże niekompatybilność dysku twardego z Agentem autoryzacji lub komponentami technologii BitLocker, komputer będzie musiał zostać uruchomiony ponownie przez wciśnięcie przycisku restartu sprzętowego. Kaspersky Endpoint Security zapisuje informacje o niekompatybilności. W oparciu o te informacje aplikacja nie uruchamia szyfrowania całego dysku przy uruchamianiu systemu operacyjnego. Informacja o tym zdarzeniu jest zapisywana w raporcie Kaspersky Security Center.

Jeśli konfiguracja sprzętowa komputera została zmieniona, informacje o niekompatybilności, zapisane przez aplikację podczas poprzedniego skanowania, powinny zostać usunięte w celu sprawdzenia dysku twardego na kompatybilność z Agentem autoryzacji i komponentami technologii BitLocker. W tym celu, przed zaszyfrowaniem całego dysku, w wierszu polecenia wpisz `avp pbatestreset`. Jeśli system operacyjny nie załaduje się po sprawdzeniu dysku twardego na kompatybilność z Agentem autoryzacji, usuń obiekty i dane pozostałe po testowym działaniu Agenta autoryzacji, korzystając z Narzędzia przywracania zaszyfrowanego urządzenia. Następnie uruchom Kaspersky Endpoint Security i ponownie wykonaj polecenie `avp pbatestreset`.

Po uruchomieniu szyfrowania całego dysku, Kaspersky Endpoint Security zaszyfruje wszystkie dane zapisane na dyskach twardych.

Jeśli podczas szyfrowania całego dysku użytkownik zamknie lub uruchomi ponownie komputer, Agent autoryzacji załaduje się przed kolejnym uruchomieniem systemu operacyjnego. Kaspersky Endpoint Security wznawia szyfrowanie całego dysku po pomyślnej autoryzacji w Agencie autoryzacji i uruchomieniu systemu operacyjnego.

Jeśli podczas szyfrowania całego dysku system operacyjny przełączy się w tryb hibernacji, Agent autoryzacji zostanie załadowany po wyjściu systemu operacyjnego z trybu hibernacji. Kaspersky Endpoint Security wznawia szyfrowanie całego dysku po pomyślnej autoryzacji w Agencie autoryzacji i uruchomieniu systemu operacyjnego.

Jeśli podczas szyfrowania całego dysku system operacyjny przejdzie w tryb uśpienia, Kaspersky Endpoint Security wznowi szyfrowanie całego dysku po wyjściu systemu operacyjnego z trybu uśpienia, bez wczytywania Agenta autoryzacji.

Autoryzacja użytkownika w Agencie autoryzacji może przebiegać na dwa sposoby:

- Poprzez wprowadzenie nazwy i hasła konta Agenta autoryzacji, utworzonego przez administratora sieci LAN przy użyciu narzędzi Kaspersky Security Center.
- Poprzez wprowadzenie hasła do tokena lub karty inteligentnej, podłączonych do komputera.

  Użycie tokena lub karty inteligentnej jest możliwe tylko wtedy, gdy dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES256. Jeśli dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES56, dodanie pliku certyfikatu elektronicznego do polecenia zostanie odrzucone.

Agent autoryzacji obsługuje układy klawiatury dla następujących języków:

- Angielski (UK)
- Angielski (USA)
- Arabski (Algieria, Maroko, Tunis; układ AZERTY)

- Hiszpański (Ameryka Łacińska)
- Włoski
- Niemiecki (Niemcy i Austria)
- Niemiecki (Szwajcaria)
- Portugalski (Brazylia, układ ABNT2)
- Rosyjski (dla klawiatury o 105 klawiszach odpowiadającej układowi QWERTY systemu IBM / Windows)
- Turecki (układ QWERTY)
- Francuski (Francja)
- Francuski (Szwajcaria)
- Francuski (Belgia, układ AZERTY)
- Japoński (dla klawiatury o 106 klawiszach z układem QWERTY)

Układ klawiatury staje się dostępny w Agencie autoryzacji, jeśli ten układ został dodany w ustawieniach języka i standardów regionalnych systemu operacyjnego oraz stał się dostępny na ekranie powitalnym Microsoft Windows.

Jeśli nazwa konta Agenta autoryzacji zawiera symbole, których nie można wprowadzić przy użyciu układów klawiatury dostępnych w Agencie autoryzacji, dostęp do zaszyfrowanych dysków twardych można uzyskać tylko po ich przywróceniu przy pomocy Narzędzia przywracania zaszyfrowanego urządzenia lub po odzyskaniu nazwy i hasła kona Agenta autoryzacji.

Specjalne funkcje szyfrowania dysku SSD

Aplikacja obsługuje szyfrowanie dysków SSD, hybryd dysków SSHD i dysków z funkcją Intel Smart Response. Aplikacja nie obsługuje szyfrowania dysków z funkcją Intel Rapid Start. Przed zaszyfrowaniem tego dysku wyłącz funkcję Intel Rapid Start.

Szyfrowanie dysków SSD ma następujące funkcje specjalne:

- Jeśli dysk SSD jest nowy i nie zawiera poufnych danych, włącz szyfrowanie tylko zajętego obszaru. To umożliwia nadpisanie odpowiednich sektorów dysku.
- Jeśli używany jest dysk SSD i zawiera poufne dane, wybierz jedną z następujących opcji:
  - Całkowicie wyczyść dysk SSD (Secure Erase), zainstaluj system operacyjny i uruchom szyfrowanie dysku SSD z włączoną opcją do szyfrowania tylko zajętego obszaru.
  - Uruchom szyfrowanie dysku SSD z wyłączoną opcją szyfrowania tylko zajętego obszaru.

Szyfrowanie dysku SSD wymaga 5-10 GB wolnego miejsca. Wymagania wolnej przestrzeni do przechowywania danych administracyjnych szyfrowania są dostępne w poniższej tabeli.

Wymagania wolnej przestrzeni do przechowywania danych administracyjnych szyfrowania

Rozmiar dysku SSD (GB)	Wolna przestrzeń na głównej partycji dysku SSD (MB)	Wolna przestrzeń na drugiej partycji dysku SSD (MB)
128	250	64
256	250	640
512	300	128

Uruchamianie Kaspersky Disk Encryption

Przed uruchomieniem szyfrowania całego dysku zalecane jest upewnienie się, że komputer nie jest zainfekowany. W tym celu uruchom zadanie Pełne skanowanie lub Skanowanie obszarów krytycznych. Wykonanie szyfrowania całego dysku na komputerze, który jest zainfekowany rootkitem, może spowodować, że komputer przestanie działać.

Przed rozpoczęciem szyfrowania dysku musisz sprawdzić ustawienia kont Agenta autoryzacji. Agent autoryzacji jest potrzebny do pracy z dyskami chronionymi za pomocą technologii Kaspersky Disk Encryption (FDE). Przed załadowaniem systemu operacyjnego użytkownik musi zakończyć uwierzytelnianie za pomocą Agenta. Kaspersky Endpoint Security umożliwia automatyczne utworzenie kont Agenta autoryzacji przed zaszyfrowaniem dysku. Możesz włączyć automatyczne tworzenie kont Agenta autoryzacji w ustawieniach zasad Szyfrowania całego dysku (patrz poniższe instrukcje). Możesz także użyć technologii jednokrotnego logowania (SSO).

Kaspersky Endpoint Security umożliwia automatyczne utworzenie Agenta autoryzacji dla następujących grup użytkownika:

- **Wszystkie konta na komputerze**. Wszystkie konta na komputerze, które były aktywne w dowolnym momencie.
- **Wszystkie konta domenowe na komputerze**. Wszystkie konta na komputerze, które należą do niektórych domen i które były aktywne w dowolnym momencie.
- **Wszystkie konta lokalne na komputerze**. Wszystkie konta lokalne na komputerze, które były aktywne w dowolnym momencie.
- **Konto usługi z hasłem jednorazowym**. Konto usługi jest niezbędne do uzyskania dostępu do komputera, na przykład, gdy użytkownik zapomni hasło. Możesz także użyć konta usługi jako konta zapasowego. Musisz wprowadzić nazwę konta (domyślnie, `ServiceAccount`). Kaspersky Endpoint Security tworzy hasło automatycznie. Hasło możesz znaleźć w konsoli Kaspersky Security Center.
- **Lokalny administrator**. Kaspersky Endpoint Security tworzy konto użytkownika Agenta autoryzacji dla lokalnego administratora komputera.
- **Menedżer komputera**. Kaspersky Endpoint Security tworzy konto użytkownika Agenta autoryzacji dla konta menadżera komputera. Możesz zobaczyć, które konto ma rolę menadżera komputera we właściwościach komputera w Active Directory. Domyślnie, rola menadżera komputera nie jest zdefiniowana, czyli nie odpowiada żadnemu kontu.
- **Aktywne konto**. Kaspersky Endpoint Security automatycznie tworzy konto Agenta autoryzacji dla konta, które jest aktywne w momencie szyfrowania dysku.

Zadanie *Zarządzanie kontami Agenta autoryzacji* służy do konfigurowania ustawień uwierzytelniania użytkownika. Możesz użyć tego zadania do dodania nowych kont, zmodyfikowania ustawień bieżących kont lub usunąć konta, jeśli jest to konieczne. Możesz używać zadań lokalnych dla pojedynczych komputerów, a także zadań grupowych dla komputerów z oddzielnych grup administracyjnych lub wybranych komputerów.

Jak uruchomić Kaspersky Disk Encryption za pomocą Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych → Szyfrowanie całego dysku**.
4. Z listy rozwijalnej **Technologia szyfrowania** wybierz **Kaspersky Disk Encryption**.

   Technologia Kaspersky Disk Encryption nie może być użyta, jeśli dyski twarde komputera zostały zaszyfrowane przy użyciu funkcji BitLocker.

5. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Zaszyfruj wszystkie dyski twarde**.

   Jeśli na komputerze jest zainstalowanych kilka systemów operacyjnych, po zaszyfrowaniu wszystkich dysków twardych będziesz mógł załadować tylko ten system operacyjny, na którym jest zainstalowana aplikacja.

   Jeśli chcesz wykluczyć niektóre dyski twarde z szyfrowania, utwórz listę tych dysków twardych.

6. Skonfiguruj zaawansowane opcje Kaspersky Disk Encryption (patrz tabela poniżej).
7. Zapisz swoje zmiany.

Jak uruchomić Kaspersky Disk Encryption za pośrednictwem konsoli Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Szyfrowanie danych → Szyfrowanie całego dysku**.
5. Wybierz technologię **Kaspersky Disk Encryption**.

   Technologia Kaspersky Disk Encryption nie może być użyta, jeśli dyski twarde komputera zostały zaszyfrowane przy użyciu funkcji BitLocker.

6. W bloku **Działania na urządzeniach** wybierz **Zaszyfruj wszystkie dyski twarde**.

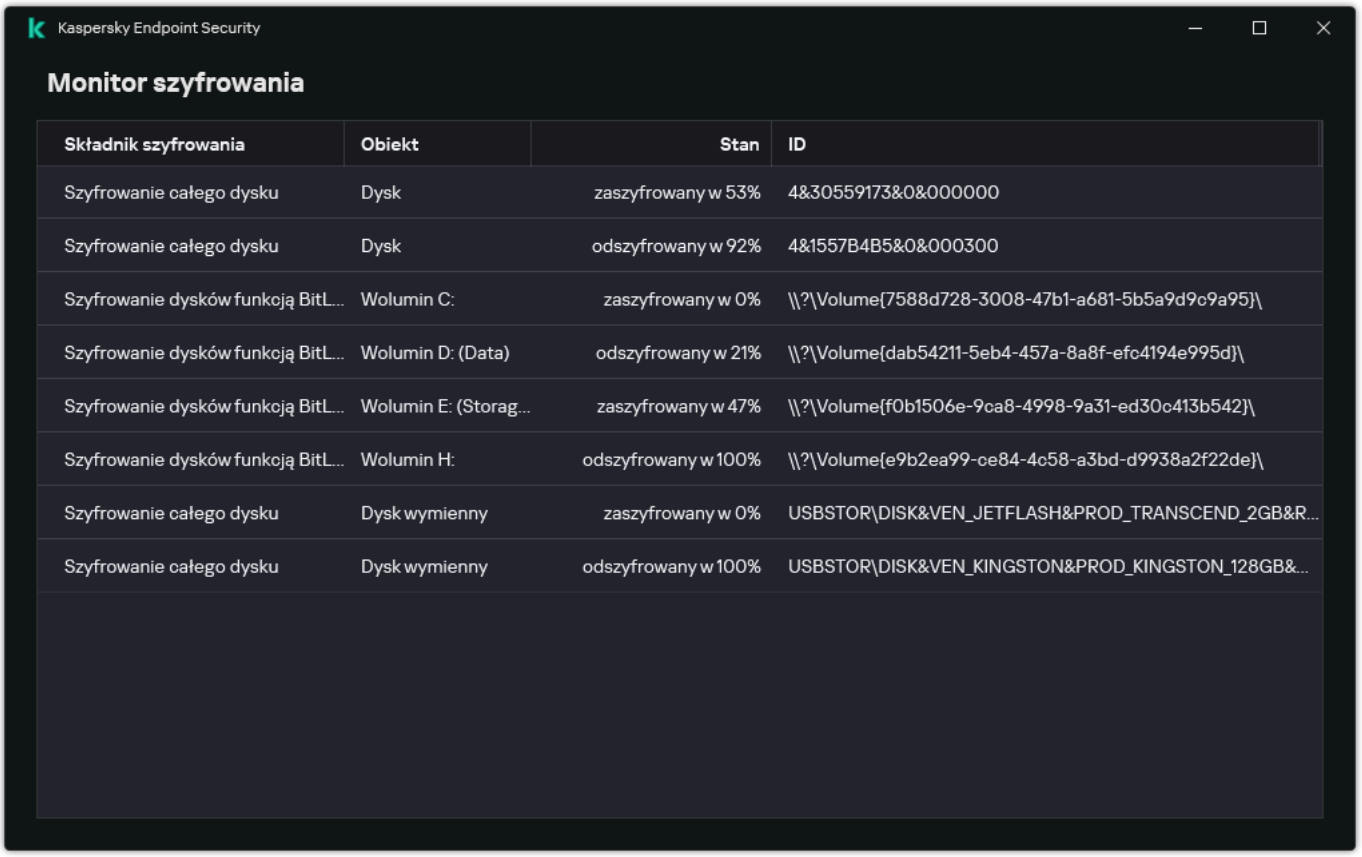
   Jeśli na komputerze jest zainstalowanych kilka systemów operacyjnych, po szyfrowaniu będziesz mógł załadować tylko ten system operacyjny, na którym szyfrowanie zostało wykonane.

   Jeśli chcesz wykluczyć niektóre dyski twarde z szyfrowania, utwórz listę tych dysków twardych.

7. Skonfiguruj zaawansowane opcje Kaspersky Disk Encryption (patrz tabela poniżej).

8. Zapisz swoje zmiany.

Możesz użyć narzędzia Monitor szyfrowania, aby kontrolować szyfrowanie dysku lub proces deszyfrowania na komputerze użytkownika. Możesz uruchomić narzędzie Monitor szyfrowania z poziomu okna głównego aplikacji.



Monitor szyfrowania

Jeśli dyski twarde są zaszyfrowane, Agent autoryzacji ładuje się przed uruchomieniem systemu operacyjnego. Użyj Agenta autoryzacji do zakończenia procesu autoryzacji, aby uzyskać dostęp do zaszyfrowanych dysków twardych i załadować system operacyjny. Po pomyślnym zakończeniu procedury autoryzacji, system operacyjny zostanie załadowany. Proces autoryzacji jest powtarzany przy każdym ponownym uruchomieniu systemu operacyjnego.

Ustawienia komponentu Kaspersky Disk Encryption

Parametr	Opis
Automatycznie utwórz konta Agenta autoryzacji dla użytkownicy podczas szyfrowania	Jeśli to pole jest zaznaczone, aplikacja tworzy konta Agenta autoryzacji w oparciu o listę kont użytkowników systemu Windows na komputerze. Domyślnie, Kaspersky Endpoint Security używa wszystkich kont lokalnych i domenowych, z którymi użytkownik logował się do systemu operacyjnego w ciągu ostatnich 30 dni.
Automatycznie utwórz konta Agenta autoryzacji dla wszystkich użytkowników tego komputera podczas pierwszego logowania	Jeśli to pole jest zaznaczone, aplikacja sprawdza informacje o kontach użytkownika systemu Windows na komputerze przed uruchomieniem Agenta autoryzacji. Jeśli Kaspersky Endpoint Security wykryje konto użytkownika systemu Windows, które nie zawiera konta Agenta autoryzacji, aplikacja utworzy nowe konto do uzyskania dostępu do zaszyfrowanych dysków. Nowe konto Agenta autoryzacji będzie posiadało domyślne ustawienia: tylko logowanie zabezpieczone hasłem oraz zmiana hasła po pierwszej autoryzacji. Dlatego też nie musisz ręcznie dodawać kont Agenta autoryzacji przy użyciu zadania *Zarządzanie kontami Agenta autoryzacji* dla komputerów z już zaszyfrowanymi dyskami.
Zapisz nazwę użytkownika wprowadzoną w Agencie autoryzacji	Jeśli to pole jest zaznaczone, aplikacja zapisze nazwę konta Agenta autoryzacji. Przy następnej próbie zalogowania się do Agenta autoryzacji z poziomu tego samego konta nie będzie konieczne wpisanie nazwy konta.

Parametr	Opis
Szyfruj tylko zajętą przestrzeń dysku (redukuje czas szyfrowania)	To pole włącza/wyłącza opcję ograniczającą obszar szyfrowania tylko do zajmowanych sektorów dysku twardego. To ograniczenie pozwala na skrócenie czasu szyfrowania. Włączenie lub wyłączenie funkcji **Szyfruj tylko zajętą przestrzeń dysku (redukuje czas szyfrowania)** po rozpoczęciu szyfrowania nie powoduje zmodyfikowania tego ustawienia, aż do odszyfrowania dysków twardych. Przed rozpoczęciem szyfrowania należy zaznaczyć lub odznaczyć to pole. Jeśli pole jest zaznaczone, zostaną zaszyfrowane tylko te obszary dysku twardego, które są zajęte przez pliki. Kaspersky Endpoint Security automatycznie szyfruje nowe dane po ich dodaniu. Jeśli pole jest odznaczone, cały dysk twardy jest szyfrowany, w tym fragmenty wcześniej usuniętych i zmodyfikowanych plików. Ta opcja jest zalecana dla nowych dysków twardych, których dane nie zostały zmodyfikowane ani usunięte. Jeśli stosujesz szyfrowanie na dysku twardym, który jest już w użyciu, zalecane jest zaszyfrowanie całego dysku twardego. Zapewni to ochronę wszystkich danych, także tych usuniętych, które potencjalnie można odzyskać. Domyślnie to pole wyboru nie jest zaznaczone.
Obsługa starszych wersji USB (niezalecane)	To pole wyboru włącza lub wyłącza funkcjonalność Legacy USB Support. *Obsługa starszych wersji USB* **to** funkcja BIOS/UEFI, która umożliwia korzystanie z urządzeń USB (takich jak token zabezpieczający) w trakcie fazy rozruchu komputera przed uruchomieniem systemu operacyjnego (tryb BIOS). Legacy USB Support nie wpływa na obsługę urządzeń USB po uruchomieniu systemu operacyjnego. Jeśli pole jest zaznaczone, obsługa urządzeń USB podczas pierwszego uruchomienia komputera będzie włączona. Jeśli funkcja Legacy USB Support jest włączona, Agent autoryzacji w trybie BIOS nie obsługuje pracy z tokenami za pośrednictwem USB. Zalecane jest użycie tej opcji tylko wtedy, gdy istnieje problem kompatybilności sprzętowej i tylko dla tych komputerów, na których wystąpił problem.

Tworzenie listy dysków twardych wykluczonych z szyfrowania

Listę wykluczeń z szyfrowania można utworzyć tylko dla technologii Kaspersky Disk Encryption.

W celu utworzenia listy dysków twardych wykluczonych z szyfrowania:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych → Szyfrowanie całego dysku**.
4. Z listy rozwijalnej **Technologia szyfrowania** wybierz **Kaspersky Disk Encryption**.

   Wpisy odpowiadające dyskom twardym wykluczonym z szyfrowania pojawią się w tabeli **Nie szyfruj następujących dysków twardych**. Ta tabela jest pusta, jeśli wcześniej nie utworzyłeś listy dysków twardych wykluczonych z szyfrowania.

5. W celu dodania dysków twardych do listy dysków twardych wykluczonych z szyfrowania:

   a. Kliknij **Dodaj**.

   b. W otwartym oknie należy określić wartości dla **Nazwa urządzenia**, **Komputer**, **Typ dysku**, **Kaspersky Disk Encryption**.

   c. Kliknij **Odśwież**.

   d. W kolumnie **Nazwa** zaznacz pola obok dysków twardych, które chcesz dodać do listy dysków twardych wykluczonych z szyfrowania.

   e. Kliknij **OK**.

   Wybrane dyski twarde pojawią się w tabeli **Nie szyfruj następujących dysków twardych**.

6. Zapisz swoje zmiany.

Eksportowanie i importowanie listy dysków twardych wykluczonych z szyfrowania

Możesz wyeksportować listę wykluczeń szyfrowania dysku twardego do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę wykluczeń tego samego typu. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy wykluczeń lub przeniesienia wykluczeń na inny serwer.

Eksportowanie i importowanie listy wykluczeń szyfrowania dysku twardego w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.

4. Z listy rozwijalnej **Technologia szyfrowania** wybierz **Kaspersky Disk Encryption**.

   Wpisy odpowiadające dyskom twardym wykluczonym z szyfrowania pojawią się w tabeli **Nie szyfruj następujących dysków twardych**.

5. W celu wyeksportowania listy wykluczeń:

   a. Wybierz wykluczenia, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.

   Jeśli nie wybrałeś żadnego wykluczenia, Kaspersky Endpoint Security wyeksportuje wszystkie wykluczenia.

   b. Kliknij przycisk → **Eksportuj**.

   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.

   d. Zapisz plik.

   Kaspersky Endpoint Security eksportuje całą listę wykluczeń do pliku XML.

6. W celu zaimportowania listy reguł:

   a. Kliknij przycisk → **Importuj**.

   b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.

   c. Otwórz plik.

      Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

7. Zapisz swoje zmiany.

Eksportowanie i importowanie listy wykluczeń szyfrowania dysku twardego w Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.

   Wybierz technologię **Kaspersky Disk Encryption**.

5. Kliknij odnośnik **Wykluczenia**.

   Zostanie otwarta lista wykluczeń.

6. W celu wyeksportowania listy reguł:

   a. Wybierz wykluczenia, które chcesz wyeksportować.

   b. Kliknij przycisk → **Eksportuj**.

      Kaspersky Endpoint Security eksportuje listę wykluczeń do pliku JSON w domyślnym folderze Pobrane.

7. W celu zaimportowania listy wykluczeń:

   a. Kliknij przycisk → **Importuj**.

      W oknie, które zostanie otwarte, wybierz plik JSON, z którego chcesz zaimportować listę wykluczeń.

   b. Otwórz plik.

      Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku JSON.

8. Zapisz swoje zmiany.

Włączanie technologii Single Sign-On (SSO)

Technologia Single Sign-On (SSO) umożliwia automatyczne logowanie do systemu operacyjnego przy użyciu poświadczeń Agenta autoryzacji. Oznacza to, że użytkownik musi wprowadzić hasło tylko raz podczas logowania się do systemu Windows (hasło konta Agenta autoryzacji). Technologia Single Sign-On pozwala także na automatyczne uaktualnianie hasła konta Agenta autoryzacji, gdy hasło konta Windows zostanie zmienione.

Podczas korzystania z technologii logowania jednokrotnego Agent autoryzacji ignoruje wymagania dotyczące siły hasła określone w Kaspersky Security Center. Możesz ustawić wymagania dotyczące siły hasła w ustawieniach systemu operacyjnego.

Włączanie technologii Single Sign-On

Jak włączyć korzystanie z technologii logowania jednokrotnego w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych** → **Ogólne ustawienia szyfrowania**.
4. W sekcji **Ustawienia hasła** kliknij przycisk **Ustawienia**.
5. W otwartym oknie, w zakładce **Agent autoryzacji** zaznacz pole wyboru **Użyj technologii logowania jednokrotnego (SSO)**.
6. W przypadku korzystania z usług zewnętrznego dostawcy danych uwierzytelniających, zaznacz pole wyboru **Zawijaj zewnętrznych dostawców poświadczeń**.
7. Zapisz swoje zmiany.

W rezultacie użytkownik musi przeprowadzić procedurę uwierzytelnienia tylko raz z Agentem. Procedura uwierzytelnienia nie jest wymagana do załadowania systemu operacyjnego. System operacyjny ładuje się automatycznie.

Jak włączyć korzystanie z logowania jednokrotnego w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
5. Wybierz technologię **Kaspersky Disk Encryption**.
6. W sekcji **Ustawienia hasła** zaznacz pole **Użyj technologii logowania jednokrotnego (SSO)**.
7. W przypadku korzystania z usług zewnętrznego dostawcy danych uwierzytelniających, zaznacz pole wyboru **Zawijaj zewnętrznych dostawców poświadczeń**.
8. Zapisz swoje zmiany.

W rezultacie użytkownik musi przeprowadzić procedurę uwierzytelnienia tylko raz z Agentem. Procedura uwierzytelnienia nie jest wymagana do załadowania systemu operacyjnego. System operacyjny ładuje się automatycznie.

Aby logowanie jednokrotne działało, hasło do konta Windows i hasło do konta Agenta autoryzacji muszą być zgodne. Jeśli hasła się nie zgadzają, użytkownik musi wykonać procedurę uwierzytelnienia dwukrotnie: w interfejsie Agenta autoryzacji i przed załadowaniem systemu operacyjnego. Te czynności muszą być wykonane tylko raz, aby zsynchronizować hasła. Następnie Kaspersky Endpoint Security zastąpi hasło do konta Agenta autoryzacji hasłem do konta Windows. Kiedy hasło do konta Windows zostanie zmienione, aplikacja automatycznie zaktualizuje hasło do konta Agenta autoryzacji.

Zewnętrzni dostawcy usług uwierzytelniania

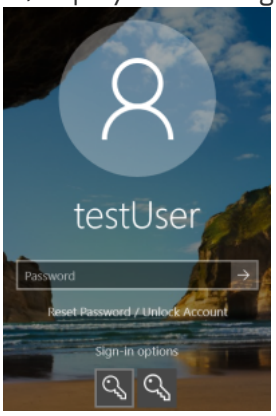
Kaspersky Endpoint Security obsługuje zewnętrznego dostawcę usług uwierzytelniania ADSelfService Plus.

Podczas pracy z zewnętrznymi dostawcami usług uwierzytelniania Agent autoryzacji przechwytuje hasło przed załadowaniem systemu operacyjnego. Oznacza to, że użytkownik musi wprowadzić hasło tylko raz podczas logowania się do systemu Windows. Po zalogowaniu się do systemu Windows użytkownik może korzystać z możliwości zewnętrznego dostawcy usług uwierzytelniających, na przykład do uwierzytelniania w usługach korporacyjnych. Zewnętrzni dostawcy usług uwierzytelniających pozwalają także użytkownikom na samodzielne resetowanie własnego hasła. W tym przypadku Kaspersky Endpoint Security automatycznie zaktualizuje hasło dla Agenta autoryzacji.

W przypadku korzystania z zewnętrznego dostawcy usług uwierzytelniających, który nie jest obsługiwany przez aplikację, można napotkać pewne ograniczenia w działaniu technologii Single Sign-On. Podczas logowania do systemu Windows użytkownik będzie miał do dyspozycji dwa profile: systemowy dostawca usług uwierzytelniających i zewnętrzny dostawca usług uwierzytelniających. Ikony tych profili będą identyczne (zobacz rysunek poniżej). Użytkownik będzie miał do wyboru następujące opcje, aby kontynuować:

- Jeśli użytkownik wybierze *zewnętrznego dostawcę usług uwierzytelniających*, Agent autoryzacji nie będzie mógł zsynchronizować hasła z kontem Windows. Dlatego też, jeśli użytkownik zmienił hasło konta Windows, Kaspersky Endpoint Security nie może zaktualizować hasła dla konta Agenta autoryzacji. W wyniku czego, użytkownik musi wykonać procedurę uwierzytelnienia dwukrotnie: w interfejsie Agenta autoryzacji i przed załadowaniem systemu operacyjnego. W takim przypadku użytkownik może korzystać z możliwości zewnętrznego dostawcy usług uwierzytelniających, na przykład do uwierzytelniania w usługach korporacyjnych.

- Jeśli użytkownik wybierze *systemowego dostawcę usług uwierzytelniających*, Agent autoryzacji będzie mógł zsynchronizować hasła z kontem Windows. W takim przypadku użytkownik nie może korzystać z możliwości zewnętrznego dostawcy usług uwierzytelniania, na przykład w usługach korporacyjnych.



Systemowy profil uwierzytelniania i zewnętrzny profil uwierzytelniania do logowania w systemie Windows

Zarządzanie kontami Agenta autoryzacji

Agent autoryzacji jest potrzebny do pracy z dyskami chronionymi za pomocą technologii Kaspersky Disk Encryption (FDE). Przed załadowaniem systemu operacyjnego użytkownik musi zakończyć uwierzytelnianie za pomocą Agenta. Zadanie *Zarządzanie kontami Agenta autoryzacji* służy do konfigurowania ustawień uwierzytelniania użytkownika. Możesz używać zadań lokalnych dla pojedynczych komputerów, a także zadań grupowych dla komputerów z oddzielnych grup administracyjnych lub wybranych komputerów.

Nie można skonfigurować terminarza uruchamiania zadania *Zarządzanie kontami Agenta autoryzacji*. Nie można również przymusowo zatrzymać zadania.

Jak utworzyć zadanie Zarządzanie kontami Agenta autoryzacji w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Zarządzanie kontami Agenta autoryzacji**.

Krok 2. Wybieranie polecenia do zarządzania kontem Agenta autoryzacji

Wygeneruj listę poleceń do zarządzania kontem Agenta autoryzacji. Polecenia do zarządzania umożliwiają dodawanie, modyfikowanie i usuwanie kont Agenta autoryzacji (patrz instrukcje poniżej). Tylko użytkownicy posiadający konto Agenta autoryzacji mogą wykonać procedurę uwierzytelnienia, załadować system operacyjny i uzyskać dostęp do zaszyfrowanego dysku.

Krok 3. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 4. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład *Konta administratora*.

Krok 5. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

W rezultacie, po zakończeniu zadania, przy następnym uruchomieniu komputera nowy użytkownik może ukończyć procedurę uwierzytelniania, załadować system operacyjny i uzyskać dostęp do zaszyfrowanego dysku.

Jak utworzyć zadanie Zarządzanie kontami Agenta autoryzacji w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (14.1)**.
2. Z listy rozwijalnej **Typ zadania** wybierz **Zarządzanie kontami Agenta autoryzacji**.
3. W polu **Nazwa zadania** wpisz krótki opis, na przykład, *Konta administratora*.
4. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

Krok 2. Zarządzanie kontami Agenta autoryzacji

Wygeneruj listę poleceń do zarządzania kontem Agenta autoryzacji. Polecenia do zarządzania umożliwiają dodawanie, modyfikowanie i usuwanie kont Agenta autoryzacji (patrz instrukcje poniżej). Tylko użytkownicy posiadający konto Agenta autoryzacji mogą wykonać procedurę uwierzytelnienia, załadować system operacyjny i uzyskać dostęp do zaszyfrowanego dysku.

Krok 3. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Nowe zadanie zostanie wyświetlone na liście zadań.

Aby uruchomić zadanie, zaznacz pole obok zadania i kliknij przycisk **Uruchom**.

W rezultacie, po zakończeniu zadania, przy następnym uruchomieniu komputera nowy użytkownik może ukończyć procedurę uwierzytelniania, załadować system operacyjny i uzyskać dostęp do zaszyfrowanego dysku.

Aby dodać konto Agenta autoryzacji, musisz dodać specjalne polecenie do zadania *Zarządzanie kontami Agenta autoryzacji*. Wygodne jest użycie zadania grupowego, na przykład, w celu dodania konta administratora do wszystkich komputerów.

Kaspersky Endpoint Security umożliwia automatyczne utworzenie kont Agenta autoryzacji przed zaszyfrowaniem dysku. Możesz włączyć automatyczne tworzenie kont Agenta autoryzacji w ustawieniach zasad Szyfrowania całego dysku. Możesz także użyć technologii jednokrotnego logowania (SSO).

Jak dodać konto Agenta autoryzacji za pomocą Konsoli administracyjnej (MMC)?

1. Otwórz właściwości zadania *Zarządzanie kontami Agenta autoryzacji*.
2. We właściwościach zadania wybierz sekcję **Ustawienia**.
3. Kliknij **Dodaj** → **Polecenie dodania konta**.
4. W oknie, które zostanie otwarte, w polu **Konto Windows** określ nazwę konta Microsoft Windows, które zostanie użyte do utworzenia konta Agenta autoryzacji.
5. Jeśli ręcznie wprowadziłeś nazwę konta systemu Windows, kliknij przycisk **Zezwól**, aby zdefiniować identyfikator zabezpieczeń konta (SID).

   Jeśli zdecydujesz się nie określać identyfikatora zabezpieczeń (SID) poprzez kliknięcie przycisku **Zezwól**, zostanie on określony w momencie wykonywania zadania na komputerze.

   > Zdefiniowanie identyfikatora zabezpieczeń konta Windows jest konieczne, aby sprawdzić, czy nazwa konta Windows została wprowadzona poprawnie. Jeśli konto systemu Windows nie istnieje na komputerze lub w zaufanej domenie, zadanie *Zarządzanie kontami Agenta autoryzacji* zakończy się błędem.

6. Zaznacz pole **Zastąp istniejące konto**, jeśli chcesz, żeby istniejące konto, które zostało wcześniej utworzone dla Agenta autoryzacji, zastąpić kontem, które jest aktualnie tworzone.

   Ten krok jest dostępny podczas dodawania polecenia tworzenia konta Agenta autoryzacji we właściwościach zadania grupowego do zarządzania kontami Agenta autoryzacji. Ten krok nie jest dostępny podczas dodawania polecenia tworzenia konta Agenta autoryzacji we właściwościach zadania lokalnego *Zarządzanie kontami Agenta autoryzacji*.

7. W polu **Nazwa użytkownika** wpisz nazwę konta Agenta autoryzacji, która ma być wprowadzona podczas procesu autoryzacji, aby uzyskać dostęp do zaszyfrowanych dysków twardych.

8. Zaznacz pole **Zezwól na uwierzytelnianie przy użyciu hasła**, jeśli chcesz, żeby podczas procesu autoryzacji aplikacja pytała użytkownika o wprowadzenie hasła do konta Agenta autoryzacji w celu uzyskania dostępu do zaszyfrowanych dysków twardych. Ustaw hasło dla konta Agenta autoryzacji. W razie potrzeby możesz poprosić użytkownika o nowe hasło po pierwszym uwierzytelnieniu.

9. Zaznacz pole **Zezwól na uwierzytelnianie przy użyciu certyfikatu**, jeśli chcesz, żeby podczas procesu autoryzacji aplikacja pytała użytkownika o połączenie tokena lub karty inteligentnej z komputerem w celu uzyskania dostępu do zaszyfrowanych dysków twardych. Wybierz plik certyfikatu do uwierzytelnienia za pomocą karty inteligentnej lub tokena.

10. Jeśli to konieczne, w polu **Opis polecenia** wprowadź szczegółowe informacje dotyczące konta Agenta autoryzacji, których potrzebujesz do zarządzania poleceniem.

11. W sekcji **Dostęp do autoryzacji przy użyciu Agenta autoryzacji** skonfiguruj dostęp do autoryzacji w Agencie autoryzacji dla użytkownika, który używa konta określonego w poleceniu.

12. Zapisz swoje zmiany.

Jak dodać konto Agenta autoryzacji za pomocą konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie **Zarządzanie kontami Agenta autoryzacji** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Na liście kont Agenta autoryzacji kliknij przycisk **Dodaj**.

   Spowoduje to uruchomienie Kreatora zarządzania kontem Agenta autoryzacji.

5. Wybierz typ polecenia **Dodaj**.

6. Wybierz konto użytkownika. Możesz wybrać konto z listy kont domeny lub ręcznie wprowadzić nazwę konta. Przejdź do następnego kroku.

   Kaspersky Endpoint Security określa identyfikator zabezpieczeń konta (SID). Jest to konieczne do zweryfikowania konta. Jeśli podałeś nieprawidłową nazwę użytkownika, Kaspersky Endpoint Security zakończy zadanie z błędem.

7. Skonfiguruj ustawienia konta Agenta autoryzacji.

   - **Utwórz nowe konto Agenta autoryzacji, aby zastąpić istniejące konto**. Kaspersky Endpoint Security skanuje istniejące konta na komputerze. Jeśli identyfikator zabezpieczeń użytkownika na komputerze i w zadaniu jest zgodny, Kaspersky Endpoint Security zmieni ustawienia konta użytkownika zgodnie z zadaniem.

   - **Nazwa użytkownika**. Domyślna nazwa użytkownika konta Agenta autoryzacji odpowiada nazwie domeny użytkownika.

   - **Zezwól na uwierzytelnianie przy użyciu hasła**. Ustaw hasło dla konta Agenta autoryzacji. W razie potrzeby możesz poprosić użytkownika o nowe hasło po pierwszym uwierzytelnieniu. W ten sposób każdy użytkownik będzie miał swoje unikatowe hasło. Możesz także ustawić wymagania dotyczące siły hasła dla konta Agenta autoryzacji w zasadzie.

   - **Zezwól na uwierzytelnianie przy użyciu certyfikatu**. Wybierz plik certyfikatu do uwierzytelnienia za pomocą karty inteligentnej lub tokena. W ten sposób użytkownik będzie musiał wprowadzić hasło do karty inteligentnej lub tokena.

   - **Dostęp konta do zaszyfrowanych danych**. Skonfiguruj dostęp użytkownika do zaszyfrowanego dysku. Możesz, na przykład, tymczasowo wyłączyć uwierzytelnianie użytkownika zamiast usuwać konto Agenta autoryzacji.

   - **Komentarz**. W razie potrzeby wprowadź opis konta.

8. Zapisz swoje zmiany.

9. Zaznacz pole obok zadania i kliknij przycisk **Uruchom**.

   W rezultacie, po zakończeniu zadania, przy następnym uruchomieniu komputera nowy użytkownik może ukończyć procedurę uwierzytelniania, załadować system operacyjny i uzyskać dostęp do zaszyfrowanego dysku.

Aby zmienić hasło i inne ustawienia konta Agenta autoryzacji, musisz dodać specjalne polecenie do zadania *Zarządzanie kontami Agenta autoryzacji*. Wygodne jest użycie zadania grupowego, na przykład, w celu zastąpienia certyfikatu tokena administratora na wszystkich komputerach.

Jak zmienić konto Agenta autoryzacji za pomocą Konsoli administracyjnej (MMC)?

1. Otwórz właściwości zadania *Zarządzanie kontami Agenta autoryzacji*.

2. We właściwościach zadania wybierz sekcję **Ustawienia**.

3. Kliknij **Dodaj → Polecenie edycji konta**.

4. W oknie, które zostanie otwarte, w polu **Konto Windows** określ nazwę konta użytkownika Microsoft Windows, które chcesz zmienić.

5. Jeśli ręcznie wprowadziłeś nazwę konta systemu Windows, kliknij przycisk **Zezwól**, aby zdefiniować identyfikator zabezpieczeń konta (SID).

   Jeśli zdecydujesz się nie określać identyfikatora zabezpieczeń (SID) poprzez kliknięcie przycisku **Zezwól**, zostanie on określony w momencie wykonywania zadania na komputerze.

   Zdefiniowanie identyfikatora zabezpieczeń konta Windows jest konieczne, aby sprawdzić, czy nazwa konta Windows została wprowadzona poprawnie. Jeśli konto systemu Windows nie istnieje na komputerze lub w zaufanej domenie, zadanie *Zarządzanie kontami Agenta autoryzacji* zakończy się błędem.

6. Zaznacz pole **Zmień nazwę użytkownika** i wprowadź nową nazwę dla konta Agenta autoryzacji, jeśli chcesz, aby Kaspersky Endpoint Security zmienił nazwę użytkownika dla wszystkich kont Agenta autoryzacji, utworzonych w oparciu o konto systemu Microsoft Windows posiadające nazwę określoną w polu **Konto Windows**, na nazwę wpisaną w polu poniżej.

7. Zaznacz pole **Modyfikuj ustawienia uwierzytelniania przy użyciu hasła**, aby możliwe było zmodyfikowanie ustawień autoryzacji opartej o hasło.

8. Zaznacz pole **Zezwól na uwierzytelnianie przy użyciu hasła**, jeśli chcesz, żeby podczas procesu autoryzacji aplikacja pytała użytkownika o wprowadzenie hasła do konta Agenta autoryzacji w celu uzyskania dostępu do zaszyfrowanych dysków twardych. Ustaw hasło dla konta Agenta autoryzacji.

9. Zaznacz pole **Edytuj regułę zmiany hasła podczas autoryzacji przy użyciu Agenta autoryzacji**, jeśli chcesz, aby Kaspersky Endpoint Security zmienił wartość ustawienia zmiany hasła dla wszystkich kont Agenta autoryzacji utworzonych w oparciu o konto systemu Microsoft Windows, posiadające nazwę określoną w polu **Konto Windows**, na wartość określoną poniżej.

10. Określ wartość ustawienia zmiany hasła po autoryzacji w Agencie autoryzacji.

11. Zaznacz pole **Modyfikuj ustawienia uwierzytelniania przy użyciu certyfikatu**, aby możliwe było zmodyfikowanie ustawień autoryzacji opartej o certyfikat elektroniczny tokena lub karty inteligentnej.

12. Zaznacz pole **Zezwól na uwierzytelnianie przy użyciu certyfikatu**, jeśli chcesz, żeby podczas procesu autoryzacji aplikacja pytała użytkownika o wprowadzenie hasła do tokena lub karty inteligentnej podłączonej do komputera w celu uzyskania dostępu do zaszyfrowanych dysków twardych. Wybierz plik certyfikatu do uwierzytelnienia za pomocą karty inteligentnej lub tokena.

13. Zaznacz pole **Edytuj opis polecenia** i zmodyfikuj opis polecenia, jeśli chcesz, aby Kaspersky Endpoint Security zmienił opis polecenia dla wszystkich kont Agenta autoryzacji, utworzonych w oparciu o konto systemu Microsoft Windows posiadające nazwę określoną w polu **Konto Windows**.

14. Zaznacz pole **Edytuj regułę dostępu do autoryzacji przy użyciu Agenta autoryzacji**, jeśli chcesz, aby Kaspersky Endpoint Security zmienił regułę dostępu użytkownika do okna autoryzacji w Agencie autoryzacji na wartość określoną poniżej dla wszystkich konta Agenta autoryzacji, utworzonych w oparciu o konto systemu Microsoft Windows posiadające nazwę określoną w polu **Konto Windows**.

15. Określ regułę dostępu do okna autoryzacji w Agencie autoryzacji.

16. Zapisz swoje zmiany.

Jak zmienić konto Agenta autoryzacji za pomocą konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie **Zarządzanie kontami Agenta autoryzacji** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Na liście kont Agenta autoryzacji kliknij przycisk **Dodaj**.

   Spowoduje to uruchomienie Kreatora zarządzania kontem Agenta autoryzacji.

5. Wybierz typ polecenia **Zmień**.

6. Wybierz konto użytkownika. Możesz wybrać konto z listy kont domeny lub ręcznie wprowadzić nazwę konta. Przejdź do następnego kroku.

   Kaspersky Endpoint Security określa identyfikator zabezpieczeń konta (SID). Jest to konieczne do zweryfikowania konta. Jeśli podałeś nieprawidłową nazwę użytkownika, Kaspersky Endpoint Security zakończy zadanie z błędem.

7. Zaznacz pola wyboru obok ustawień, które chcesz edytować.

8. Skonfiguruj ustawienia konta Agenta autoryzacji.

   - **Utwórz nowe konto Agenta autoryzacji, aby zastąpić istniejące konto**. Kaspersky Endpoint Security skanuje istniejące konta na komputerze. Jeśli identyfikator zabezpieczeń użytkownika na komputerze i w zadaniu jest zgodny, Kaspersky Endpoint Security zmieni ustawienia konta użytkownika zgodnie z zadaniem.

   - **Nazwa użytkownika**. Domyślna nazwa użytkownika konta Agenta autoryzacji odpowiada nazwie domeny użytkownika.

   - **Zezwól na uwierzytelnianie przy użyciu hasła**. Ustaw hasło dla konta Agenta autoryzacji. W razie potrzeby możesz poprosić użytkownika o nowe hasło po pierwszym uwierzytelnieniu. W ten sposób każdy użytkownik będzie miał swoje unikatowe hasło. Możesz także ustawić wymagania dotyczące siły hasła dla konta Agenta autoryzacji w zasadzie.

   - **Zezwól na uwierzytelnianie przy użyciu certyfikatu**. Wybierz plik certyfikatu do uwierzytelnienia za pomocą karty inteligentnej lub tokena. W ten sposób użytkownik będzie musiał wprowadzić hasło do karty inteligentnej lub tokena.

   - **Dostęp konta do zaszyfrowanych danych**. Skonfiguruj dostęp użytkownika do zaszyfrowanego dysku. Możesz, na przykład, tymczasowo wyłączyć uwierzytelnianie użytkownika zamiast usuwać konto Agenta autoryzacji.

   - **Komentarz**. W razie potrzeby wprowadź opis konta.

9. Zapisz swoje zmiany.

10. Zaznacz pole obok zadania i kliknij przycisk **Uruchom**.

Aby usunąć konto Agenta autoryzacji, musisz dodać specjalne polecenie do zadania *Zarządzanie kontami Agenta autoryzacji*. Wygodnie jest skorzystać z zadania grupowego, na przykład, aby usunąć konto zwolnionego pracownika.

Jak usunąć konto Agenta autoryzacji za pomocą Konsoli administracyjnej (MMC)?

1. Otwórz właściwości zadania *Zarządzanie kontami Agenta autoryzacji*.

2. We właściwościach zadania wybierz sekcję **Ustawienia**.

3. Kliknij **Dodaj** → **Polecenie usunięcia konta**.

4. W otwartym oknie, w polu **Konto Windows** określ nazwę konta użytkownika systemu Windows, w oparciu o które zostało utworzone konto Agenta autoryzacji, które chcesz usunąć.

5. Jeśli ręcznie wprowadziłeś nazwę konta systemu Windows, kliknij przycisk **Zezwól**, aby zdefiniować identyfikator zabezpieczeń konta (SID).

   Jeśli zdecydujesz się nie określać identyfikatora zabezpieczeń (SID) poprzez kliknięcie przycisku **Zezwól**, zostanie on określony w momencie wykonywania zadania na komputerze.

Zdefiniowanie identyfikatora zabezpieczeń konta Windows jest konieczne, aby sprawdzić, czy nazwa konta Windows została wprowadzona poprawnie. Jeśli konto systemu Windows nie istnieje na komputerze lub w zaufanej domenie, zadanie *Zarządzanie kontami Agenta autoryzacji* zakończy się błędem.

6. Zapisz swoje zmiany.

Jak usunąć konto Agenta autoryzacji za pomocą konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie **Zarządzanie kontami Agenta autoryzacji** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Na liście kont Agenta autoryzacji kliknij przycisk **Dodaj**.

   Spowoduje to uruchomienie Kreatora zarządzania kontem Agenta autoryzacji.

5. Wybierz typ polecenia **Usuń**.

6. Wybierz konto użytkownika. Możesz wybrać konto z listy kont domeny lub ręcznie wprowadzić nazwę konta.

7. Zapisz swoje zmiany.

8. Zaznacz pole obok zadania i kliknij przycisk **Uruchom**.

   W rezultacie, po zakończeniu zadania, przy następnym uruchomieniu komputera użytkownik nie będzie mógł ukończyć procedury uwierzytelniania i załadować systemu operacyjnego. Kaspersky Endpoint Security odmówi dostępu do zaszyfrowanych danych.

Aby wyświetlić listę użytkowników, którzy mogą ukończyć uwierzytelnianie za pomocą Agenta i załadować system operacyjny, musisz przejść do właściwości zarządzanego komputera.

Jak wyświetlić listę kont Agenta autoryzacji za pomocą Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W drzewie konsoli wybierz **Urządzenia**.

3. Kliknij dwukrotnie komputer, aby otworzyć okno właściwości komputera.

4. W oknie ustawień komputera wybierz sekcję **Zadania**.

5. Na liście zadań wybierz **Zarządzanie kontami Agenta autoryzacji** i otwórz właściwości zadania poprzez dwukrotne kliknięcie.

6. We właściwościach zadania wybierz sekcję **Ustawienia**.

   Dzięki temu będziesz mógł uzyskać dostęp do listy kont Agenta autoryzacji na tym komputerze. Tylko użytkownicy z listy mogą zakończyć uwierzytelnianie za pomocą Agenta i załadować system operacyjny.

Jak wyświetlić listę kont Agenta autoryzacji za pomocą konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Kliknij nazwę komputera, na którym chcesz wyświetlić listę kont Agenta autoryzacji.
3. We właściwościach komputera wybierz zakładkę **Zadania**.
4. We właściwościach zadania wybierz **Zarządzanie kontami Agenta autoryzacji**.
5. W właściwościach zadania wybierz zakładkę **Ustawienia aplikacji**.

Dzięki temu będziesz mógł uzyskać dostęp do listy kont Agenta autoryzacji na tym komputerze. Tylko użytkownicy z listy mogą zakończyć uwierzytelnianie za pomocą Agenta i załadować system operacyjny.

Używanie tokenów i kart inteligentnych z Agentem autoryzacji

Token lub karta inteligentna mogą zostać użyte do autoryzacji podczas dostępu do zaszyfrowanych dysków twardych. Aby to zrobić, musisz dodać plik certyfikatu elektronicznego tokena lub karty inteligentnej do zadania *Zarządzanie kontami Agenta autoryzacji*.

Użycie tokena lub karty inteligentnej jest możliwe tylko wtedy, gdy dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES256. Jeśli dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES56, dodanie pliku certyfikatu elektronicznego do polecenia zostanie odrzucone.

Kaspersky Endpoint Security obsługuje następujące tokeny, czytniki kart inteligentnych oraz karty inteligentne:

- SafeNet eToken PRO 64K (4.2b);
- SafeNet eToken PRO 72K Java;
- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;
- Athena IDProtect Laser;

- SafeNet eToken PRO 72K Java;
- Aladdin-RD JaCarta PKI.

Aby dodać plik certyfikatu elektronicznego tokena lub karty inteligentnej do polecenia tworzenia konta Agenta autoryzacji, w pierwszej kolejności zapisz plik, korzystając z oprogramowania firmy trzeciej do zarządzania certyfikatami.

Certyfikat tokena lub karty inteligentnej musi posiadać następujące parametry:

- Certyfikat musi być zgodny ze standardem X.509, a plik certyfikatu musi być kodowany przy użyciu algorytmu DER.
- Certyfikat zawiera klucz RSA o długości minimum 1024 bitów.

Jeśli certyfikat elektroniczny tokena lub karty inteligentnej nie spełnia tych wymagań, nie można załadować pliku certyfikatu do polecenia utworzenia konta Agenta autoryzacji.

Parametr `KeyUsage` certyfikatu musi posiadać wartość `keyEncipherment` lub `dataEncipherment`. Parametr `KeyUsage` określa cel certyfikatu. Jeśli parametr ma inną wartość, Kaspersky Security Center pobierze plik certyfikatu, ale wyświetli ostrzeżenie.

Jeśli użytkownik zgubił token lub kartę inteligentną, administrator musi dodać plik certyfikatu elektronicznego tokena lub karty inteligentnej do polecenia tworzenia konta Agenta autoryzacji. Następnie użytkownik musi przejść procedurę przywracania dostępu do zaszyfrowanych urządzeń lub przywracania danych na zaszyfrowanych urządzeniach.

Deszyfrowanie dysków twardych

Dyski twarde można odszyfrować nawet wtedy, gdy nie ma bieżącej licencji zezwalającej na szyfrowanie danych.

W celu odszyfrowania dysków twardych:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
4. Z listy rozwijalnej **Technologia szyfrowania** wybierz technologię, za pomocą której zostały zaszyfrowane dyski twarde.

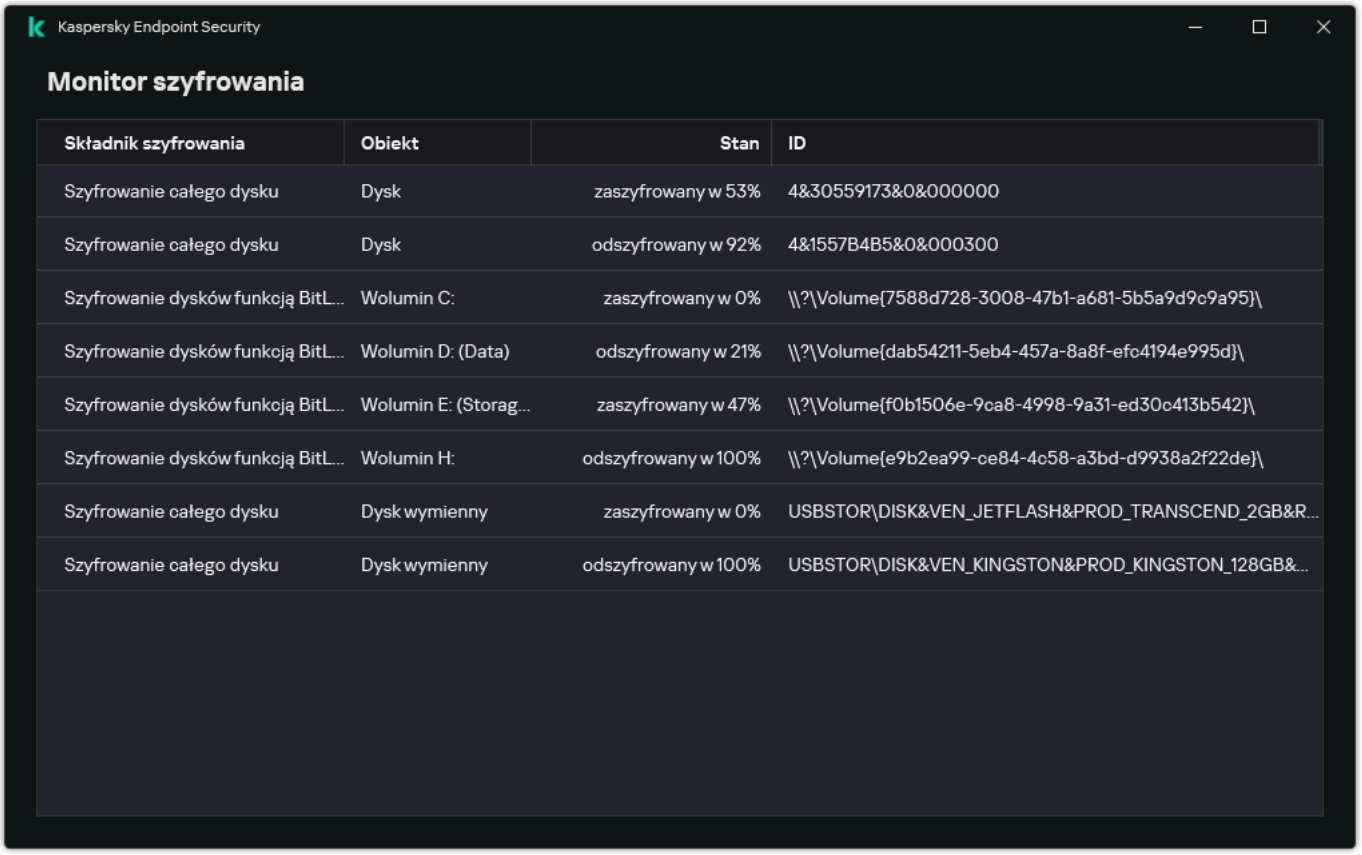
5. Wykonaj jedną z poniższych czynności:

- Z listy rozwijalnej **Tryb szyfrowania** wybierz opcję **Odszyfruj wszystkie dyski twarde**, jeśli chcesz odszyfrować wszystkie zaszyfrowane dyski twarde.
- Dodaj zaszyfrowane dyski twarde, które chcesz odszyfrować, do tabeli **Nie szyfruj następujących dysków twardych**.

  Ta opcja jest dostępna tylko dla technologii Kaspersky Disk Encryption.

6. Zapisz swoje zmiany.

Możesz użyć narzędzia Monitor szyfrowania, aby kontrolować szyfrowanie dysku lub proces deszyfrowania na komputerze użytkownika. Możesz uruchomić narzędzie Monitor szyfrowania z poziomu okna głównego aplikacji.



Monitor szyfrowania

Jeśli podczas deszyfrowania dysków twardych, zaszyfrowanych za pomocą technologii Kaspersky Disk Encryption, użytkownik zamknie lub uruchomi ponownie komputer, Agent autoryzacji załaduje się przed kolejnym uruchomieniem systemu operacyjnego. Kaspersky Endpoint Security wznawia deszyfrowanie dysku twardego po pomyślnej autoryzacji w Agencie autoryzacji i uruchomieniu systemu operacyjnego.

Jeśli podczas deszyfrowania dysków twardych, zaszyfrowanych za pomocą technologii Kaspersky Disk Encryption, system operacyjny przełączy się w tryb hibernacji, Agent autoryzacji załaduje się po wyjściu systemu operacyjnego z trybu hibernacji. Kaspersky Endpoint Security wznawia deszyfrowanie dysku twardego po pomyślnej autoryzacji w Agencie autoryzacji i uruchomieniu systemu operacyjnego. Po odszyfrowaniu dysku twardego, tryb hibernacji jest niedostępny, aż do pierwszego ponownego uruchomienia systemu operacyjnego.

Jeśli podczas deszyfrowania dysku twardego system operacyjny przejdzie w tryb uśpienia, Kaspersky Endpoint Security wznowi deszyfrowanie dysku twardego po wyjściu systemu operacyjnego z trybu uśpienia, bez wczytywania Agenta autoryzacji.

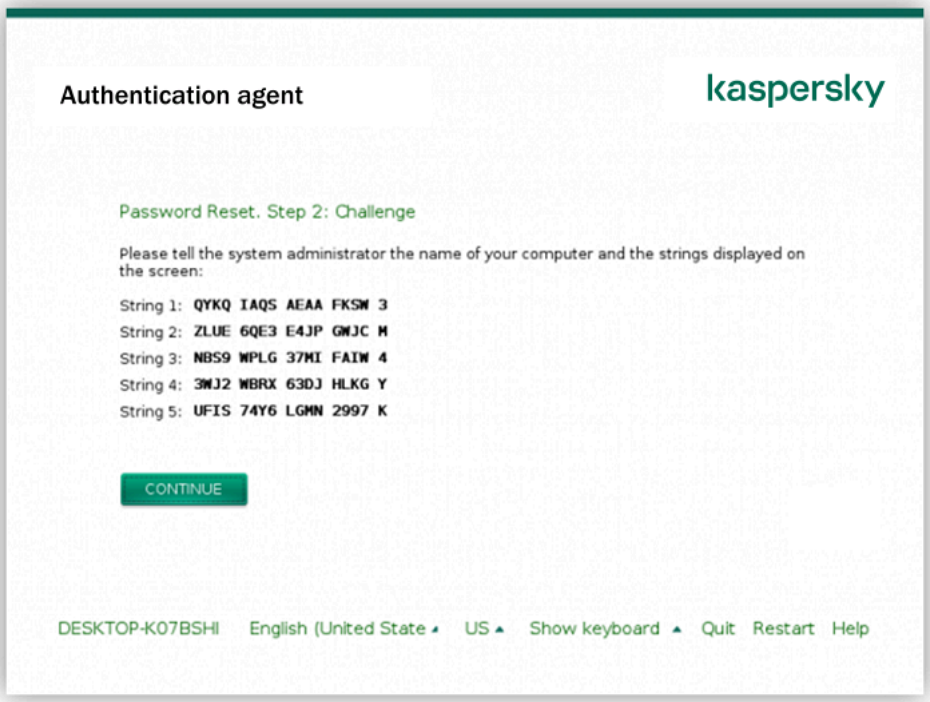
Przywracanie dostępu do dysku chronionego przez technologię Kaspersky Disk Encryption

Jeśli użytkownik zapomniał hasła dostępu do dysku twardego chronionego przez technologię Kaspersky Disk Encryption, musisz rozpocząć procedurę odzyskiwania (Żądanie-Odpowiedź). Możesz także użyć konta usługi, aby uzyskać dostęp do dysku twardego, jeśli ta funkcja jest włączona w ustawieniach szyfrowania dysku.

Przywracanie dostępu do systemowego dysku twardego

Przywrócenie dostępu do systemowego dysku twardego chronionego technologią Kaspersky Disk Encryption składa się z następujących kroków:

1. Użytkownik zgłasza blokady administratorowi (patrz rysunek poniżej).
2. Administrator wprowadza sekcje zgłoszeń do Kaspersky Security Center, odbiera sekcje odpowiedzi i zgłasza sekcje odpowiedzi użytkownikowi.
3. Użytkownik wprowadza sekcje odpowiedzi w interfejsie Agenta autoryzacji i uzyskuje dostęp do dysku twardego.



Przywracanie dostępu do systemowego dysku twardego chronionego przez technologię Kaspersky Disk Encryption

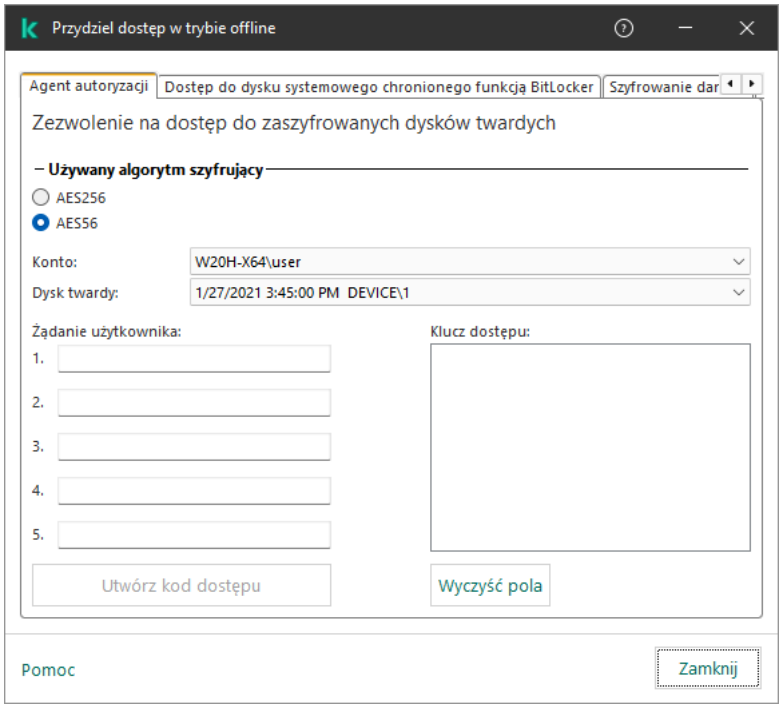
Aby rozpocząć procedurę odzyskiwania, użytkownik musi kliknąć przycisk **Forgot your password** w interfejsie Agenta autoryzacji.

Jak uzyskać sekcje odpowiedzi dla systemowego dysku twardego chronionego przez technologię Kaspersky Disk Encryption w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Urządzenia**.
3. W zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanych danych, i kliknij go prawym przyciskiem myszy, aby otworzyć menu kontekstowe.
4. Z otwartego menu kontekstowego wybierz **Przydziel dostęp w trybie offline**.
5. Spowoduje to otwarcie okna. Wybierz w nim zakładkę **Agent autoryzacji**.
6. W sekcji **Używany algorytm szyfrujący** wybierz algorytm szyfrowania: **AES56** lub **AES256**.

   Algorytm szyfrowania danych zależy od biblioteki szyfrowania AES zawartej w pakiecie dystrybucyjnym: *Silne szyfrowanie (AES256)* lub *Uproszczone szyfrowanie (AES56)*. Biblioteka szyfrowania AES jest instalowana wraz z aplikacją.
7. Z listy rozwijalnej **Konto** wybierz nazwę konta Agenta autoryzacji użytkownika, który prosi o przywrócenie dostępu do dysku.
8. Z listy rozwijalnej **Dysk twardy** wybierz zaszyfrowany dysk twardy, dla którego chcesz przywrócić dostęp.
9. W sekcji **Żądanie użytkownika** wprowadź sekcje ze zgłoszeniami użytkownika.

W rezultacie, zawartość sekcji z odpowiedziami na żądanie użytkownika dotyczące przywrócenia nazwy użytkownika i hasła dla konta Agenta autoryzacji będzie wyświetlana w polu **Klucz dostępu**. Prześlij zawartość sekcji odpowiedzi do użytkownika.



Przydzielanie dostępu w trybie offline

Jak uzyskać sekcje odpowiedzi dla systemowego dysku twardego chronionego przez technologię Kaspersky Disk Encryption w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasoby (urządzenia)**.
2. Zaznacz pole wyboru obok nazwy komputera, do dysku którego chcesz przywrócić dostęp.
3. Kliknij **Udziel dostępu do urządzenia w trybie offline**.
4. W otwartym oknie wybierz sekcję **Agent autoryzacji**.
5. Z listy rozwijalnej **Konto** wybierz nazwę konta Agenta autoryzacji utworzonego dla użytkownika, który prosi o przywrócenie nazwy konta i hasła dla Agenta autoryzacji.
6. Wprowadź sekcje żądań przesłane przez użytkownika.

   Zawartość sekcji z odpowiedziami na żądanie użytkownika dotyczące przywrócenia nazwy użytkownika i hasła dla konta Agenta autoryzacji będzie wyświetlana w dolnej części okna. Prześlij zawartość sekcji odpowiedzi do użytkownika.

Po zakończeniu procedury odzyskiwania Agent autoryzacji poprosi użytkownika o zmianę hasła.

Przywracanie dostępu do niesystemowego dysku twardego

Przywrócenie dostępu do niesystemowego dysku twardego chronionego technologią Kaspersky Disk Encryption składa się z następujących kroków:

1. Użytkownik wyśle plik zawierający żądanie dostępu do administratora.
2. Administrator dodaje plik żądania dostępu do Kaspersky Security Center, tworzy plik klucza dostępu i wysyła ten plik do użytkownika.
3. Użytkownik dodaje plik klucza dostępu do Kaspersky Endpoint Security i uzyskuje dostęp do dysku twardego.

Aby rozpocząć procedurę odzyskiwania, użytkownik musi spróbować uzyskać dostęp do dysku twardego. W rezultacie Kaspersky Endpoint Security utworzy plik dostępu do żądania (plik z rozszerzeniem KESDC), który użytkownik musi wysłać administratorowi, na przykład, za pośrednictwem poczty elektronicznej.

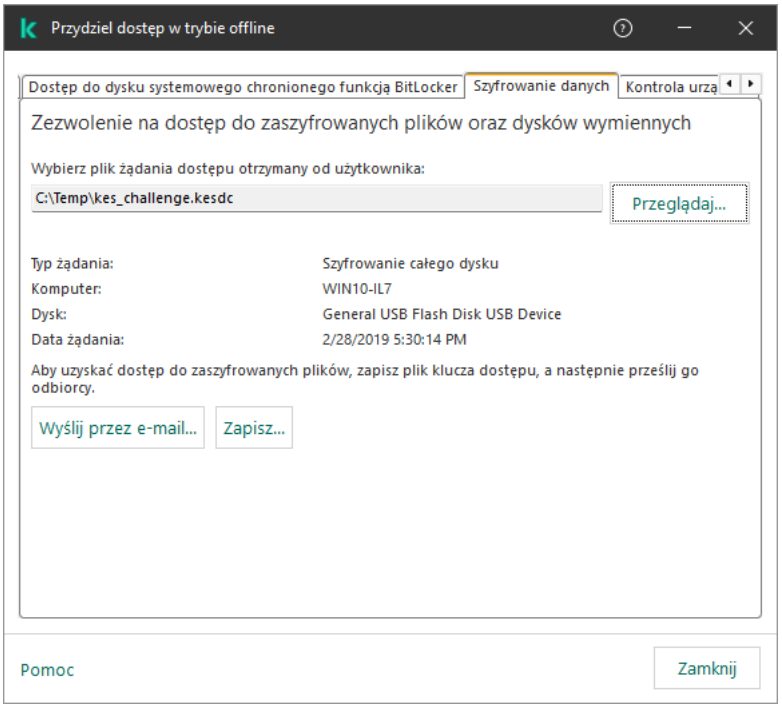
Jak uzyskać plik klucza dostępu do zaszyfrowanego niesystemowego dysku twardego w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Urządzenia**.
3. W zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanych danych, i kliknij go prawym przyciskiem myszy, aby otworzyć menu kontekstowe.
4. Z otwartego menu kontekstowego wybierz **Przydziel dostęp w trybie offline**.
5. Spowoduje to otwarcie okna. Wybierz w nim zakładkę **Szyfrowanie danych**.

6. Na zakładce **Szyfrowanie danych** kliknij przycisk **Przeglądaj**.

7. W oknie wyboru pliku dostępu do żądania określ ścieżkę do pliku otrzymanego od użytkownika.

Zobaczysz informacje o żądaniu użytkownika. Kaspersky Security Center wygeneruje plik klucza. Wyślij do użytkownika wygenerowany plik klucza dostępu do zaszyfrowanych danych. Lub zapisz plik dostępu i użyj dowolnej dostępnej metody, aby przenieść plik.



Przydzielanie dostępu w trybie offline

Jak uzyskać zaszyfrowany niesystemowy plik klucza dostępu do dysku twardego w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

2. Zaznacz pole wyboru obok nazwy komputera, do którego danych chcesz przywrócić dostęp.

3. Kliknij **Udziel dostępu do urządzenia w trybie offline**.

4. Wybierz **Szyfrowanie danych**.

5. Kliknij przycisk **Wybierz plik** i wybierz plik żądania dostępu otrzymany od użytkownika (plik z rozszerzeniem KESDC).

   Konsola Web Console wyświetli informacje o żądaniu. Obejmuje to nazwę komputera, na którym użytkownik żąda dostępu do pliku.

6. Kliknij przycisk **Zapisz klucz** i wybierz folder, aby zapisać plik klucza dostępu do zaszyfrowanych danych (plik z rozszerzeniem KESDR).

W rezultacie będziesz mógł uzyskać klucz dostępu do zaszyfrowanych danych, który będziesz musiał przekazać użytkownikowi.

Logowanie z użyciem konta usługi Agenta autoryzacji

Kaspersky Endpoint Security umożliwia dodanie konta usługi Agenta autoryzacji podczas szyfrowania dysku. Konto usługi jest niezbędne do uzyskania dostępu do komputera, na przykład, gdy użytkownik zapomni hasło. Możesz także użyć konta usługi jako konta zapasowego. Aby dodać konto, wybierz konto usługi w ustawieniach szyfrowania dysku i wprowadź nazwę konta użytkownika (domyślnie, `ServiceAccount`). Aby przeprowadzić uwierzytelnianie przy użyciu agenta, potrzebne będzie hasło jednorazowe.

Jak odnaleźć hasło jednorazowe w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Urządzenia**.
3. Kliknij dwukrotnie komputer, aby otworzyć okno właściwości komputera.
4. W oknie ustawień komputera wybierz sekcję **Zadania**.
5. Na liście zadań wybierz **Zarządzanie kontami Agenta autoryzacji** i otwórz właściwości zadania poprzez dwukrotne kliknięcie.
6. W oknie właściwości zadania wybierz sekcję **Ustawienia**.
7. Na liście kont wybierz konto usługi Agenta autoryzacji (na przykład: `WIN10-USER\ServiceAccount`).
8. Z listy rozwijalnej **Akcja** wybierz **Wyświetl konto**.
9. We właściwościach konta zaznacz pole **Wyświetl pierwotne hasło**.
10. Skopiuj hasło jednorazowe do zalogowania za pośrednictwem konta usługi.

Jak odnaleźć hasło jednorazowe w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Kliknij nazwę komputera, na którym chcesz wyświetlić listę kont Agenta autoryzacji.

   Spowoduje to otwarcie właściwości komputera.
3. We właściwościach komputera wybierz zakładkę **Zadania**.
4. We właściwościach zadania wybierz **Zarządzanie kontami Agenta autoryzacji**.
5. W właściwościach zadania wybierz zakładkę **Ustawienia aplikacji**.
6. Na liście kont wybierz konto usługi Agenta autoryzacji (na przykład: `WIN10-USER\ServiceAccount`).
7. We właściwościach konta zaznacz pole **Pokaż hasło**.
8. Skopiuj hasło jednorazowe do zalogowania za pośrednictwem konta usługi.

Kaspersky Endpoint Security automatycznie aktualizuje hasło za każdym razem, gdy użytkownik uwierzytelnia się za pośrednictwem konta usługi. Po uwierzytelnieniu przy użyciu agenta, musisz wprowadzić hasło do konta systemu Windows. Podczas logowania przy pomocy usługi konta nie możesz użyć technologii SSO.

Aktualizowanie systemu operacyjnego

Istnieje szereg specjalnych uwag dotyczących aktualizacji systemu operacyjnego komputera chronionego przez Szyfrowanie całego dysku (FDE). Zaktualizuj system operacyjny w następujący sposób: najpierw zaktualizuj system operacyjny na jednym komputerze, następnie zaktualizuj system operacyjny na małej części komputerów, a następnie zaktualizuj system operacyjny na wszystkich komputerach w sieci.

Jeśli korzystasz z technologii Kaspersky Disk Encryption, Agent autoryzacji jest ładowany przed uruchomieniem systemu operacyjnego. Korzystając z Agenta autoryzacji, użytkownik może zalogować się do systemu i uzyskać dostęp do zaszyfrowanych dysków. Następnie system operacyjny zaczyna się ładować. Jeśli rozpoczniesz aktualizację systemu operacyjnego na komputerze chronionym przy użyciu technologii Kaspersky Disk Encryption, Kreator aktualizacji systemu operacyjnego usunie Agenta autoryzacji. W rezultacie komputer może zostać zablokowany, ponieważ moduł ładujący systemu operacyjnego nie będzie mógł uzyskać dostępu do zaszyfrowanego dysku.

Funkcje aktualizacji systemu operacyjnego:

- **Aktualizowanie systemu operacyjnego za pomocą WSUS**. Możesz zaktualizować system operacyjny w zwykły sposób.
- **Aktualizacja systemu operacyjnego z obrazu ISO**. Aby zaktualizować system operacyjny, musisz określić folder ze sterownikami szyfrowania dysku Kaspersky. Aplikacja automatycznie kopiuje sterowniki do osobnego folderu. Wykonaj następujące czynności:

  1. Zamontuj obraz ISO.
  2. Rozpocznij instalację aktualizacji systemu za pomocą następującego klucza:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.1\reflect_drivers
     ```

Automatyczna aktualizacja systemu operacyjnego jest dostępna tylko wtedy, gdy na komputerze działa system Windows 10 w wersji 1607 (RS1) lub nowszy. Aby uaktualnić wcześniejsze wersje systemu operacyjnego, zaleca się najpierw odszyfrowanie dysku, potem przeprowadzenie aktualizacji systemu operacyjnego, a następnie zaszyfrowanie dysku.

Jeśli używasz technologii szyfrowania BitLocker, nie musisz odszyfrowywać dysków twardych, aby zaktualizować system Windows 10. Więcej informacji na temat działania BitLocker znajdziesz na stronie internetowej firmy Microsoft.

Eliminowanie błędów aktualizacji funkcjonalności szyfrowania

Szyfrowanie całego dysku jest aktualizowane, gdy poprzednia wersja aplikacji zostanie zaktualizowana do Kaspersky Endpoint Security for Windows 14.1.

Podczas uruchamiania aktualizacji funkcjonalności Szyfrowanie całego dysku mogą wystąpić następujące błędy:

- Brak możliwości zainicjowania aktualizacji.
- Urządzenie nie jest kompatybilne z Agentem autoryzacji.

W celu wyeliminowania błędów, które wystąpiły podczas uruchamiania procesu aktualizacji funkcjonalności Szyfrowanie całego dysku w nowej wersji aplikacji:

1. Odszyfruj dyski twarde.
2. Ponownie zaszyfruj dyski twarde.

Podczas aktualizacji funkcjonalności Szyfrowanie całego dysku mogą wystąpić następujące błędy:

- Brak możliwości zakończenia aktualizacji.
- Wycofanie aktualizacji Szyfrowania całego dysku zakończyło się błędem.

W celu wyeliminowania błędów, które wystąpiły podczas procesu aktualizacji funkcjonalności Szyfrowanie całego dysku:

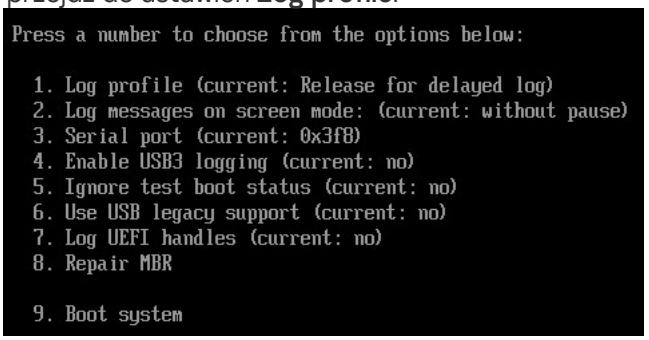
Przywróć dostęp do zaszyfrowanych urządzeń przy użyciu Narzędzia przywracania zaszyfrowanego urządzenia.

Śledzenie Agenta autoryzacji

Aplikacja zapisuje w pliku śledzenia informacje serwisowe o działaniu Agenta autoryzacji oraz informacje o działaniach użytkownika dotyczących Agenta autoryzacji.

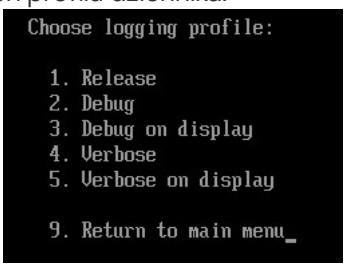
Aby włączyć śledzenie Agenta autoryzacji:

1. Włącz śledzenie Kaspersky Endpoint Security.
2. Uruchom ponownie komputer.
3. Jak tylko uruchomi się komputer z zaszyfrowanymi dyskami twardymi, wciśnij klawisz **F3**, aby wywołać okno konfiguracji ustawień Agenta autoryzacji.
4. Po uruchomieniu programu ładującego FDE wybierz menedżer rozruchu **KES (FDE <version>)**.
5. W menu menedżera rozruchu przejdź do ustawień **Log profile**.



Menu menedżera rozruchu

6. Wybierz poziom śledzenia w oknie ustawień profilu dziennika:



Poziomy śledzenia Agenta autoryzacji

- **Release**. Jeśli ta opcja jest zaznaczona, aplikacja nie rejestruje informacji o zdarzeniach Agenta autoryzacji w pliku śledzenia.
- **Debug**. Jeśli ta opcja jest zaznaczona, aplikacja rejestruje w pliku śledzenia informacje dotyczące działania Agenta autoryzacji oraz działań użytkownika wykonywanych na Agencie autoryzacji.
- **Debug on display**. Jeśli ta opcja jest zaznaczona, aplikacja rejestruje w pliku śledzenia informacje dotyczące działania Agenta autoryzacji oraz działań użytkownika wykonywanych na Agencie autoryzacji i przesyła je poprzez port COM.

  Jeśli komputer z zaszyfrowanymi dyskami twardymi jest podłączony do innego komputera poprzez port COM, zdarzenia Agenta autoryzacji mogą zostać sprawdzone z tego innego komputera.
- **Verbose**. Jeśli ta opcja jest zaznaczona, aplikacja rejestruje w pliku śledzenia szczegółowe informacje dotyczące działania Agenta autoryzacji oraz działań użytkownika wykonywanych na Agencie autoryzacji.

  Poziom szczegółowości wpisów w tej opcji jest wyższy niż w opcji **Debug**. Wysoki poziom szczegółowości wpisów może spowalniać uruchamianie Agenta autoryzacji i systemu operacyjnego.
- **Verbose on display**. Jeśli ta opcja jest zaznaczona, aplikacja rejestruje w pliku śledzenia szczegółowe informacje dotyczące działania Agenta autoryzacji oraz działań użytkownika wykonywanych na Agencie autoryzacji i przesyła je poprzez port COM.

  Poziom szczegółowości wpisów w tej opcji jest wyższy niż w opcji **Debug on display**. Wysoki poziom szczegółowości wpisów może spowalniać uruchamianie Agenta autoryzacji i systemu operacyjnego.

Po wybraniu poziomu śledzenia menedżer rozruchu ponownie wyświetli menu.

7. W menu menedżera rozruchu wybierz **Boot system**.

   Program ładujący FDE uruchamia Agenta autoryzacji.

   Odtwórz problem.

   Dane są zapisywane w pliku śledzenia Agenta autoryzacji, jeśli na komputerze lub podczas szyfrowania całego dysku znajdują się zaszyfrowane dyski twarde.

8. Aby zatrzymać proces śledzenia, wróć do okna Narzędzia pomocy technicznej i wyłącz śledzenie.

W rezultacie pliki śledzenia działania Agenta autoryzacji KES.SRV zostaną utworzone w folderze `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. W przeciwieństwie do innych plików śledzenia aplikacji, plik śledzenia Agenta autoryzacji nie jest wysyłany na serwer Kaspersky. Jeśli jest to konieczne, możesz ręcznie wysłać plik śledzenia Agenta autoryzacji do Kaspersky w celu przeprowadzenia jego analizy.

Modyfikowanie komunikatów pomocy Agenta Autoryzacji

Przed zmodyfikowaniem komunikatów pomocy Agenta Autoryzacji należy przejrzeć listę znaków obsługiwanych w środowisku wykonawczym przed uruchomieniem systemu (patrz poniżej).

W celu zmodyfikowania komunikaty pomocy Agenta Autoryzacji:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych** → **Ogólne ustawienia szyfrowania**.
4. W sekcji **Szablony** kliknij przycisk **Pomoc**.
5. W otwartym oknie wykonaj następujące czynności:
   - Wybierz zakładkę **Autoryzacja**, aby zmodyfikować treść wiadomości pomocy wyświetlanej w oknie Agenta autoryzacji podczas wprowadzania danych uwierzytelniających konta.
   - Wybierz zakładkę **Zmiana hasła**, aby zmodyfikować treść wiadomości pomocy wyświetlanej w oknie Agenta autoryzacji, gdy zmieniane jest hasło do konta Agenta autoryzacji.
   - Wybierz zakładkę **Przywracanie hasła**, aby zmodyfikować treść wiadomości pomocy wyświetlanej w oknie Agenta autoryzacji, gdy odzyskiwane jest hasło do konta Agenta autoryzacji.
6. Zmodyfikuj treść pomocy.

   Jeśli chcesz przywrócić oryginalny tekst, kliknij przycisk **Tryb domyślny**.

   Wprowadzana treść pomocy powinna zawierać 16 linijek lub mniej. Maksymalna długość wiersza to 64 znaki.
7. Zapisz swoje zmiany.

Ograniczona obsługa znaków w wiadomościach pomocy Agenta autoryzacji

W środowisku wykonawczym przed uruchomieniem systemu obsługiwane są następujące znaki Unicode:

- Alfabet łaciński podstawowy (0000 - 007F)
- Dodatkowe znaki alfabetu łacińskiego Latin-1 (0080 - 00FF)
- Łaciński rozszerzony Latin-A (0100 - 017F)
- Łaciński rozszerzony Latin-B (0180 - 024F)
- Oddzielone litery modyfikujące (02B0 - 02FF)

- Składające znaki diakrytyczne (0300 - 036F)
- Alfabet grecki i alfabet koptyjski (0370 - 03FF)
- Cyrylica (0400 - 04FF)
- Hebrajski (0590 - 05FF)
- Arabski (0600 - 06FF)
- Łaciński rozszerzony dodatkowy (1E00 - 1EFF)
- Znaki interpunkcyjne (2000 - 206F)
- Symbole walut (20A0 - 20CF)
- Symbole literopodobne (2100 - 214F)
- Figury geometryczne (25A0 - 25FF)
- Arabskie formy prezentacyjne B (FE70 - FEFF)

Znaki, które nie zostały wymienione na liście, nie są obsługiwane w środowisku wykonawczym przed uruchomieniem systemu. Nie jest zalecane używanie tych znaków w wiadomościach pomocy Agenta autoryzacji.

Usuwanie obiektów i danych pozostałych po testowym działaniu Agenta autoryzacji

Podczas dezinstalacji aplikacji, jeśli Kaspersky Endpoint Security wykryje obiekty i dane, które pozostały na dysku twardym po działaniu Agenta autoryzacji, dezinstalacja aplikacji zostanie przerwana i nie będzie możliwa, dopóki te obiekty nie zostaną usunięte.

Obiekty i dane mogą pozostać na dysku twardym po testowym działaniu Agenta autoryzacji tylko w wyjątkowych przypadkach. Na przykład wtedy, gdy komputer nie został uruchomiony ponownie po zastosowaniu profilu Kaspersky Security Center z ustawieniami szyfrowania lub gdy nie powiodło się uruchomienie aplikacji po testowym działaniu Agenta autoryzacji.

Obiekty i dane pozostające na dysku twardym po testowym działaniu Agenta autoryzacji można usunąć na następujące sposoby:

- Przy pomocy profilu Kaspersky Security Center.
- Przy użyciu Narzędzia przywracania zaszyfrowanego urządzenia.

W celu użycia profilu Kaspersky Security Center do usunięcia obiektów i danych, które pozostały po testowym działaniu Agenta autoryzacji:

1. Zastosuj na komputerze profil Kaspersky Security Center z ustawieniami skonfigurowanymi do deszyfracji wszystkich dysków twardych komputera.
2. Uruchom Kaspersky Endpoint Security.

Aby użyć Narzędzia przywracania w celu usunięcia obiektów i danych, które pozostały po testowym działaniu Agenta autoryzacji:

1. Uruchom plik o nazwie fdert.exe, który jest plikiem wykonywalnym narzędzia przywracania. Ten plik jest tworzony przez Kaspersky Endpoint Security.
2. W oknie Narzędzia przywracania wybierz wymagane urządzenie.
3. Kliknij **Skanuj**.
4. Jeśli po zdiagnozowaniu systemowego dysku twardego zostanie wyświetlony komunikat informujący, że po testowym działaniu Agenta autoryzacji pozostały obiekty i dane, kliknij **Usuń dane i obiekty AA**.

   Przycisk **Usuń dane i obiekty AA** jest dostępny tylko wtedy, gdy wykryto obiekty i dane pozostałe po testowym działaniu Agenta autoryzacji.

W celu usunięcia informacji o niekompatybilności aplikacji z Agentem autoryzacji:

w wierszu polecenia wprowadź `avp pbatestreset`.

Zarządzanie BitLocker

BitLocker to technologia szyfrowania wbudowana w systemy operacyjne Windows. Kaspersky Endpoint Security pozwala kontrolować i zarządzać funkcją Bitlocker za pomocą infrastruktury Kaspersky Next. BitLocker szyfruje woluminy logiczne. Funkcja BitLocker nie może być używana do szyfrowania dysków wymiennych. Więcej informacji na temat BitLocker można znaleźć w dokumentacji firmy Microsoft.

Podczas szyfrowania dysku program BitLocker umieszcza program rozruchowy i inne pliki pomocnicze w system partition. Ta partycja nie jest szyfrowana. System operacyjny automatycznie tworzy partycję systemową podczas instalacji systemu Windows. Jeśli dysk został całkowicie podzielony na partycje przed zainstalowaniem systemu Windows, system operacyjny nie będzie mógł utworzyć partycji systemowej. W takim przypadku po uruchomieniu szyfrowania dysku funkcją BitLocker, system operacyjny wyświetla użytkownikowi monit o ponowne podzielenie dysku na partycje i utworzenie partycji systemowej. Po utworzeniu partycji systemowej system operacyjny uruchamia szyfrowanie BitLocker.

Algorytm szyfrowania BitLocker nie jest zależny od wersji Biblioteki AES zawartej w pakiecie dystrybucyjnym (AES256 lub AES56). Szyfrowanie wykorzystuje wbudowaną bibliotekę szyfrującą systemu operacyjnego.

Domyślnie aplikacja używa algorytmu szyfrowania BitLocker o faktycznej długości klucza wynoszącej 256 bitów, aby szyfrować urządzenia, które nigdy nie były szyfrowane. Jeśli urządzenie zostało zaszyfrowane przed instalacją aplikacji, algorytm szyfrowania może być inny. Aby uzyskać szczegółowe informacje na temat wyboru algorytmu szyfrowania, odwiedź witrynę pomocy technicznej firmy Microsoft. Od wersji 12.9 program Kaspersky Endpoint Security wysyła oryginalny klucz odzyskiwania dla urządzeń, które zostały wcześniej zaszyfrowane przez aplikacje innych firm, do Kaspersky Security Center.

Funkcja BitLocker zapewnia bezpieczne przechowywanie kluczy dostępu za pomocą zaufanego modułu platformy. *Trusted Platform Module* (TPM) to mikroczip zaprojektowany do zapewnienia podstawowych funkcji związanych z bezpieczeństwem (na przykład, do przechowywania kluczy szyfrowania). Trusted Platform Module jest zazwyczaj instalowany w płycie głównej komputera i komunikuje się z wszystkimi pozostałymi komponentami systemu za pośrednictwem magistrali sprzętowej. Korzystanie z modułu TPM jest najbezpieczniejszym sposobem przechowywania kluczy dostępu funkcji BitLocker, ponieważ moduł TPM zapewnia weryfikację integralności systemu przed uruchomieniem. Nadal możesz szyfrować dyski na komputerze bez modułu TPM. W takim przypadku klucz dostępu zostanie zaszyfrowany przy użyciu hasła. Funkcja BitLocker używa następujących metod uwierzytelniania:

- TPM.
- TPM i PIN.
- Hasło.

Po zaszyfrowaniu systemowego dysku twardego użytkownik musi przejść uwierzytelnianie funkcją BitLocker, aby uruchomić system operacyjny. Po uwierzytelnieniu BitLocker umożliwia użytkownikowi zalogowanie się. Funkcja BitLocker nie obsługuje technologii pojedynczego logowania (SSO).

Po zaszyfrowaniu dysku funkcja BitLocker tworzy klucz odzyskiwania. Kaspersky Endpoint Security wysyła klucz odzyskiwania do Kaspersky Security Center, aby umożliwić przywrócenie dostępu do dysku, na przykład, jeśli użytkownik zapomniał hasło.

Jeśli użytkownik zaszyfruje dysk przy użyciu funkcji BitLocker, Kaspersky Endpoint Security wyśle klucz odzyskiwania i informacje o szyfrowaniu dysku do Kaspersky Security Center.

Jeśli używasz zasad grupy Windows, wyłącz zarządzanie funkcją BitLocker w ustawieniach zasad. Ustawienia zasad Windows mogą kolidować z ustawieniami zasad Kaspersky Endpoint Security. Podczas szyfrowania dysku mogą wystąpić błędy.

Uruchamianie Szyfrowania dysków funkcją BitLocker

Przed uruchomieniem szyfrowania całego dysku zalecane jest upewnienie się, że komputer nie jest zainfekowany. W tym celu uruchom zadanie Pełne skanowanie lub Skanowanie obszarów krytycznych. Wykonanie szyfrowania całego dysku na komputerze, który jest zainfekowany rootkitem, może spowodować, że komputer przestanie działać.

Aby użyć Szyfrowania dysków funkcją BitLocker na komputerach z systemem operacyjnym Windows dla serwerów, może być wymagana instalacja komponentu Szyfrowanie dysków funkcją BitLocker. Zainstaluj komponent za pomocą narzędzi systemu operacyjnego (Kreator dodawania ról i komponentów). Więcej informacji o instalowaniu szyfrowania dysków funkcją BitLocker można znaleźć w dokumentacji firmy Microsoft.

Jak uruchomić szyfrowanie dysków funkcją BitLocker za pomocą Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.

4. Z listy rozwijalnej **Technologia szyfrowania** wybierz **Szyfrowanie dysków funkcją BitLocker**.

5. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Zaszyfruj wszystkie dyski twarde**.

   Jeśli na komputerze jest zainstalowanych kilka systemów operacyjnych, po szyfrowaniu będziesz mógł załadować tylko ten system operacyjny, na którym szyfrowanie zostało wykonane.

6. Skonfiguruj zaawansowane opcje szyfrowania dysków funkcją BitLocker (patrz tabela poniżej).

7. Zapisz swoje zmiany.

Jak uruchomić szyfrowanie dysków funkcją BitLocker za pośrednictwem konsoli Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.

5. Wybierz technologię **Szyfrowanie dysku BitLocker**.

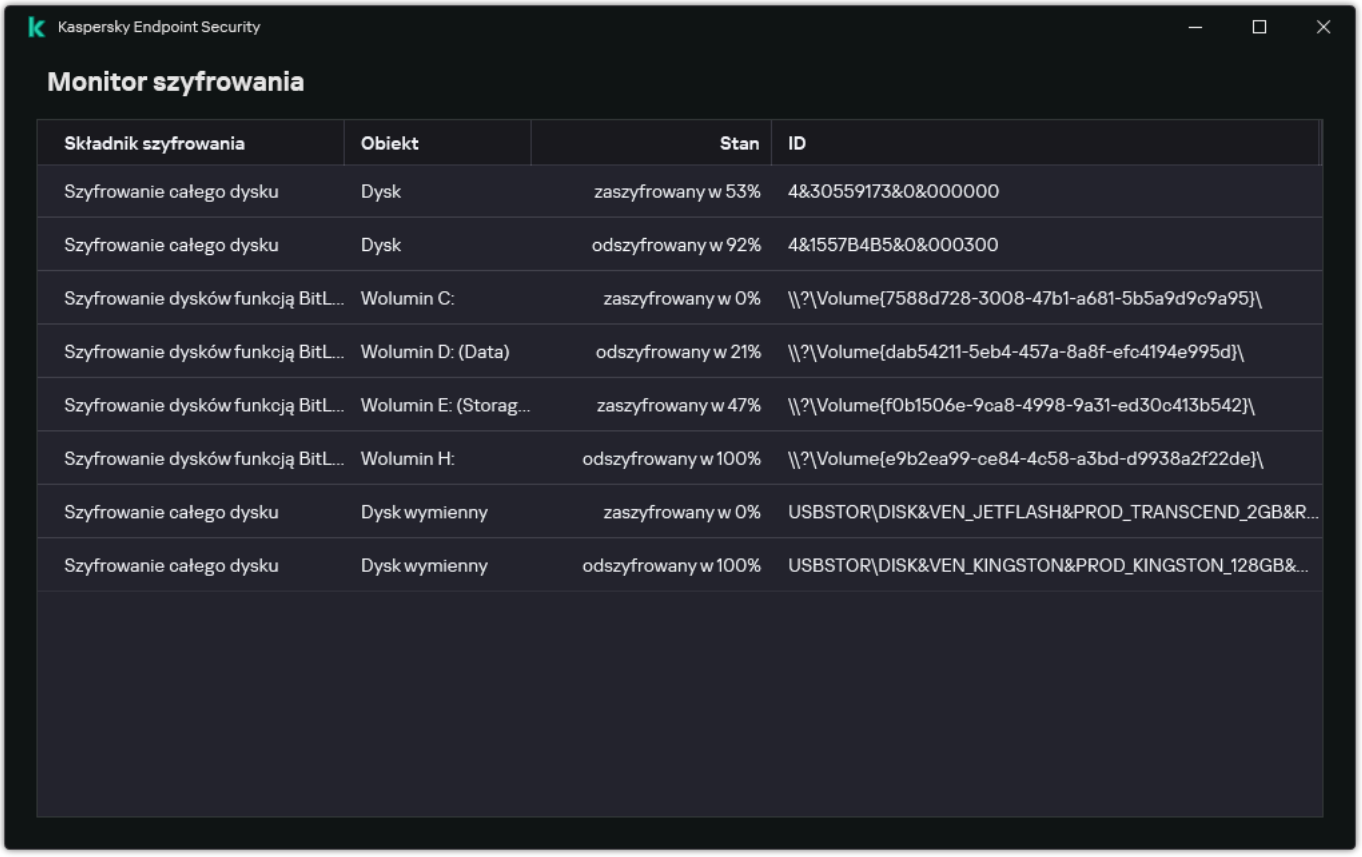
6. W bloku **Działania na urządzeniach** wybierz **Zaszyfruj wszystkie dyski twarde**.

   Jeśli na komputerze jest zainstalowanych kilka systemów operacyjnych, po szyfrowaniu będziesz mógł załadować tylko ten system operacyjny, na którym szyfrowanie zostało wykonane.

7. Skonfiguruj zaawansowane opcje szyfrowania dysków funkcją BitLocker (patrz tabela poniżej).

8. Zapisz swoje zmiany.

Możesz użyć narzędzia Monitor szyfrowania, aby kontrolować szyfrowanie dysku lub proces deszyfrowania na komputerze użytkownika. Możesz uruchomić narzędzie Monitor szyfrowania z poziomu okna głównego aplikacji.



Monitor szyfrowania

Po zastosowaniu zasady aplikacja wyświetli następujące zapytania w zależności od ustawień uwierzytelniania:

- Tylko TPM. Wprowadzanie przez użytkownika nie jest wymagane. Dysk zostanie zaszyfrowany po ponownym uruchomieniu komputera.
- TPM + PIN / Hasło. Jeśli moduł TPM jest dostępny, pojawi się konto z prośbą o podanie kodu PIN. Jeśli moduł TPM nie jest dostępny, pojawi się okno z prośbą o wpisanie hasła do autoryzacji przed rozruchem.
- Tylko hasło. Zostanie wyświetlone okno z prośbą o wpisanie hasła do autoryzacji przed rozruchem.

Jeśli w systemie operacyjnym komputera jest włączona funkcja zgodności ze standardami FIPS (Federal Information Processing Standard), wówczas w systemie Windows 8 i wcześniejszych wersjach będzie wyświetlane okno z żądaniem podłączenia urządzenia magazynującego w celu zapisania pliku klucza odzyskiwania. Możesz zapisać kilka plików kluczy odzyskiwania na jednym urządzeniu magazynującym.

Po ustawieniu hasła lub kodu PIN funkcja BitLocker poprosi o ponowne uruchomienie komputera w celu dokończenia szyfrowania. Następnie użytkownik musi przejść procedurę uwierzytelniania funkcją BitLocker. Po procedurze uwierzytelnienia użytkownik musi zalogować się do systemu. Po załadowaniu systemu operacyjnego funkcja BitLocker zakończy szyfrowanie.

Jeśli nie ma dostępu do kluczy szyfrowania, użytkownik może poprosić administratora sieci lokalnej o dostarczenie klucza odzyskiwania (jeśli klucz odzyskiwania nie został wcześniej zapisany na urządzeniu magazynującym lub został utracony).

Parametr	Opis
Włącz korzystanie z uwierzytelniania BitLocker wymagającego wprowadzania danych z klawiatury przed uruchomieniem na tabletach	Korzystanie z uwierzytelniania wymagającego wprowadzenia danych przed rozruchem nawet wtedy, gdy platforma nie oferuje takiej możliwości (na przykład klawiatury dotykowe na tabletach). Ekran dotykowy komputerów typu tablet nie jest dostępny w środowisku wykonawczym przed uruchomieniem systemu. Aby zakończyć uwierzytelnianie funkcji BitLocker na komputerach typu tablet, użytkownik musi, na przykład, podłączyć klawiaturę USB. Jeśli pole jest zaznaczone, użycie uwierzytelniania wymagającego wprowadzenia danych przed rozruchem jest dozwolone. Zalecane jest korzystanie z tego ustawienia tylko na urządzeniach, na których znajdują się alternatywne narzędzia do wprowadzania danych przed rozruchem, na przykład klawiatura USB będąca dodatkiem do klawiatury dotykowej. Jeśli pole jest odznaczone, szyfrowanie dysków funkcją BitLocker nie jest możliwe na tabletach.
Użyj szyfrowania sprzętowego (dla Windows 8 i nowszych)	Jeśli pole jest zaznaczone, aplikacja stosuje szyfrowanie sprzętu. Umożliwia to przyspieszenie szyfrowania i zużycie mniejszej ilości zasobów.
Szyfruj tylko zajętą przestrzeń dysku (dla Windows 8 i nowszych)	To pole włącza/wyłącza opcję ograniczającą obszar szyfrowania tylko do zajmowanych sektorów dysku twardego. To ograniczenie pozwala na skrócenie czasu szyfrowania. Włączenie lub wyłączenie funkcji **Szyfruj tylko zajętą przestrzeń dysku (redukuje czas szyfrowania)** po rozpoczęciu szyfrowania nie powoduje zmodyfikowania tego ustawienia, aż do odszyfrowania dysków twardych. Przed rozpoczęciem szyfrowania należy zaznaczyć lub odznaczyć to pole. Jeśli pole jest zaznaczone, zostaną zaszyfrowane tylko te obszary dysku twardego, które są zajęte przez pliki. Kaspersky Endpoint Security automatycznie szyfruje nowe dane po ich dodaniu. Jeśli pole jest odznaczone, cały dysk twardy jest szyfrowany, w tym fragmenty wcześniej usuniętych i zmodyfikowanych plików. Ta opcja jest zalecana dla nowych dysków twardych, których dane nie zostały zmodyfikowane ani usunięte. Jeśli stosujesz szyfrowanie na dysku twardym, który jest już w użyciu, zalecane jest zaszyfrowanie całego dysku twardego. Zapewni to ochronę wszystkich danych, także tych usuniętych, które potencjalnie można odzyskać. Domyślnie to pole wyboru nie jest zaznaczone.

Parametr	Opis
Metoda uwierzytelniania	**Tylko hasło (dla Windows 8 i nowszych)** Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security wyświetli pytanie o wprowadzenie hasła podczas próby uzyskania dostępu do zaszyfrowanego dysku. Ta opcja może zostać wybrana, gdy moduł TPM nie jest używany. **Moduł TPM (Trusted platform module)** Jeśli ta opcja jest zaznaczona, BitLocker korzysta z modułu TPM (Trusted Platform Module). *Trusted Platform Module* (TPM) to mikroczip zaprojektowany do zapewnienia podstawowych funkcji związanych z bezpieczeństwem (na przykład, do przechowywania kluczy szyfrowania). Trusted Platform Module jest zazwyczaj instalowany w płycie głównej komputera i komunikuje się z wszystkimi pozostałymi komponentami systemu za pośrednictwem magistrali sprzętowej. Dla komputerów działających pod kontrolą systemu Windows 7 lub Windows Server 2008 R2 dostępne jest tylko szyfrowanie przy użyciu modułu TPM. Jeśli moduł TPM nie jest zainstalowany, szyfrowanie funkcją BitLocker nie jest możliwe. Użycie hasła na tych komputerach nie jest obsługiwane. Urządzenie posiadające moduł Trusted Platform Module może tworzyć klucze szyfrowania, które mogą zostać odszyfrowane tylko z pomocą urządzenia. TPM szyfruje klucze szyfrowania, korzystając z własnych kluczy głównych magazynowania. Klucz główny magazynowania jest przechowywany w Trusted Platform Module. Zapewnia to dodatkowy poziom ochrony przed próbami zhakowania kluczy szyfrowania. To ustawienie jest wybrane domyślnie. Możesz ustawić dodatkową warstwę ochrony dostępu do klucza szyfrowania i zaszyfrować klucz z hasłem lub kodu PIN: • **Użyj kodu PIN dla TPM**. Jeśli to pole jest zaznaczone, użytkownik może użyć kodu PIN do uzyskania dostępu do klucza szyfrowania przechowywanego w Trusted Platform Module (TPM). Jeśli to pole jest odznaczone, użytkownicy nie mogą korzystać z kodów PIN. Aby uzyskać dostęp do klucza szyfrowania, użytkownik musi wprowadzić hasło. • **Moduł TPM (Trusted platform module) lub hasło, jeśli moduł TPM jest niedostępny**. Jeśli ta opcja jest zaznaczona, użytkownik może użyć hasła w celu uzyskania dostępu do kluczy szyfrowania, gdy moduł Trusted Platform Module (TPM) jest niedostępny. Jeśli pole wyboru zostanie odznaczone, a TPM nie jest dostępny, szyfrowanie całego dysku nie rozpocznie się. Wybraną metodę uwierzytelniania należy skonfigurować, określając wymagania dotyczące hasła lub kodu PIN: • **Minimalna długość kodu PIN (znaki)**. • **Minimalna długość hasła (znaki)**. • **Ogranicz okres ważności hasła / numeru PIN dla TPM (liczba dni)**. • **Użyj ulepszonego kodu PIN (litery i cyfry)**. *Rozszerzony kod PIN* umożliwia używanie innych znaków jako dodatku do znaków numerycznych: wielkich i małych liter alfabetu łacińskiego, znaków specjalnych i spacji.
Automatycznie odtwórz klucz odzyskiwania (liczba dni)	Umożliwia automatyczne aktualizowanie hasła w celu przywrócenia dostępu do dysku chronionego funkcją BitLocker. Jeśli to pole jest zaznaczone, musisz wybrać okres ważności hasła klucza odzyskiwania. Zapobiega to ponownemu wykorzystaniu hasła klucza odzyskiwania.

Deszyfrowanie dysku twardego chronionego przez funkcję BitLocker

Użytkownicy mogą odszyfrować dysk za pomocą systemu operacyjnego (funkcja *Wyłącz funkcję BitLocker*). Następnie Kaspersky Endpoint Security poprosi użytkownika o ponowne zaszyfrowanie dysku. Kaspersky Endpoint Security będzie monitował o zaszyfrowanie dysku, chyba że włączysz deszyfrowanie dysku w zasadzie.

Jak odszyfrować dysk twardy chroniony funkcją BitLocker za pomocą Konsoli administracyjnej (MMC)?

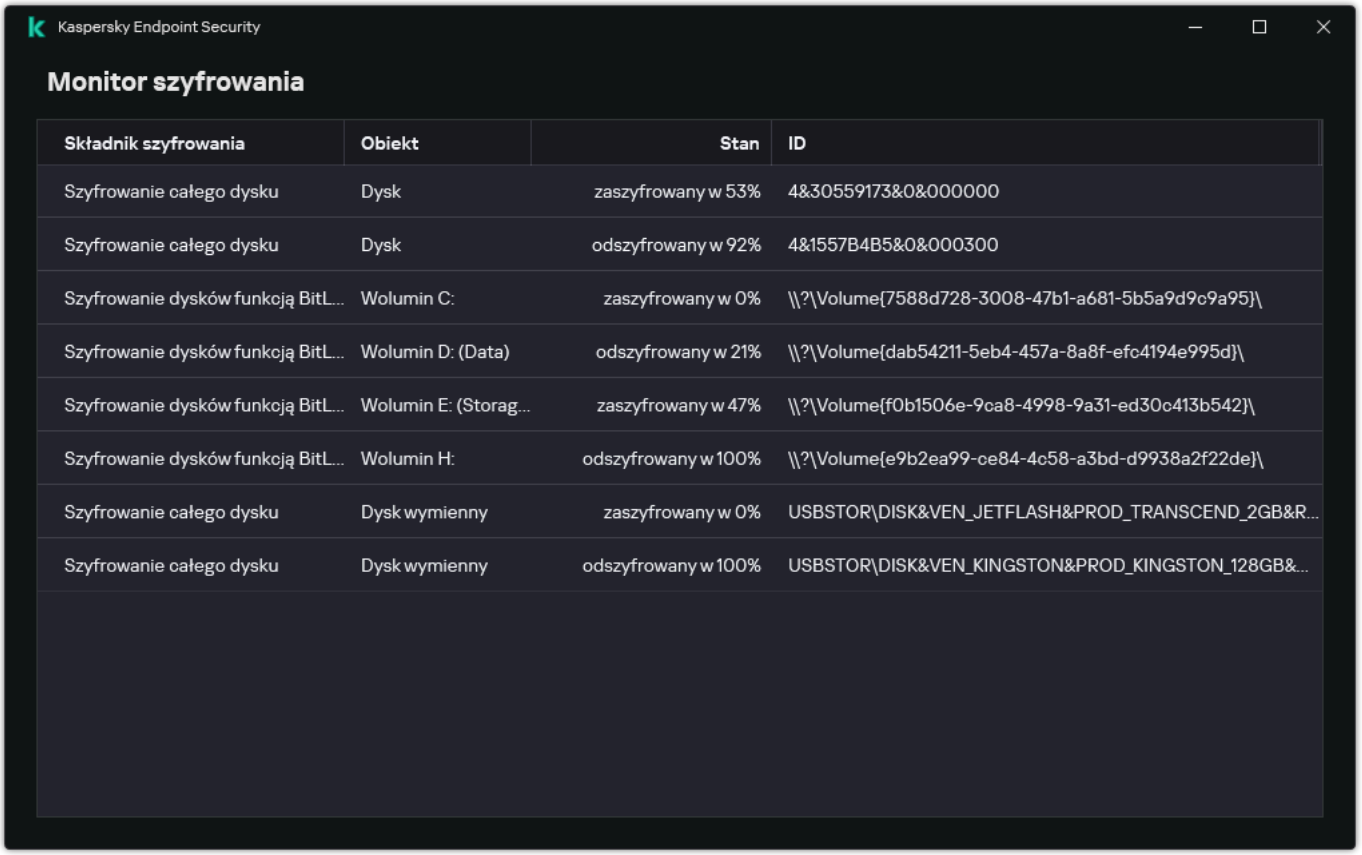
1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych → Szyfrowanie całego dysku**.

4. Z listy rozwijalnej **Technologia szyfrowania** wybierz **Szyfrowanie dysków funkcją BitLocker**.
5. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Odszyfruj wszystkie dyski twarde**.
6. Zapisz swoje zmiany.

Jak odszyfrować dysk twardy zaszyfrowany przy pomocy funkcji BitLocker w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
5. Wybierz technologię **Szyfrowanie dysku BitLocker**.
6. W bloku **Działania na urządzeniach** wybierz **Odszyfruj wszystkie dyski twarde**.
7. Zapisz swoje zmiany.

Możesz użyć narzędzia Monitor szyfrowania, aby kontrolować szyfrowanie dysku lub proces deszyfrowania na komputerze użytkownika. Możesz uruchomić narzędzie Monitor szyfrowania z poziomu okna głównego aplikacji.



Monitor szyfrowania

Przywracanie dostępu do dysku chronionego funkcją BitLocker

Jeśli użytkownik zapomniał hasła dostępu do dysku twardego zaszyfrowanego przez BitLocker, musisz rozpocząć procedurę odzyskiwania (Żądanie-Odpowiedź).

Jeśli system operacyjny komputera posiada włączony tryb kompatybilności FIPS (Federal Information Processing), wówczas w systemie Windows 8 i starszych plik klucza odzyskiwania jest zapisywany na nośniku wymiennym przed szyfrowaniem. Aby odzyskać dostęp do dysku, włóż nośnik wymienny i postępuj zgodnie z instrukcjami na ekranie.

Przywrócenie dostępu do dysku twardego zaszyfrowanego przez BitLocker składa się z następujących kroków:

1. Użytkownik informuje administratora o identyfikatorze klucza odzyskiwania (patrz rysunek poniżej).
2. Administrator weryfikuje identyfikator klucza odzyskiwania we właściwościach komputera w Kaspersky Security Center. Identyfikator podany przez użytkownika musi być zgodny z identyfikatorem wyświetlanym we właściwościach komputera.
3. Jeśli identyfikatory klucza odzyskiwania są zgodne, administrator dostarcza użytkownikowi klucz odzyskiwania lub wysyła plik klucza odzyskiwania.

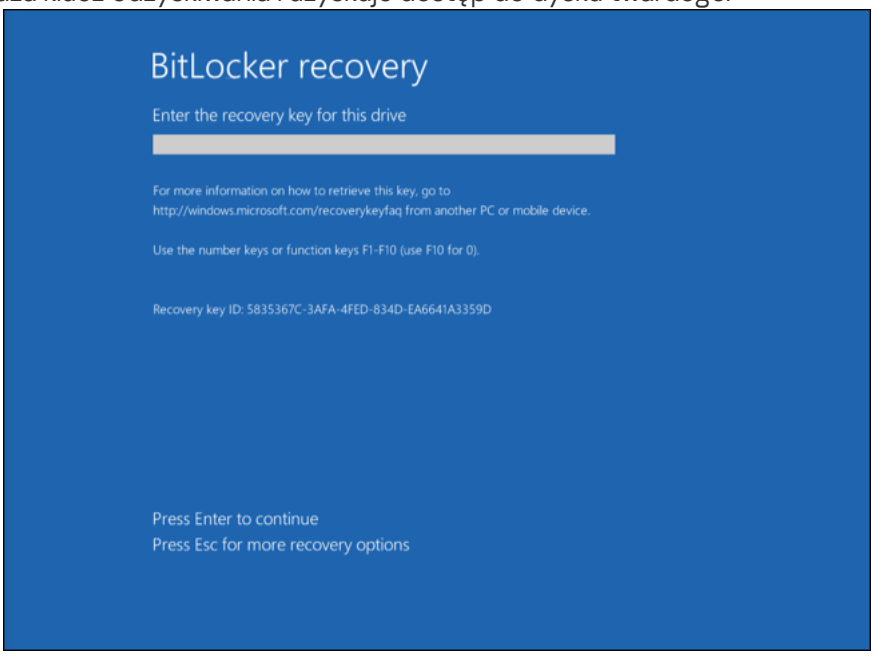
   Plik klucza odzyskiwania jest używany dla komputerów z następującymi systemami operacyjnymi:

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011
   - Windows Server 2012

   W przypadku wszystkich innych systemów operacyjnych używany jest klucz odzyskiwania.

   Aby zapobiec ponownemu wykorzystywaniu klucza odzyskiwania, możesz skonfigurować automatyczną aktualizację hasła w ustawieniach zasad.

4. Użytkownik wprowadza klucz odzyskiwania i uzyskuje dostęp do dysku twardego.



Przywracanie dostępu do dysku systemowego zaszyfrowanego funkcją BitLocker

Przywracanie dostępu do dysku systemowego

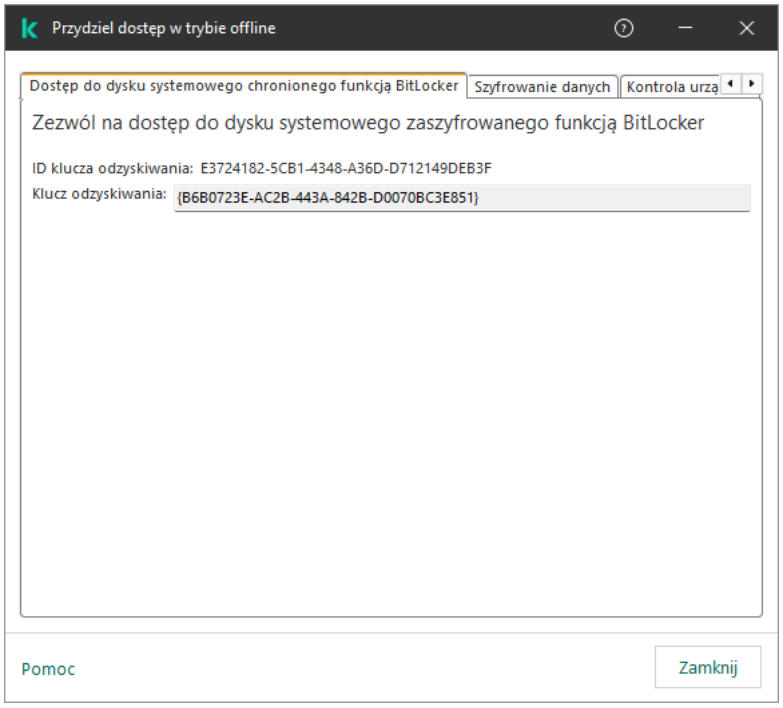
Aby rozpocząć procedurę odzyskiwania, użytkownik musi wcisnąć klawisz **Esc** na etapie uwierzytelniania przed uruchomieniem.

Jak wyświetlić klucz odzyskiwania dla dysku systemowego zaszyfrowanego przy pomocy funkcji BitLocker w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zarządzane urządzenia**.
3. W zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanych danych, i kliknij go prawym przyciskiem myszy, aby otworzyć menu kontekstowe.
4. Z otwartego menu kontekstowego wybierz **Przydziel dostęp w trybie offline**.
5. Spowoduje to otwarcie okna. Wybierz w nim zakładkę **Dostęp do dysku systemowego chronionego funkcją BitLocker**.
6. Zapytaj użytkownika o ID klucza odzyskiwania wskazany w oknie do wprowadzenia hasła do funkcji BitLocker, a następnie porównaj go z ID w polu **ID klucza odzyskiwania**.

Jeśli numery ID nie pasują do siebie, ten klucz nie służy do przywrócenia dostępu do określonego dysku systemowego. Upewnij się, że nazwa wybranego komputera odpowiada nazwie komputera użytkownika.

W rezultacie będziesz mieć dostęp do klucza odzyskiwania lub pliku klucza odzyskiwania, który będzie musiał zostać przesłany do użytkownika.



Przywracanie dostępu do dysku zaszyfrowanego funkcją BitLocker

Jak wyświetlić klucz odzyskiwania dla dysku systemowego zaszyfrowanego przy pomocy funkcji BitLocker w konsoli Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Zaznacz pole wyboru obok nazwy komputera, do dysku którego chcesz przywrócić dostęp.
3. Kliknij **Udziel dostępu do urządzenia w trybie offline**.
4. W otwartym oknie wybierz sekcję **BitLocker**.
5. Sprawdź identyfikator klucza odzyskiwania. Identyfikator podany przez użytkownika musi być zgodny z identyfikatorem wyświetlanym w ustawieniach komputera.

   Jeśli numery ID nie pasują do siebie, ten klucz nie służy do przywrócenia dostępu do określonego dysku systemowego. Upewnij się, że nazwa wybranego komputera odpowiada nazwie komputera użytkownika.

6. Kliknij **Uzyskaj klucz**.

W rezultacie będziesz mieć dostęp do klucza odzyskiwania lub pliku klucza odzyskiwania, który będzie musiał zostać przesłany do użytkownika.

Po załadowaniu systemu operacyjnego program Kaspersky Endpoint Security wyświetli monit o zmianę hasła lub kodu PIN. Po ustawieniu nowego hasła lub kodu PIN, funkcja BitLocker utworzy nowy klucz odzyskiwania i wyśle go do Kaspersky Security Center. W wyniku tego działania klucz odzyskiwania oraz plik klucza odzyskiwania zostaną zaktualizowane. Jeśli użytkownik nie zmienił hasła, możesz użyć starego klucza odzyskiwania przy następnym ładowaniu systemu operacyjnego.

Komputery z systemem Windows 7 nie pozwalają na zmianę hasła lub kodu PIN. Po wprowadzeniu klucza odzyskiwania i załadowaniu systemu operacyjnego, program Kaspersky Endpoint Security nie wyświetli monitu o zmianę hasła lub kodu PIN. Dlatego też niemożliwe jest ustawienie nowego hasła lub kodu PIN. Ten problem jest spowodowany przez szczególne właściwości systemu operacyjnego. Aby kontynuować, należy ponownie zaszyfrować dysk twardy.

Przywracanie dostępu do dysku niesystemowego

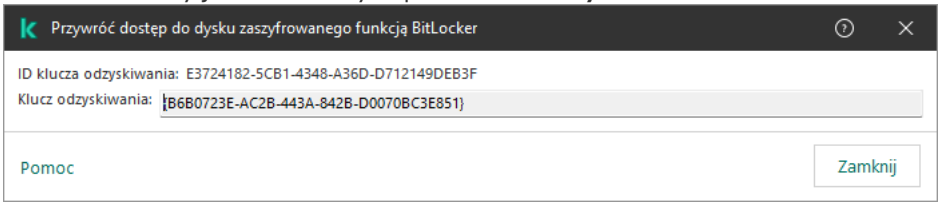
Aby rozpocząć procedurę odzyskiwania, użytkownik musi kliknąć odnośnik **Nie pamiętam hasła** w oknie zapewniającym dostęp do dysku. Po uzyskaniu dostępu do zaszyfrowanego dysku, użytkownik może włączyć automatyczne odblokowywanie dysku podczas uwierzytelniania systemu Windows w ustawieniach funkcji BitLocker.

Jak wyświetlić klucz odzyskiwania dla dysku niesystemowego zaszyfrowanego przez funkcję BitLocker w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz folder **Zaawansowane** → **Ochrona i szyfrowanie danych** → **Zaszyfrowane dyski**.
3. W obszarze roboczym wybierz zaszyfrowane urządzenie, dla którego chcesz utworzyć plik klucza dostępu, a z menu kontekstowego urządzenia wybierz **Uzyskaj dostęp do urządzenia w Kaspersky Endpoint Security**.
4. Zapytaj użytkownika o ID klucza odzyskiwania wskazany w oknie do wprowadzenia hasła do funkcji BitLocker, a następnie porównaj go z ID w polu **ID klucza odzyskiwania**.

   Jeśli numery ID nie pasują do siebie, ten klucz nie służy do przywrócenia dostępu do określonego dysku. Upewnij się, że nazwa wybranego komputera odpowiada nazwie komputera użytkownika.

5. Wyślij do użytkownika klucz, który jest wskazany w polu **Klucz odzyskiwania**.



Przywracanie dostępu do dysku zaszyfrowanego funkcją BitLocker

Jak wyświetlić klucz odzyskiwania dla dysku niesystemowego zaszyfrowanego przy pomocy funkcji BitLocker w konsoli Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Operacje** → **Ochrona i szyfrowanie danych** → **Zaszyfrowane dyski**.
2. Zaznacz pole wyboru obok nazwy komputera, do dysku którego chcesz przywrócić dostęp.

3. Kliknij **Udziel dostępu do urządzenia w trybie offline**.

   Spowoduje to uruchomienie Kreatora umożliwiającego uzyskanie dostępu do urządzenia.

4. Postępuj zgodnie z instrukcjami Kreatora, aby przyznać dostęp do urządzenia:

   a. Wybierz wtyczkę **Kaspersky Endpoint Security for Windows**

   b. Sprawdź identyfikator klucza odzyskiwania. Identyfikator podany przez użytkownika musi być zgodny z identyfikatorem wyświetlanym w ustawieniach komputera.

   > Jeśli numery ID nie pasują do siebie, ten klucz nie służy do przywrócenia dostępu do określonego dysku systemowego. Upewnij się, że nazwa wybranego komputera odpowiada nazwie komputera użytkownika.

   c. Kliknij **Uzyskaj klucz**.

W rezultacie będziesz mieć dostęp do klucza odzyskiwania lub pliku klucza odzyskiwania, który będzie musiał zostać przesłany do użytkownika.

Wstrzymywanie ochrony funkcją BitLocker w celu zaktualizowania oprogramowania

Istnieje liczba kwestii specjalnych dla aktualizacji systemu operacyjnego, instalacji pakietów aktualizacji dla systemu operacyjnego lub aktualizacji innego oprogramowania z włączoną ochroną funkcją BitLocker. Instalowanie aktualizacji może wymagać ponownego uruchomienia komputera kilka razy. Po każdym ponownym uruchomieniu użytkownik musi zakończyć uwierzytelnianie funkcji BitLocker. Aby poprawnie zainstalować aktualizacje, możesz tymczasowo wyłączyć uwierzytelnianie funkcji BitLocker. W tym przypadku dysk pozostaje zaszyfrowany, a użytkownik posiada dostęp do danych po zalogowaniu do systemu. Aby zarządzać uwierzytelnianiem funkcji BitLocker, musisz użyć zadania *Zarządzanie ochroną BitLocker*. Możesz użyć tego zadania do określenia liczby ponownych uruchomień komputera, które nie wymagają uwierzytelniania funkcji BitLocker. W ten sposób, po zainstalowaniu aktualizacji i zakończeniu zadania *Zarządzanie ochroną BitLocker*, uwierzytelnianie funkcji BitLocker jest automatycznie włączone. Możesz włączyć uwierzytelnianie funkcji BitLocker w dowolnym momencie.

Jak wstrzymać ochronę BitLocker przy użyciu Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Zarządzanie ochroną BitLocker**.

Krok 2. Zarządzanie ochroną BitLocker

Skonfiguruj uwierzytelnianie funkcji BitLocker. Aby wstrzymać ochronę BitLocker, wybierz **Tymczasowo zezwól na pomijanie uwierzytelniania funkcji BitLocker** i wprowadź liczbę ponownych uruchomień bez uwierzytelniania funkcji BitLocker (1 do 15 razy). Jeśli to konieczne, wprowadź datę i godzinę wygaśnięcia zadania. O określonej godzinie zadanie jest automatycznie wyłączone, a użytkownik musi zakończyć uwierzytelnianie funkcji BitLocker po ponownym uruchomieniu komputera.

Krok 3. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 4. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład, *Aktualizowanie do Windows 10*.

Krok 5. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Jak wstrzymać ochronę BitLocker przy użyciu konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security**.
2. Z listy rozwijalnej **Typ zadania** wybierz **Zarządzanie ochroną BitLocker**.
3. W polu **Nazwa zadania** wpisz krótki opis, na przykład *Aktualizowanie do Windows 10*.
4. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

Krok 2. Zarządzanie ochroną BitLocker

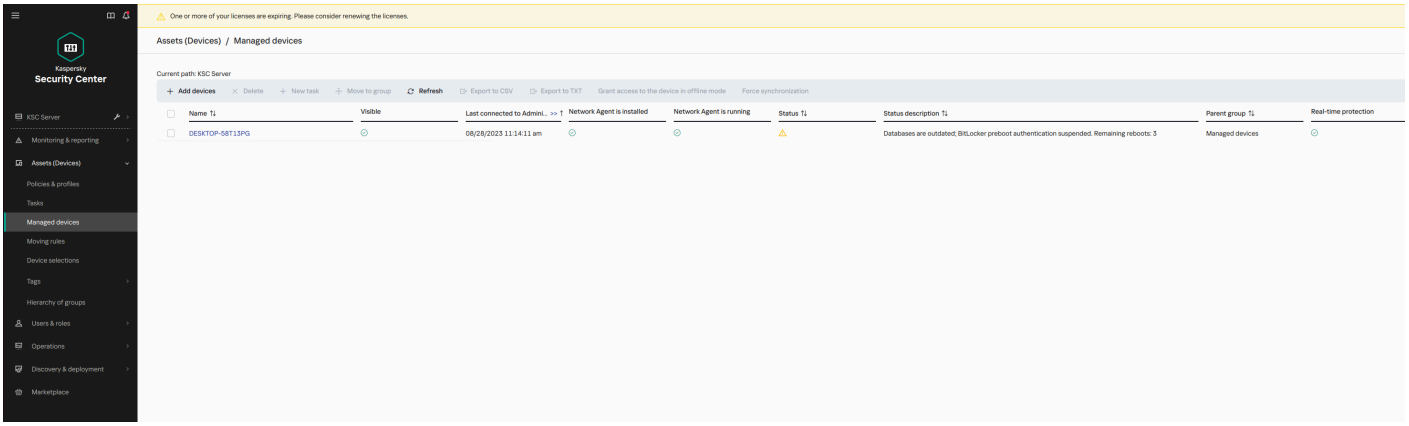
Skonfiguruj uwierzytelnianie funkcji BitLocker. Aby wstrzymać ochronę BitLocker, wybierz **Tymczasowo zezwól na pomijanie uwierzytelniania funkcji BitLocker** i wprowadź liczbę ponownych uruchomień bez uwierzytelniania funkcji BitLocker (1 do 15 razy). Jeśli to konieczne, wprowadź datę i godzinę wygaśnięcia zadania. O określonej godzinie zadanie jest automatycznie wyłączone, a użytkownik musi zakończyć uwierzytelnianie funkcji BitLocker po ponownym uruchomieniu komputera.

Krok 3. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Nowe zadanie zostanie wyświetlone na liście zadań.

Aby uruchomić zadanie, zaznacz pole obok zadania i kliknij przycisk **Uruchom**.

W wyniku tego działania, podczas uruchamiania zadani, po kolejnym ponownym uruchomieniu komputera, BitLocker nie wyświetli pytania o autoryzację. Po każdym ponownym uruchomieniu komputera bez uwierzytelnienia funkcji BitLocker, Kaspersky Endpoint Security wygeneruje odpowiednie zdarzenie i zarejestruje liczbę pozostałych ponownych uruchomień. Następnie Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center do monitorowania przez administratora. Możesz także wyświetlić liczbę pozostałych ponownych uruchomień w folderze **Zarządzane urządzenia** konsoli Kaspersky Security Center w opisie stanu urządzenia.



Lista zarządzanych urządzeń

Jeśli określona liczba ponownych uruchomień lub czas wygaśnięcia zadania zostaną osiągnięte, uwierzytelnianie funkcji BitLocker zostanie automatycznie włączone. Aby uzyskać dostęp do danych, użytkownik musi zakończyć uwierzytelnianie funkcji BitLocker.

Na komputerach działających pod kontrolą systemu Windows 7, BitLocker nie może zliczać ponownych uruchomień komputera. Zliczanie ponownych uruchomień na komputerach z systemem Windows 7 jest zarządzane przez Kaspersky Endpoint Security. Dlatego też, aby uwierzytelnianie funkcji BitLocker było automatycznie włączane po każdym ponownym uruchomieniu, należy uruchomić Kaspersky Endpoint Security.

Aby włączyć uwierzytelnianie funkcji BitLocker z wyprzedzeniem, otwórz właściwości zadania *Zarządzanie ochroną BitLocker* i zaznacz opcję **Żądaj uwierzytelnienia za każdym razem przed rozruchem**.

Szyfrowanie na poziomie plików na lokalnych dyskach komputera

Szyfrowanie plików nie jest obsługiwane na komputerach opartych na architekturze ARM.

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Szyfrowanie plików ma następujące funkcje specjalne:

- Kaspersky Endpoint Security szyfruje / deszyfruje pliki w wstępnie określonych folderach tylko dla profili lokalnego użytkownika systemu operacyjnego. Kaspersky Endpoint Security nie szyfruje / deszyfruje plików w predefiniowanych folderach profili użytkownika mobilnego, obowiązkowych profili użytkownika, tymczasowych profili użytkownika lub folderach przekierowanych.
- Kaspersky Endpoint Security nie szyfruje plików, których modyfikacja mogłaby uszkodzić system operacyjny i zainstalowane aplikacje. Na przykład, na liście wykluczeń szyfrowania znajdują się następujące pliki i foldery ze wszystkimi osadzonymi folderami:
  - %WINDIR%;
  - %PROGRAMFILES% i %PROGRAMFILES(X86)%;
  - Pliki rejestru systemu Windows.

  Lista wykluczeń z szyfrowania nie może być podglądana ani modyfikowana. Pliki i foldery znajdujące się na liście wykluczeń z szyfrowania mogą być dodawane do listy szyfrowania, ale i tak nie będą szyfrowane podczas wykonywania szyfrowania plików.

Szyfrowanie plików na lokalnych dyskach komputera

Kaspersky Endpoint Security nie szyfruje plików, które znajdują się z magazynie w chmurze OneDrive lub w innych folderach, które w nazwie posiadają OneDrive. Kaspersky Endpoint Security blokuje także kopiowanie zaszyfrowanych plików do folderów OneDrive, jeśli te pliki nie są dodawane do reguły odszyfrowywania.

W celu zaszyfrowania plików na dyskach lokalnych:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie plików**.
4. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Zgodnie z regułami**.
5. Na zakładce **Szyfrowanie** kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz jeden z następujących elementów:
   a. Wybierz element **Wstępnie określone foldery**, aby dodać pliki z folderów lokalnych profili użytkowników, zasugerowanych przez specjalistów z Kaspersky, do reguły szyfrowania.
      - **Dokumenty**. Pliki w standardowym folderze *Dokumenty* systemu operacyjnego i jego podfolderach.
      - **Ulubione**. Pliki w standardowym folderze *Ulubione* systemu operacyjnego i jego podfolderach.
      - **Pulpit**. Pliki w standardowym folderze *Pulpit* systemu operacyjnego i jego podfolderach.
      - **Pliki tymczasowe**. Pliki tymczasowe związane z działaniem aplikacji zainstalowanych na komputerze. Na przykład, aplikacje Microsoft Office tworzą pliki tymczasowe zawierające kopie zapasowe dokumentów.

        Nie zaleca się szyfrowania plików tymczasowych, ponieważ może to spowodować utratę danych. Na przykład Microsoft Word tworzy pliki tymczasowe podczas przetwarzania dokumentu. Jeśli pliki tymczasowe zostaną zaszyfrowane, ale oryginalny plik nie, podczas próby zapisania dokumentu może wystąpić błąd *Odmowa dostępu*. Dodatkowo Microsoft Word może zapisać plik, ale nie będzie można otworzyć dokumentu następnym razem, czyli dane zostaną utracone.

      - **Pliki programu Outlook**. Pliki dotyczące działania klienta poczty Outlook: pliki danych (PST), pliki danych offline (OST), pliki książki adresowej offline (OAB) oraz pliki osobistej książki adresowej (PAB).

   b. Wybierz element **Folder niestandardowy**, aby dodać ręcznie wprowadzoną ścieżkę folderu do reguły szyfrowania.

      Dodając ścieżkę folderu, przestrzegaj następujących zasad:

      - Użyj zmiennej środowiskowej (na przykład: `%FOLDER%\UserFolder\`). Możesz użyć zmiennej środowiskowej tylko raz i tylko na początku ścieżki.
      - Nie używaj ścieżek względnych.
      - Nie używaj znaków `*` i `?`.

- Nie używaj ścieżek UNC.
- Użyj `;` lub `,` jako separatora.

c. Wybierz element **Pliki według rozszerzenia**, aby dodać rozszerzenia pojedynczych plików do reguły szyfrowania. Kaspersky Endpoint Security zaszyfruje pliki z określonymi rozszerzeniami na wszystkich lokalnych dyskach komputera.

d. Wybierz element **Pliki według grup rozszerzeń**, aby dodać grupy rozszerzeń plików do reguły szyfrowania (na przykład: *dokumenty Microsoft Office*). Kaspersky Endpoint Security szyfruje pliki, które mają rozszerzenia znajdujące się na liście grup rozszerzeń na wszystkich lokalnych dyskach komputera.

6. Zapisz swoje zmiany.

Natychmiast po zastosowaniu profilu program Kaspersky Endpoint Security szyfruje te pliki, które znajdują się w regule szyfrowania, a nie znajdują się w regule deszyfrowania.

Szyfrowanie plików ma następujące funkcje specjalne:

- Jeśli ten sam plik zostanie dodany zarówno do reguły szyfrowania, jak i reguły deszyfrowania, wówczas Kaspersky Endpoint Security wykonuje następujące działania:
  - Jeśli plik nie jest zaszyfrowany, Kaspersky Endpoint Security nie szyfruje tego pliku.
  - Jeśli plik jest zaszyfrowany, Kaspersky Endpoint Security odszyfrowuje ten plik.
- Kaspersky Endpoint Security kontynuuje szyfrowanie nowych plików, jeśli pliki te spełniają kryteria reguły szyfrowania. Na przykład, po zmianie właściwości niezaszyfrowanego pliku (ścieżki lub rozszerzenia) plik spełnia kryteria reguły szyfrowania. Kaspersky Endpoint Security szyfruje ten plik.
- Jeśli użytkownik tworzy nowy pik, którego właściwości spełniają kryteria reguły szyfrowania, Kaspersky Endpoint Security szyfruje plik, gdy tylko zostanie on otwarty.
- Kaspersky Endpoint Security odracza szyfrowanie otwartych plików, aż do ich zamknięcia.
- Jeśli przeniesiesz zaszyfrowany plik do innego folderu na dysku lokalnym, plik pozostanie zaszyfrowany bez względu na to, czy ten folder znajduje się w regule szyfrowania.
- Jeśli odszyfrujesz plik i skopiujesz go do innego folderu lokalnego, który nie jest objęty regułą deszyfrowania, kopia pliku może zostać zaszyfrowana. Aby zapobiec szyfrowaniu kopiowanego pliku, utwórz regułę deszyfrowania folderu docelowego.

Tworzenie reguł dostępu do zaszyfrowanego pliku dla aplikacji

Domyślnie wszystkie aplikacje pracują z plikami zaszyfrowanymi w stanie odszyfrowanym. Jeśli często korzystasz z określonych aplikacji (na przykład przeglądarek lub edytorów tekstu), możesz utworzyć reguły dostępu do zaszyfrowanego pliku, aby chronić informacje.

Zalecamy utworzenie reguły dostępu do zaszyfrowanego pliku dla przeglądarek Microsoft Internet Explorer i Microsoft Edge. Przeglądarki te działają tak, że jeśli prześlesz zaszyfrowany plik na stronę internetową (np. do pamięci masowej w chmurze), plik zostanie automatycznie odszyfrowany. Może to spowodować wyciek danych. Nie można przesyłać zaszyfrowanego pliku za pomocą tych przeglądarek. Zalecamy skonfigurowanie reguły **Udziel dostępu do szyfrowanych plików tylko w postaci szyfru**. Nie musisz tworzyć reguły dla innych przeglądarek (np. Google Chrome).

W celu utworzenia reguł dostępu do zaszyfrowanego pliku dla aplikacji:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych → Szyfrowanie plików**.
4. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Zgodnie z regułami**.

   Reguły dostępu są stosowane tylko w trybie **Zgodnie z regułami**. Po zastosowaniu reguł dostępu w trybie **Zgodnie z regułami**, jeśli zmienisz na tryb **Pozostaw niezmienione**, Kaspersky Endpoint Security będzie ignorował wszystkie reguły dostępu. Wszystkie aplikacje będą miały dostęp do wszystkich zaszyfrowanych plików.

5. W prawej części okna wybierz zakładkę **Reguły dla aplikacji**.
6. Jeśli chcesz wybrać aplikacje wyłącznie z listy Kaspersky Security Center, kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz element **Aplikacje z listy Kaspersky Security Center**.
   a. Określ filtry w celu zawężenia listy aplikacji w tabeli. W tym celu określ wartości parametrów **Aplikacja**, **Producent** i **Okres dodania** oraz wszystkich pól z sekcji **Grupa**.
   b. Kliknij **Odśwież**.
   c. Tabela wyświetla aplikacje, które odpowiadają stosowanym filtrom.
   d. W kolumnie **Aplikacja** zaznacz pola obok aplikacji, dla których chcesz utworzyć reguły dostępu do zaszyfrowanych plików.
   e. Z listy rozwijalnej **Reguła dla aplikacji** wybierz regułę, która będzie determinować dostęp aplikacji do zaszyfrowanych plików.
   f. Z listy rozwijalnej **Działania dla aplikacji wybranych wcześniej** wybierz działanie, jakie Kaspersky Endpoint Security podejmie na regułach dostępu do zaszyfrowanego pliku, które zostały wcześniej utworzone dla tych aplikacji.

Szczegółowe informacje o regule dostępu do zaszyfrowanego pliku dla aplikacji pojawią się w tabeli, na zakładce **Reguły dla aplikacji**.

7. Jeżeli chcesz ręcznie wybrać aplikacje, kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz element **Niestandardowe aplikacje**.

   a. W polu do wprowadzania danych wpisz nazwę lub listę nazw plików wykonywalnych, w tym ich rozszerzenia.

      Możesz także dodać nazwy plików wykonywalnych aplikacji z listy Kaspersky Security Center poprzez kliknięcie przycisku **Dodaj z listy Kaspersky Security Center**.

   b. Jeśli to konieczne, w polu **Opis** wprowadź opis listy aplikacji.

   c. Z listy rozwijalnej **Reguła dla aplikacji** wybierz regułę, która będzie determinować dostęp aplikacji do zaszyfrowanych plików.

   Szczegółowe informacje o regule dostępu do zaszyfrowanego pliku dla aplikacji pojawią się w tabeli, na zakładce **Reguły dla aplikacji**.

8. Zapisz swoje zmiany.

Szyfrowanie plików utworzonych lub zmodyfikowanych przez określone aplikacje

Możesz utworzyć regułę, według której Kaspersky Endpoint Security będzie szyfrować pliki utworzone lub zmodyfikowane przez aplikacje określone w regule.

Pliki utworzone lub zmodyfikowane przez określone aplikacje przed zastosowaniem reguły szyfrowania nie zostaną zaszyfrowane.

W celu skonfigurowania szyfrowania plików utworzonych lub zmodyfikowanych przez określone aplikacje:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie plików**.
4. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Zgodnie z regułami**.

   Reguły szyfrowania są stosowane tylko w trybie **Zgodnie z regułami**. Po zastosowaniu reguł szyfrowania w trybie **Zgodnie z regułami**, jeśli zmienisz na tryb **Pozostaw niezmienione**, Kaspersky Endpoint Security będzie ignorował wszystkie reguły szyfrowania. Pliki, które zostały wcześniej zaszyfrowane, pozostaną zaszyfrowane.

5. W prawej części okna wybierz zakładkę **Reguły dla aplikacji**.

6. Jeśli chcesz wybrać aplikacje wyłącznie z listy Kaspersky Security Center, kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz element **Aplikacje z listy Kaspersky Security Center**.

   a. Określ filtry w celu zawężenia listy aplikacji w tabeli. W tym celu określ wartości parametrów **Aplikacja**, **Producent** i **Okres dodania** oraz wszystkich pól z sekcji **Grupa**.

   b. Kliknij **Odśwież**.

      Tabela wyświetla aplikacje, które odpowiadają stosowanym filtrom.

   c. W kolumnie **Aplikacja** zaznacz pola obok aplikacji, których utworzone pliki mają być zaszyfrowane.

   d. Z listy rozwijalnej **Reguła dla aplikacji** wybierz **Zaszyfruj wszystkie utworzone pliki**.

   e. Z listy rozwijalnej **Działania dla aplikacji wybranych wcześniej** wybierz działanie, jakie Kaspersky Endpoint Security podejmie na regułach szyfrowania plików, które zostały wcześniej utworzone dla tych aplikacji.

   Informacje o regule szyfrowania dla plików utworzonych lub zmodyfikowanych przez wybrane aplikacje zostaną wyświetlone w tabeli na zakładce **Reguły dla aplikacji**.

7. Jeżeli chcesz ręcznie wybrać aplikacje, kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz element **Niestandardowe aplikacje**.

   a. W polu do wprowadzania danych wpisz nazwę lub listę nazw plików wykonywalnych, w tym ich rozszerzenia.

      Możesz także dodać nazwy plików wykonywalnych aplikacji z listy Kaspersky Security Center poprzez kliknięcie przycisku **Dodaj z listy Kaspersky Security Center**.

   b. Jeśli to konieczne, w polu **Opis** wprowadź opis listy aplikacji.

   c. Z listy rozwijalnej **Reguła dla aplikacji** wybierz **Zaszyfruj wszystkie utworzone pliki**.

   Informacje o regule szyfrowania dla plików utworzonych lub zmodyfikowanych przez wybrane aplikacje zostaną wyświetlone w tabeli na zakładce **Reguły dla aplikacji**.

8. Zapisz swoje zmiany.

Generowanie reguły deszyfrowania

W celu wygenerowania reguły deszyfrowania:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie plików**.

4. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Zgodnie z regułami**.

5. Na zakładce **Odszyfrowywanie** kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz jeden z następujących elementów:

   a. Wybierz element **Wstępnie określone foldery**, aby dodać pliki z folderów lokalnych profili użytkowników, zasugerowanych przez specjalistów z Kaspersky, do reguły deszyfrowania.

   b. Wybierz element **Folder niestandardowy**, aby dodać ręcznie wprowadzoną ścieżkę folderu do reguły deszyfrowania.

   c. Wybierz element **Pliki według rozszerzenia**, aby dodać pojedyncze rozszerzenia plików do reguły deszyfrowania. Kaspersky Endpoint Security nie szyfruje plików z określonymi rozszerzeniami na wszystkich lokalnych dyskach komputera.

   d. Wybierz element **Pliki według grup rozszerzeń**, aby dodać grupy rozszerzeń plików do reguły deszyfrowania (na przykład: *dokumenty Microsoft Office*). Kaspersky Endpoint Security nie szyfruje plików, które mają rozszerzenia znajdujące się na liście grup rozszerzeń na wszystkich lokalnych dyskach komputera.

6. Zapisz swoje zmiany.

Jeśli ten sam plik został dodany do reguły szyfrowania oraz do reguły deszyfrowania, Kaspersky Endpoint Security nie zaszyfruje tego pliku, jeśli nie jest zaszyfrowany, a odszyfruje plik, jeśli jest zaszyfrowany.

Deszyfrowanie plików na lokalnych dyskach komputera

W celu odszyfrowania plików na dyskach lokalnych:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie plików**.

4. W prawej części okna wybierz zakładkę **Szyfrowanie**.

5. Usuń z listy szyfrowania te pliki i foldery, które chcesz odszyfrować. W tym celu zaznacz pliki i wybierz element **Usuń regułę i odszyfruj pliki** z menu kontekstowego przycisku **Usuń**.

   Pliki i foldery usuwane z listy zaszyfrowanych są automatycznie dodawane do listy odszyfrowanych.

6. Utwórz listę deszyfrowanych plików.

7. Zapisz swoje zmiany.

Jak tylko profil zostanie zastosowany, Kaspersky Endpoint Security odszyfruje zaszyfrowane pliki, które zostały dodane do listy deszyfrowanych.

Kaspersky Endpoint Security deszyfruje zaszyfrowane pliki, jeśli ich parametry (ścieżka dostępu do pliku / nazwa pliku / rozszerzenie pliku) zostały zmienione, aby pasowały do parametrów obiektów dodanych do listy deszyfrowanych.

Kaspersky Endpoint Security odracza deszyfrację otwartych plików, aż do ich zamknięcia.

Tworzenie zaszyfrowanych pakietów

Aby chronić dane podczas wysyłania plików do użytkowników poza sieć korporacyjną, możesz użyć zaszyfrowanych pakietów. Zaszyfrowane pakiety mogą być wygodne do przesyłania plików o dużych rozmiarach na nośniki wymienne, gdyż klienci poczty e-mail posiadają ograniczenia rozmiaru plików.

Przed utworzeniem zaszyfrowanych pakietów Kaspersky Endpoint Security wyświetli pytanie o podanie hasła. Aby solidnie chronić dane, możesz włączyć sprawdzanie siły hasła oraz określić wymagania co do siły hasła. Uniemożliwi to użytkownikom korzystanie z krótkich i prostych haseł, na przykład: `1234`.

Jak włączyć sprawdzanie siły hasła podczas tworzenia zaszyfrowanych archiwów w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych → Ogólne ustawienia szyfrowania**.
4. W sekcji **Ustawienia hasła** kliknij przycisk **Ustawienia**.
5. Spowoduje to otwarcie okna. Wybierz w nim zakładkę **Zaszyfrowane pakiety**.
6. Podczas tworzenia zaszyfrowanych pakietów skonfiguruj ustawienia złożoności hasła.

Jak włączyć sprawdzanie siły hasła podczas tworzenia zaszyfrowanych archiwów w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Szyfrowanie danych → Szyfrowanie plików**.
5. W sekcji **Ustawienia hasła pakietu zaszyfrowanego** skonfiguruj kryteria siły hasła wymagane podczas tworzenia zaszyfrowanych pakietów.

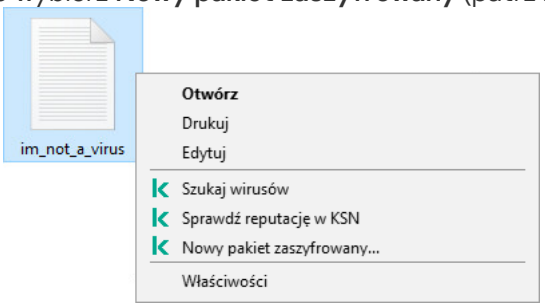
Możesz utworzyć zaszyfrowane pakiety na komputerach z zainstalowanym programem Kaspersky Endpoint Security z dostępnym Szyfrowaniem plików.

Podczas dodawania pliku do zaszyfrowanego pakietu, którego zawartość znajduje się w magazynie w chmurze OneDrive, Kaspersky Endpoint Security pobierze zawartość pliku i przeprowadzi szyfrowanie.

W celu utworzenia zaszyfrowanego pakietu:

1. W dowolnym menedżerze plików wybierz pliki lub foldery, które chcesz dodać do zaszyfrowanego pakietu. Kliknij je prawym przyciskiem myszy w celu otwarcia ich menu kontekstowego.

2. Z otwartego menu kontekstowego wybierz **Nowy pakiet zaszyfrowany** (patrz rysunek poniżej).



Tworzenie zaszyfrowanego pakietu

3. W otwartym oknie określ hasło i potwierdź je.

   Hasło musi spełniać złożone kryteria określone w zasadzie.

4. Kliknij **Utwórz**.

   Zostanie uruchomiony proces tworzenia zaszyfrowanego pakietu. Podczas tworzenia zaszyfrowanego pakietu Kaspersky Endpoint Security nie przeprowadza kompresji plików. Po zakończeniu procesu, w wybranym folderze docelowym zostanie utworzony samorozpakowujący się zaszyfrowany pakiet chroniony hasłem (plik wykonywalny z rozszerzeniem .exe –).

Aby uzyskać dostęp do plików w zaszyfrowanym pakiecie, kliknij go dwukrotnie, aby uruchomić Kreator rozpakowywania, a następnie wprowadź hasło. Jeśli zapomniałeś lub zgubiłeś swoje hasło, nie jest możliwe odzyskanie go i uzyskanie dostępu do plików w zaszyfrowanym pakiecie. Możesz ponownie utworzyć zaszyfrowany pakiet.

Przywracanie dostępu do zaszyfrowanych plików

Jeśli pliki są szyfrowane, Kaspersky Endpoint Security otrzymuje klucz szyfrowania wymagany do bezpośredniego dostępu do zaszyfrowanych plików. Użytkownik pracujący z poziomu dowolnego konta Windows, które było aktywne podczas szyfrowania pliku, może uzyskać bezpośredni dostęp do zaszyfrowanych plików, używając tego klucza szyfrowania. Użytkownicy pracujący z poziomu kont Windows, które były nieaktywne podczas szyfrowania pliku muszą być połączeni z Kaspersky Security Center w celu uzyskania dostępu do zaszyfrowanych plików.

Zaszyfrowane pliki mogą być niedostępne w następujących przypadkach:

- Na komputerze użytkownika przechowywane są klucze szyfrowania, ale nie ma połączenia z Kaspersky Security Center w celu zarządzania nimi. W tym przypadku użytkownik musi poprosić administratora lokalnej sieci firmowej o dostęp do zaszyfrowanych plików.

  Jeśli nie ma dostępu do Kaspersky Security Center, należy:

  - poprosić o klucz dostępu do plików zaszyfrowanych na dyskach twardych komputera;
  - poprosić o oddzielne klucze dostępu dla zaszyfrowanych plików na każdym dysku wymiennym, aby móc uzyskać dostęp do zaszyfrowanych plików przechowywanych na nośnikach wymiennych.

- Moduły szyfrujące są usuwane z komputera użytkownika. W tej sytuacji użytkownik może otworzyć zaszyfrowane pliki na dyskach lokalnych i nośnikach wymiennych, ale zawartość tych plików będzie zaszyfrowana.

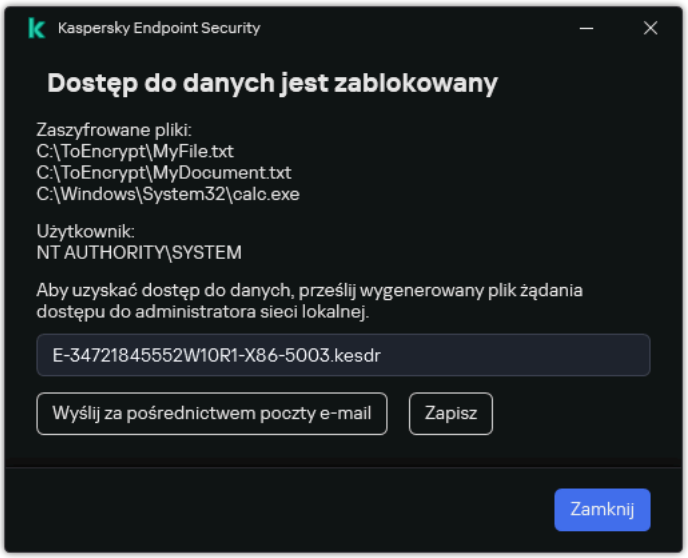
  Użytkownik może pracować z zaszyfrowanymi plikami w następujących przypadkach:

  - Pliki są umieszczane w zaszyfrowanych pakietach utworzonych na komputerze z zainstalowanym programem Kaspersky Endpoint Security.
  - Pliki są przechowywane na nośnikach wymiennych, na których dozwolony jest tryb przenośny.

Aby uzyskać dostęp do zaszyfrowanych plików, użytkownik musi rozpocząć procedurę odzyskiwania (Żądanie-Odpowiedź).

Odzyskiwanie dostępu do zaszyfrowanych plików składa się z następujących kroków:

1. Użytkownik wyśle plik zawierający żądanie dostępu do administratora (patrz rysunek poniżej).
2. Administrator dodaje plik żądania dostępu do Kaspersky Security Center, tworzy plik klucza dostępu i wysyła ten plik do użytkownika.
3. Użytkownik dodaje plik klucza dostępu do Kaspersky Endpoint Security i uzyskuje dostęp do plików.



Przywracanie dostępu do zaszyfrowanych plików

Aby rozpocząć procedurę odzyskiwania, użytkownik musi spróbować uzyskać dostęp do pliku. W rezultacie Kaspersky Endpoint Security utworzy plik dostępu do żądania (plik z rozszerzeniem KESDC), który użytkownik musi wysłać administratorowi, na przykład, za pośrednictwem poczty elektronicznej.

Kaspersky Endpoint Security generuje plik zawierający żądanie dostępu do wszystkich zaszyfrowanych plików przechowywanych na dysku komputera (dysk lokalny lub dysk wymienny).

Jak uzyskać zaszyfrowany plik klucza dostępu do danych w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Urządzenia**.
3. W zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanych danych, i kliknij go prawym przyciskiem myszy, aby otworzyć menu kontekstowe.

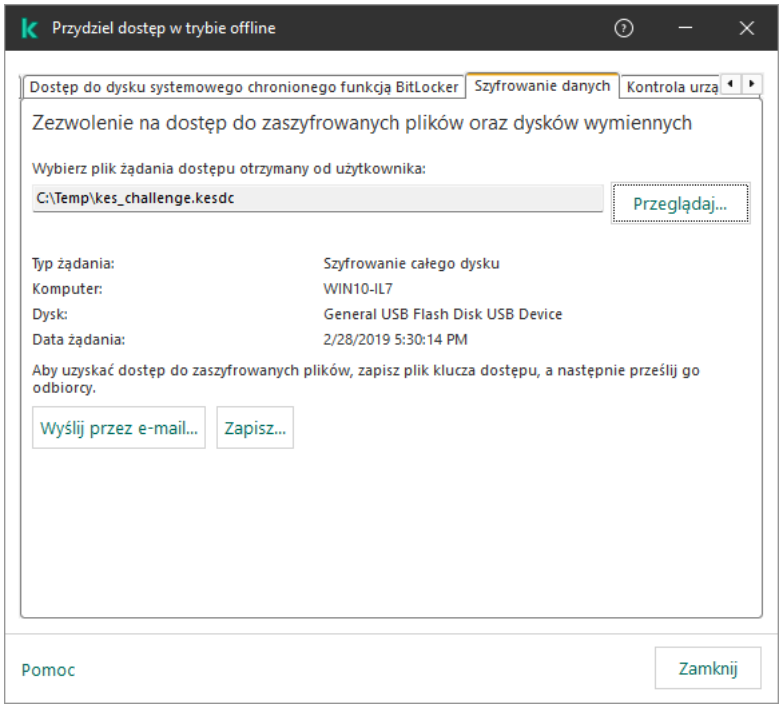
4. Z otwartego menu kontekstowego wybierz **Przydziel dostęp w trybie offline**.

5. Spowoduje to otwarcie okna. Wybierz w nim zakładkę **Szyfrowanie danych**.

6. Na zakładce **Szyfrowanie danych** kliknij przycisk **Przeglądaj**.

7. W oknie wyboru pliku dostępu do żądania określ ścieżkę do pliku otrzymanego od użytkownika.

Zobaczysz informacje o żądaniu użytkownika. Kaspersky Security Center wygeneruje plik klucza. Wyślij do użytkownika wygenerowany plik klucza dostępu do zaszyfrowanych danych. Lub zapisz plik dostępu i użyj dowolnej dostępnej metody, aby przenieść plik.



Przydzielanie dostępu w trybie offline

Jak uzyskać zaszyfrowany plik klucza dostępu do danych w konsoli Wen Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.

2. Zaznacz pole wyboru obok nazwy komputera, do którego danych chcesz przywrócić dostęp.

3. Kliknij **Udziel dostępu do urządzenia w trybie offline**.

4. Wybierz **Szyfrowanie danych**.

5. Kliknij przycisk **Wybierz plik** i wybierz plik żądania dostępu otrzymany od użytkownika (plik z rozszerzeniem KESDC).

   Konsola Web Console wyświetli informacje o żądaniu. Obejmuje to nazwę komputera, na którym użytkownik żąda dostępu do pliku.

6. Kliknij przycisk **Zapisz klucz** i wybierz folder, aby zapisać plik klucza dostępu do zaszyfrowanych danych (plik z rozszerzeniem KESDR).

W rezultacie będziesz mógł uzyskać klucz dostępu do zaszyfrowanych danych, który będziesz musiał przekazać użytkownikowi.

Po otrzymaniu pliku klucza dostępu do zaszyfrowanych danych, użytkownik musi uruchomić plik, klikając go dwukrotnie. W rezultacie Kaspersky Endpoint Security zapewni dostęp do wszystkich zaszyfrowanych plików przechowywanych na dysku. Aby mieć dostęp do zaszyfrowanych plików przechowywanych na innych dyskach, należy uzyskać oddzielny plik klucza dostępu dla każdego dysku.

Przywracanie dostępu do zaszyfrowanych danych po awarii systemu operacyjnego

Możesz przywrócić dostęp do danych po błędzie systemu operacyjnego tylko dla szyfrowania na poziomie plików (FLE). Nie możesz przywrócić dostępu do danych, jeśli używane jest szyfrowanie całego dysku (FDE).

W celu przywrócenia dostępu do zaszyfrowanych danych po awarii systemu operacyjnego:

1. Przeinstaluj system operacyjny bez formatowania dysku twardego.
2. Zainstaluj Kaspersky Endpoint Security.
3. Nawiąż połączenie między komputerem a Serwerem administracyjnym Kaspersky Security Center, który kontrolował komputer, gdy dane były zaszyfrowane.

Dostęp do zaszyfrowanych danych zostanie nadany na tych samych warunkach, które zostały zastosowane przed awarią systemu operacyjnego.

Modyfikowanie szablonów wiadomości dostępu do zaszyfrowanego pliku

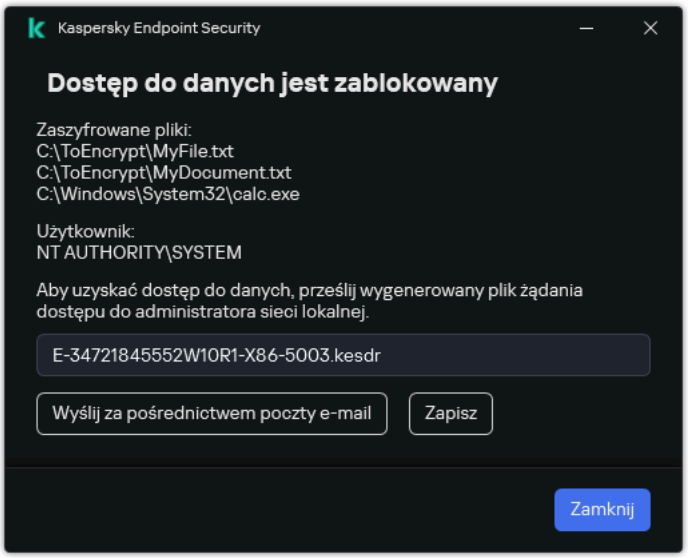
W celu zmodyfikowania szablonów wiadomości dostępu do zaszyfrowanego pliku:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych** → **Ogólne ustawienia szyfrowania**.
4. W sekcji **Szablony** kliknij przycisk **Szablony**.
5. W otwartym oknie wykonaj następujące czynności:
   - Jeśli chcesz zmodyfikować szablon wiadomości użytkownika, wybierz zakładkę **Komunikat użytkownika**. Poniższe okno otwiera się, gdy użytkownik próbuje uzyskać dostęp do zaszyfrowanego pliku, gdy na komputerze nie ma klucza dostępu do zaszyfrowanych plików (patrz rysunek poniżej). Klikając przycisk **Wyślij za pośrednictwem poczty e-mail** automatycznie tworzy się wiadomość użytkownika. Wiadomość ta jest wysyłana do administratora korporacyjnej sieci LAN wraz z prośbą o dostęp do zaszyfrowanych plików.
   - Jeśli chcesz zmodyfikować szablon wiadomości administratora, wybierz zakładkę **Komunikat administratora**. Użytkownik otrzymuje tę wiadomość po uzyskaniu dostępu do zaszyfrowanych plików.
6. Zmodyfikuj szablony wiadomości.

Aby dodać zmienną do tekstu szablonu, umieść kursor w odpowiednim miejscu, kliknij przycisk **Zmienna** i wybierz wymaganą zmienną z listy dostępnych opcji.

Możesz również przywrócić domyślny tekst szablonu za pomocą przycisku **Domyślny**.

7. Zapisz swoje zmiany.



Przywracanie dostępu do zaszyfrowanych plików

Szyfrowanie nośników wymiennych

Szyfrowanie dysków wymiennych nie jest obsługiwane na komputerach opartych na architekturze ARM.

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Kaspersky Endpoint Security obsługuje szyfrowanie plików w systemach plików FAT32 i NTFS. Jeśli dysk wymienny z nieobsługiwanym systemem plików jest podłączony do komputera, zadanie szyfrowania dla tego dysku wymiennego zakończy się błędem, a Kaspersky Endpoint Security przypisze do dysku wymiennego stan tylko do odczytu.

W celu ochrony danych na dyskach wymiennych możesz użyć następujących typów szyfrowania:

- Full Disk Encryption (FDE).

  Szyfrowanie całego dysku wymiennego, w tym systemu plików.

  Nie jest możliwy dostęp do zaszyfrowanych danych poza siecią korporacyjną. Dostęp do zaszyfrowanych danych w sieci korporacyjnej jest również niemożliwy, jeśli komputer nie jest podłączony do Kaspersky Security Center (na przykład, na komputerze gościa).

- File Level Encryption (FLE).

Szyfrowanie tylko plików na dysku wymiennym. System plików pozostaje niezmieniony.

> Szyfrowanie plików na dyskach wymiennych umożliwia dostęp do danych poza siecią korporacyjną za pomocą specjalnego trybu zwanego *trybem przenośnym*.

Podczas szyfrowania Kaspersky Endpoint Security tworzy klucz główny. Kaspersky Endpoint Security zapisuje klucz główny w następujących repozytoriach:

- Kaspersky Security Center.
- Na komputerze użytkownika.

  Klucz główny jest szyfrowany za pomocą tajnego klucza użytkownika.
- Na dysku wymiennym.

  Klucz główny jest szyfrowany za pomocą klucza publicznego Kaspersky Security Center.

Po zakończeniu szyfrowania dane na dysku wymiennym mogą być dostępne w sieci korporacyjnej tak, jakbyś używał zwykłego niezaszyfrowanego dysku wymiennego.

Uzyskiwanie dostępu do zaszyfrowanych danych

Gdy podłączony jest dysk wymienny z zaszyfrowanymi danymi, Kaspersky Endpoint Security wykonuje następujące czynności:

1. Sprawdza klucz główny w lokalnej pamięci na komputerze użytkownika.

   Jeśli klucz główny zostanie znaleziony, użytkownik uzyskuje dostęp do danych na dysku wymiennym.

   Jeśli klucz główny nie zostanie znaleziony, Kaspersky Endpoint Security wykonuje następujące działania:

   a. Wysyła zapytanie do Kaspersky Security Center.

      Po otrzymaniu zapytania, Kaspersky Security Center wysyła odpowiedź zawierającą klucz główny.

   b. Kaspersky Endpoint Security zapisuje klucz główny w lokalnej pamięci na komputerze użytkownika do późniejszych operacji na zaszyfrowanym dysku wymiennym.

2. Odszyfrowuje dane.

Specjalne funkcje szyfrowania dysku wymiennego

Szyfrowanie dysków wymiennych ma następujące funkcje specjalne:

- Zasada z predefiniowanymi ustawieniami szyfrowania dysku wymiennego zostanie utworzona dla określonej grupy zarządzanych komputerów. Dlatego też, wynik stosowania profilu Kaspersky Security Center, skonfigurowanego dla szyfrowania/deszyfrowania dysków wymiennych zależy od komputera, do którego podłączony jest dysk wymienny.
- Kaspersky Endpoint Security nie szyfruje/deszyfruje plików tylko do odczytu, które są przechowywane na nośnikach wymiennych.

- Następujące typy urządzeń są obsługiwane jako dyski wymienne:
  - Nośniki danych podłączane poprzez magistralę USB
  - Dyski twarde podłączane poprzez magistrale USB i FireWire
  - Dyski SSD podłączane poprzez magistrale USB i FireWire

Uruchamianie szyfrowania nośników wymiennych

Możesz użyć zasady do odszyfrowania dysku wymiennego. Dla określonej grupy administracyjnej generowana jest zasada ze zdefiniowanymi ustawieniami szyfrowania dysku wymiennego. Dlatego też wynik deszyfrowania danych na dyskach wymiennych zależy od komputera, do którego podłączony został dysk wymienny.

Kaspersky Endpoint Security obsługuje szyfrowanie plików w systemach plików FAT32 i NTFS. Jeśli dysk wymienny z nieobsługiwanym systemem plików jest podłączony do komputera, zadanie szyfrowania dla tego dysku wymiennego zakończy się błędem, a Kaspersky Endpoint Security przypisze do dysku wymiennego stan tylko do odczytu.

Przed zaszyfrowaniem plików na dysku wymiennym upewnij się, że jest on sformatowany i nie ma żadnych ukrytych partycji (takich jak partycja systemowa EFI). Jeśli dysk zawiera niesformatowane lub ukryte partycje, szyfrowanie plików może się zakończyć błędem.

W celu zaszyfrowania dysków wymiennych:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
4. Z listy rozwijalnej **Tryb szyfrowania** wybierz domyślne działanie, które Kaspersky Endpoint Security ma wykonać na dyskach wymiennych:
   - **Zaszyfruj cały dysk wymienny** (FDE). Kaspersky Endpoint Security zaszyfruje zawartość dysku wymiennego sektor po sektorze. W rezultacie aplikacja zaszyfruje nie tylko pliki przechowywane na dysku wymiennym, ale także jego systemy plików, w tym nazwy plików i struktury folderów na dysku wymiennym.
   - **Zaszyfruj wszystkie pliki** (FLE). Kaspersky Endpoint Security szyfruje wszystkie pliki, które są przechowywane na dyskach wymiennych. Aplikacja nie szyfruje systemów plików dysków wymiennych, łącznie z nazwami plików i strukturami folderów.
   - **Zaszyfruj tylko nowe pliki** (FLE). Kaspersky Endpoint Security szyfruje tylko te pliki, które zostały dodane do dysków wymiennych lub które były przechowywane na dyskach wymiennych i zostały zmodyfikowane po ostatnim zastosowaniu profilu Kaspersky Security Center.

   Kaspersky Endpoint Security nie szyfruje dysku wymiennego, który został już zaszyfrowany.

5. Jeśli chcesz użyć trybu przenośnego dla szyfrowania dysków wymiennych, zaznacz pole **Tryb przenośny**.

   Tryb przenośny to tryb szyfrowania plików (FLE) na dyskach wymiennych, które oferują możliwość dostępu do danych poza siecią korporacyjną. Tryb przenośny umożliwia także pracę z zaszyfrowanymi danymi na komputerach bez zainstalowanego programu Kaspersky Endpoint Security.

6. Jeśli chcesz zaszyfrować nowy dysk wymienny, zalecane jest zaznaczenie pola **Zaszyfruj tylko używaną przestrzeń dyskową**. Jeśli pole jest odznaczone, Kaspersky Endpoint Security zaszyfruje wszystkie pliki, w tym pozostałe fragmenty usuniętych lub zmodyfikowanych plików.

7. Jeśli chcesz skonfigurować szyfrowanie dla pojedynczych dysków wymiennych, zdefiniuj reguły szyfrowania.

8. Jeśli chcesz użyć szyfrowania całego dysku dla dysków wymiennych w trybie offline, zaznacz pole **Zezwól na szyfrowanie dysków wymiennych w trybie offline**.

   Tryb szyfrowania offline to szyfrowanie dysków wymiennych (FDE), gdy nie ma połączenia z Kaspersky Security Center. Podczas szyfrowania Kaspersky Endpoint Security zapisuje główny klucz tylko na komputerze użytkownika. Kaspersky Endpoint Security wyśle główny klucz do Kaspersky Security Center podczas następnej synchronizacji.

   Jeśli komputer, na którym zapisany jest główny klucz, jest uszkodzony, a dane nie są wysyłane do Kaspersky Security Center, nie jest możliwe uzyskanie dostępu do dysku wymiennego.

   Jeśli pole **Zezwól na szyfrowanie dysków wymiennych w trybie offline** jest odznaczone i nie ma połączenia z Kaspersky Security Center, szyfrowanie dysku wymiennego nie jest możliwe.

9. Zapisz swoje zmiany.

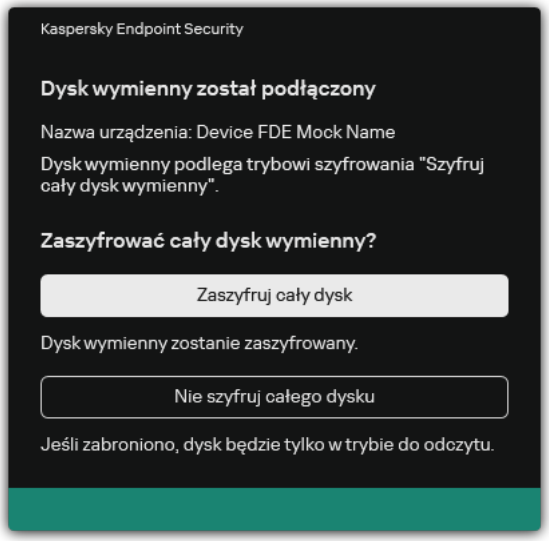
Po zastosowaniu profilu, gdy użytkownik podłącza dysk wymienny lub jeśli dysk wymienny jest już podłączony, Kaspersky Endpoint Security zapyta użytkownika o potwierdzenie wykonania operacji szyfrowania (patrz rysunek poniżej).

Aplikacja umożliwia wykonywanie następujących działań:

- Jeśli użytkownik potwierdzi żądanie szyfrowania, Kaspersky Endpoint Security zaszyfruje dane.
- Jeśli użytkownik odrzuci żądanie szyfrowania, Kaspersky Endpoint Security pozostawi dane niezmienione i przypisze dla tego dysku wymiennego dostęp tylko do odczytu.
- Jeśli użytkownik nie odpowie na żądanie szyfrowania, Kaspersky Endpoint Security pozostawi dane niezmienione i przypisze dla tego dysku wymiennego dostęp tylko do odczytu. Aplikacja ponownie wyświetli monit o potwierdzenie przy jednoczesnym zastosowaniu zasady lub następnym razem, gdy ten dysk wymienny zostanie podłączony.

Jeśli użytkownik zainicjuje bezpieczne usuwanie dysku wymiennego w trakcie szyfrowania danych, Kaspersky Endpoint Security przerwie proces szyfrowania i pozwoli na usunięcie dysku wymiennego przed zakończeniem procesu szyfrowania. Szyfrowanie danych będzie kontynuowane następnym razem, gdy dysk wymienny zostanie podłączony do tego komputera.

Jeśli szyfrowanie nośnika wymiennego nie powiodło się, przejrzyj raport **Szyfrowanie danych** w interfejsie Kaspersky Endpoint Security. Dostęp do plików może być zablokowany przez inną aplikację. W tym przypadku spróbuj odłączyć nośnik wymienny od komputera i podłączyć go ponownie.



Żądanie szyfrowania dysku wymiennego

Dodawanie reguły szyfrowania dla nośników wymiennych

W celu dodania reguły szyfrowania dla dysków wymiennych:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
4. Kliknij przycisk **Dodaj** i z otwartej listy rozwijalnej wybierz jeden z następujących elementów:
   - Jeśli chcesz dodać regułę szyfrowania dla nośników wymiennych, które znajdują się na liście zaufanych urządzeń komponentu Kontrola urządzeń, wybierz **Z listy zaufanych urządzeń określonej w tej zasadzie**.
   - Jeśli chcesz dodać regułę szyfrowania dla nośników wymiennych, które znajdują się na liście Kaspersky Security Center, wybierz **Z listy urządzeń Kaspersky Security Center**.
5. Z listy rozwijalnej **Tryb szyfrowania dla wybranych urządzeń** wybierz akcję, jaka zostanie wykonana przez Kaspersky Endpoint Security na plikach przechowywanych na wybranych dyskach wymiennych.

6. Zaznacz pole **Tryb przenośny**, jeśli chcesz, aby przed szyfrowaniem program Kaspersky Endpoint Security przygotował dyski wymienne, umożliwiając użycie w trybie przenośnym przechowywanych na nich zaszyfrowanych plików.

   Tryb przenośny umożliwia użycie zaszyfrowanych plików, przechowywanych na dyskach wymiennych podłączonych do komputerów bez funkcji szyfrowania.

7. Jeśli chcesz, aby Kaspersky Endpoint Security szyfrował tylko te sektory dysku, które są zajęte przez pliki, zaznacz pole **Zaszyfruj tylko używaną przestrzeń dyskową**.

   Jeśli stosujesz szyfrowanie na dysku, który jest już w użyciu, zalecane jest zaszyfrowanie całego dysku. Zapewni to ochronę wszystkich danych, także tych usuniętych, gdyż mogą zawierać informacje, które można odzyskać. Użycie funkcji **Zaszyfruj tylko używaną przestrzeń dyskową** jest zalecane w przypadku nowych dysków, które nie były wcześniej używane.

   Jeśli urządzenie zostało wcześniej zaszyfrowane przy użyciu funkcji **Zaszyfruj tylko używaną przestrzeń dyskową**, po zastosowaniu profilu w trybie **Zaszyfruj cały dysk wymienny**, sektory, które nie są zajęte przez pliki, będą wciąż niezaszyfrowane.

8. Z listy rozwijalnej **Działania dla urządzeń wybranych wcześniej** wybierz akcję wykonywaną przez Kaspersky Endpoint Security zgodnie z regułami szyfrowania, wcześniej zdefiniowanymi dla dysków wymiennych:

   - Jeśli chcesz, aby wcześniej utworzona reguła szyfrowania dla nośnika wymiennego pozostała niezmieniona, wybierz **Pomiń**.
   - Jeśli chcesz, aby wcześniej utworzona reguła szyfrowania dla nośnika wymiennego została zastąpiona przez nową regułę, wybierz **Odśwież**.

9. Zapisz swoje zmiany.

Dodane reguły szyfrowania dysków wymiennych zostaną zastosowane do dysków wymiennych podłączonych do dowolnych komputerów w organizacji.

Eksportowanie i importowanie listy reguł szyfrowania dla nośników wymiennych

Możesz wyeksportować listę reguł szyfrowania nośników wymiennych do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę reguł tego samego typu nośników wymiennych. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy reguł lub przeniesienia reguł na inny serwer.

Eksportowanie i importowanie listy reguł szyfrowania nośników wymiennych w Konsoli administracyjnej (MMC)

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.

5. W sekcji **Reguły szyfrowania dla wybranych urządzeń** kliknij odnośnik **<N> reguły**.

   Spowoduje to otwarcie listy reguł szyfrowania dla nośników wymiennych.

6. W celu wyeksportowania listy reguł szyfrowania dla nośników wymiennych:

   a. Wybierz reguły, które chcesz zmienić.

   b. Kliknij **Eksportuj**.

   c. Potwierdź chęć wyeksportowania tylko wybranych reguł lub wyeksportuj całą listę.

   d. Zapisz plik.

      Kaspersky Endpoint Security eksportuje listę reguł do pliku XML w domyślnym folderze do pobrania.

7. W celu zaimportowania listy reguł:

   a. Kliknij odnośnik **Importuj**.

      W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.

   b. Otwórz plik.

      Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

8. Zapisz swoje zmiany.

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Szyfrowanie danych → Szyfrowanie dysków wymiennych**.

4. W celu wyeksportowania listy reguł szyfrowania dla nośników wymiennych:

   a. Wybierz reguły, które chcesz zmienić. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.

      Jeśli nie wybrałeś żadnej reguły, Kaspersky Endpoint Security wyeksportuje wszystkie reguły.

   b. Kliknij odnośnik **Eksportuj**.

   c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę reguł, i wybierz folder, w którym chcesz zapisać ten plik.

   d. Zapisz plik.

      Kaspersky Endpoint Security eksportuje listę reguł do pliku XML.

5. W celu zaimportowania listy reguł szyfrowania dla nośników wymiennych:

   a. Kliknij odnośnik **Importuj**.

      W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.

b. Otwórz plik.

Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

6. Zapisz swoje zmiany.

Tryb przenośny dla uzyskiwania dostępu do zaszyfrowanych plików na dyskach wymiennych

Tryb przenośny to tryb szyfrowania plików (FLE) na dyskach wymiennych, które oferują możliwość dostępu do danych poza siecią korporacyjną. Tryb przenośny umożliwia także pracę z zaszyfrowanymi danymi na komputerach bez zainstalowanego programu Kaspersky Endpoint Security.

Tryb przenośny jest wygodny w użyciu w następujących przypadkach:

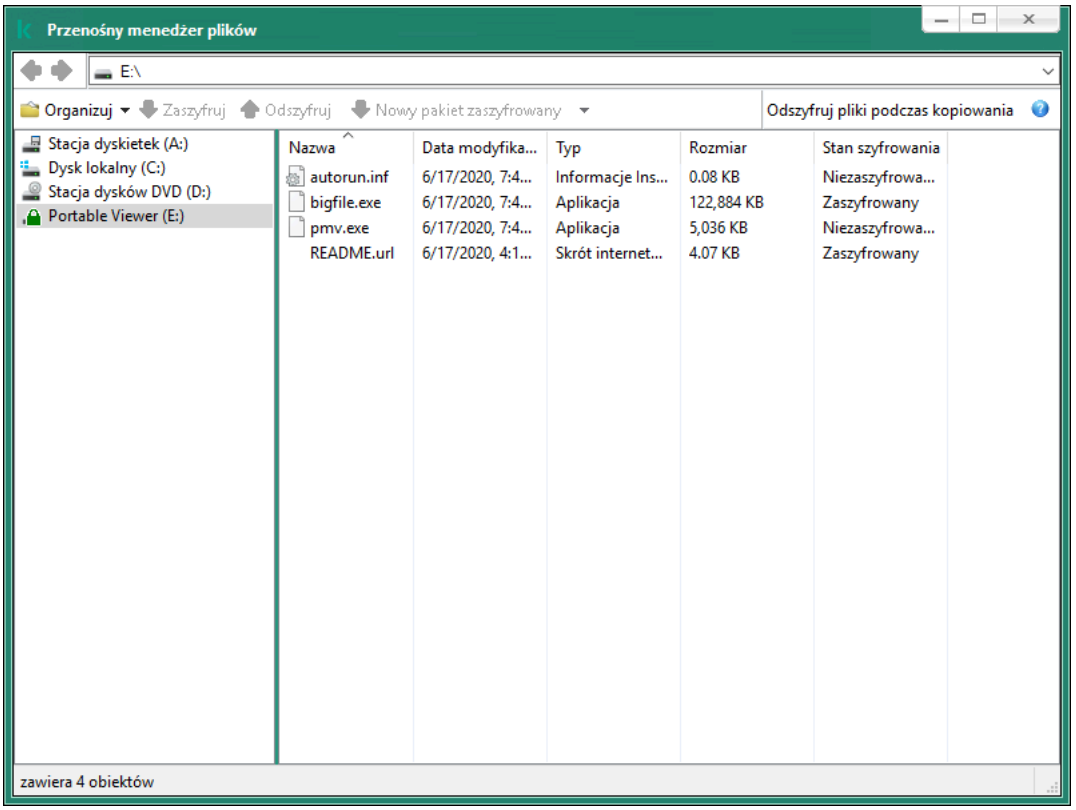
- Nie ma połączenia między komputerem a Serwerem administracyjnym Kaspersky Security Center.
- Infrastruktura zmieniła się wraz ze zmianą Serwera administracyjnego Kaspersky Security Center.
- Kaspersky Endpoint Security nie jest zainstalowany na komputerze.

Przenośny menedżer plików

Aby pracować w trybie przenośnym, Kaspersky Endpoint Security instaluje specjalny moduł szyfrowania o nazwie *Przenośny menedżer plików* na dysku wymiennym. Przenośny menedżer plików zapewnia interfejs do pracy z zaszyfrowanymi danymi, jeśli Kaspersky Endpoint Security nie jest zainstalowany na komputerze (patrz rysunek poniżej). Jeśli na Twoim komputerze jest zainstalowany Kaspersky Endpoint Security, możesz pracować z zaszyfrowanymi dyskami wymiennymi przy użyciu zwykłego menedżera plików (na przykład Eksploratora).

Przenośny menedżer plików przechowuje klucz do szyfrowania plików na dysku wymiennym. Klucz jest szyfrowany hasłem użytkownika. Użytkownik ustawia hasło przed zaszyfrowaniem plików na dysku wymiennym.

Przenośny menedżer plików uruchamia się automatycznie, gdy dysk wymienny jest podłączony do komputera, na którym nie jest zainstalowany Kaspersky Endpoint Security. Jeśli automatyczne uruchamianie aplikacji jest wyłączone na komputerze, ręcznie uruchom Przenośny menedżer plików. Aby to zrobić, uruchom plik o nazwie pmv.exe, który jest przechowywany na dysku wymiennym.



Przenośny menedżer plików

Obsługa trybu przenośnego do pracy z zaszyfrowanymi plikami

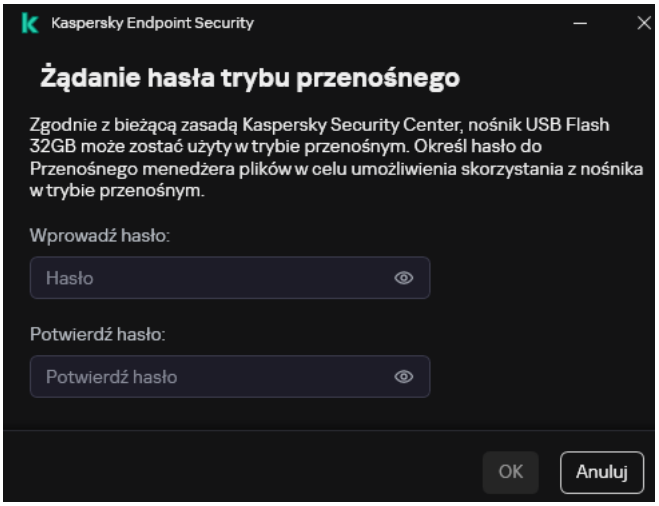
Jak włączyć obsługę trybu przenośnego podczas pracy z zaszyfrowanymi plikami na dyskach wymiennych w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
4. Z listy rozwijalnej **Tryb szyfrowania dla wybranych urządzeń** wybierz **Zaszyfruj wszystkie pliki** lub **Zaszyfruj tylko nowe pliki**.

   Tryb przenośny jest dostępny tylko z Szyfrowaniem plików (FLE). Nie można włączyć obsługi trybu przenośnego dla Szyfrowania całego dysku (FDE).

5. Zaznacz pole **Tryb przenośny**.
6. Jeśli to konieczne, dodaj reguły szyfrowania dla poszczególnych dysków wymiennych.
7. Zapisz swoje zmiany.
8. Po zastosowaniu zasady, podłącz dysk wymienny do komputera.
9. Potwierdź operację szyfrowania nośnika wymiennego.

Zostanie otwarte okno, w którym można utworzyć hasło dla Przenośnego Menedżera plików.



Żądanie hasła trybu przenośnego

10. Określ hasło, które spełnia wymagania co do siły, i potwierdź je.
11. Zapisz swoje zmiany.

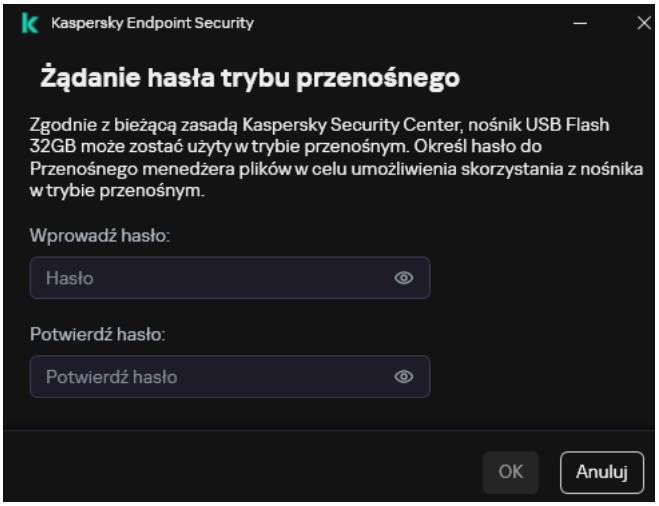
Jak włączyć obsługę trybu przenośnego podczas pracy z zaszyfrowanymi plikami na dyskach wymiennych w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
5. W bloku **Działanie domyślne** wybierz **Zaszyfruj wszystkie pliki** lub **Zaszyfruj tylko nowe pliki**.

   Tryb przenośny jest dostępny tylko z Szyfrowaniem plików (FLE). Nie można włączyć obsługi trybu przenośnego dla Szyfrowania całego dysku (FDE).
6. Zaznacz pole **Tryb przenośny**.
7. Jeśli to konieczne, dodaj reguły szyfrowania dla poszczególnych dysków wymiennych.
8. Zapisz swoje zmiany.
9. Po zastosowaniu zasady, podłącz dysk wymienny do komputera.
10. Potwierdź operację szyfrowania nośnika wymiennego.

Zostanie otwarte okno, w którym można utworzyć hasło dla Przenośnego Menedżera plików.



Żądanie hasła trybu przenośnego

11. Określ hasło, które spełnia wymagania co do siły, i potwierdź je.

12. Zapisz swoje zmiany.

Kaspersky Endpoint Security szyfruje pliki na dysku wymiennym. Przenośny menedżer plików używany do pracy z zaszyfrowanymi plikami także zostanie dodany na nośniku wymiennym. Jeśli na dysku wymiennym znajdują się już zaszyfrowane pliki, Kaspersky Endpoint Security zaszyfruje je ponownie przy użyciu własnego klucza. Umożliwia to użytkownikowi dostęp do wszystkich plików na dysku wymiennym w trybie przenośnym.

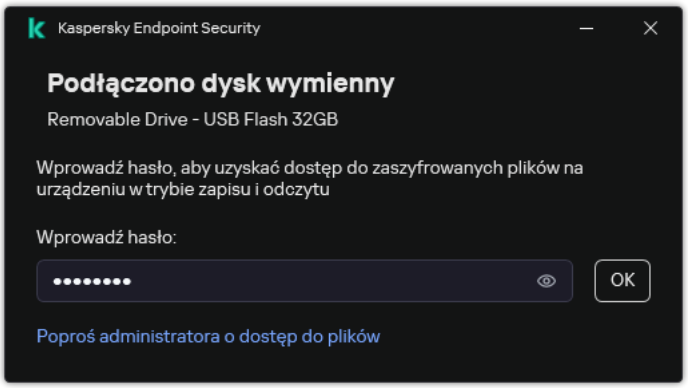
Uzyskiwanie dostępu do zaszyfrowanych plików na dysku wymiennym

Po zaszyfrowaniu plików na dysku wymiennym z obsługą trybu przenośnego dostępne są następujące metody uzyskania dostępu do plików:

- Jeśli Kaspersky Endpoint Security nie jest zainstalowany na komputerze, Przenośny menedżer plików poprosi o podanie hasła. Konieczne będzie wprowadzenie hasła przy każdym ponownym uruchomieniu komputera lub ponownym podłączeniu dysku wymiennego.

- Jeśli komputer znajduje się poza siecią korporacyjną, a na nim jest zainstalowany program Kaspersky Endpoint Security, aplikacja poprosi o podanie hasła lub wyśle administratorowi żądanie dostępu do plików. Po uzyskaniu dostępu do plików na dysku wymiennym Kaspersky Endpoint Security zapisze tajny klucz w pamięci kluczy komputera. Umożliwi to dostęp do plików w przyszłości bez konieczności wprowadzania hasła lub pytania administratora (patrz rysunek poniżej).

- Jeśli komputer znajduje się w sieci korporacyjnej, a na nim jest zainstalowany program Kaspersky Endpoint Security, uzyskasz dostęp do urządzenia bez podawania hasła. Kaspersky Endpoint Security otrzyma tajny klucz z Serwera administracyjnego Kaspersky Security Center, z którym komputer jest połączony.



Uzyskiwanie dostępu do zaszyfrowanych plików na dysku wymiennym

Odzyskiwanie hasła do pracy w trybie przenośnym

Jeśli zapomniałeś hasła do pracy w trybie przenośnym, musisz podłączyć dysk wymienny do komputera z programem Kaspersky Endpoint Security zainstalowanym w sieci korporacyjnej. Uzyskasz dostęp do plików, ponieważ tajny klucz jest przechowywany w pamięci kluczy komputera lub na Serwerze administracyjnym. Odszyfruj i ponownie zaszyfruj pliki za pomocą nowego hasła.

Funkcje trybu przenośnego podczas podłączania dysku wymiennego do komputera z innej sieci

Jeśli komputer znajduje się poza siecią korporacyjną, a na nim jest zainstalowany program Kaspersky Endpoint Security, uzyskasz dostęp do plików w następujące sposoby:

- **Dostęp oparty na haśle**

  Po wprowadzeniu hasła, możliwe będzie przeglądanie, modyfikowanie i zapisywanie plików na dysku wymiennym (*przezroczysty dostęp*). Kaspersky Endpoint Security może ustawić prawo dostępu tylko do odczytu dla dysku wymiennego, jeśli w ustawieniach zasady skonfigurowane są następujące parametry szyfrowania dysków wymiennych:

  - Obsługa trybu przenośnego jest wyłączona.
  - Tryb **Zaszyfruj wszystkie pliki** lub **Zaszyfruj tylko nowe pliki** został wybrany.

  We wszystkich pozostałych przypadkach uzyskasz pełny dostęp do dysku wymiennego (uprawnienie do odczytu/zapisu). Będziesz mógł dodawać i usuwać pliki.

  Możesz zmienić uprawnienia dostępu do dysku wymiennego nawet wtedy, gdy dysk wymienny jest podłączony do komputera. Jeśli uprawnienia dostępu do dysku wymiennego zostały zmienione, Kaspersky Endpoint Security zablokuje dostęp do plików i ponownie wyświetli pytanie o podanie hasła.

  Po wprowadzeniu hasła nie możesz zastosować ustawień zasady szyfrowania do dysku wymiennego. W tym przypadku niemożliwe jest odszyfrowanie lub ponowne zaszyfrowanie plików na dysku wymiennym.

- **Zapytaj administratora o dostęp do plików**

Jeśli zapomniałeś hasła do pracy w trybie przenośnym, poproś administratora o dostęp do plików. Aby uzyskać dostęp do plików, użytkownik powinien wysłać do administratora plik żądania dostępu (plik z rozszerzeniem KESDC). Na przykład, użytkownik może wysłać plik żądania dostępu za pośrednictwem poczty elektronicznej. Administrator wyśle zaszyfrowany plik dostępu do danych (plik z rozszerzeniem KESDR).

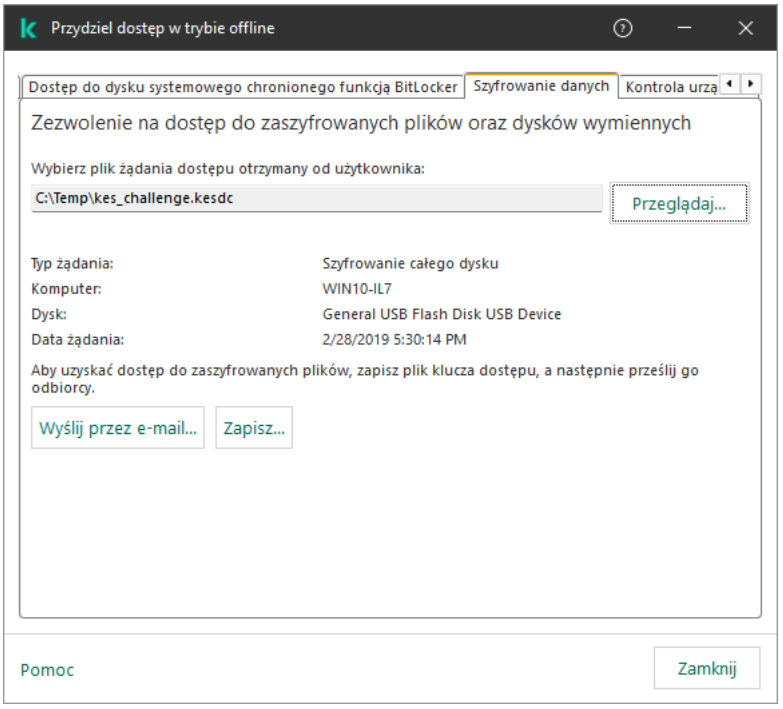
Po zakończeniu procedury odzyskiwania hasła Żądanie-Odpowiedź, uzyskasz przezroczysty dostęp do plików na dysku wymiennym, a także pełny dostęp do dysku wymiennego (uprawnienie do odczytu/zapisu).

Na przykład, możesz zastosować zasadę szyfrowania dysku wymiennego i odszyfrować pliki. Po odzyskaniu hasła lub gdy zasada zostanie zaktualizowana, Kaspersky Endpoint Security wyświetli pytanie o potwierdzenie wprowadzenia zmian.

Jak uzyskać plik dostępu do zaszyfrowanych danych w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Urządzenia**.
3. W zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanych danych, i kliknij go prawym przyciskiem myszy, aby otworzyć menu kontekstowe.
4. Z otwartego menu kontekstowego wybierz **Przydziel dostęp w trybie offline**.
5. Spowoduje to otwarcie okna. Wybierz w nim zakładkę **Szyfrowanie danych**.
6. Na zakładce **Szyfrowanie danych** kliknij przycisk **Przeglądaj**.
7. W oknie wyboru pliku dostępu do żądania określ ścieżkę do pliku otrzymanego od użytkownika.

Zobaczysz informacje o żądaniu użytkownika. Kaspersky Security Center wygeneruje plik klucza. Wyślij do użytkownika wygenerowany plik klucza dostępu do zaszyfrowanych danych. Lub zapisz plik dostępu i użyj dowolnej dostępnej metody, aby przenieść plik.



Przydzielanie dostępu w trybie offline

Jak uzyskać plik dostępu do zaszyfrowanych danych w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Zaznacz pole wyboru obok nazwy komputera, do którego danych chcesz przywrócić dostęp.
3. Kliknij **Udziel dostępu do urządzenia w trybie offline**.
4. Wybierz **Szyfrowanie danych**.
5. Kliknij przycisk **Wybierz plik** i wybierz plik żądania dostępu otrzymany od użytkownika (plik z rozszerzeniem KESDC).

   Konsola Web Console wyświetli informacje o żądaniu. Obejmuje to nazwę komputera, na którym użytkownik żąda dostępu do pliku.
6. Kliknij przycisk **Zapisz klucz** i wybierz folder, aby zapisać plik klucza dostępu do zaszyfrowanych danych (plik z rozszerzeniem KESDR).

W rezultacie będziesz mógł uzyskać klucz dostępu do zaszyfrowanych danych, który będziesz musiał przekazać użytkownikowi.

Deszyfrowanie nośników wymiennych

Możesz użyć zasady do odszyfrowania dysku wymiennego. Dla określonej grupy administracyjnej generowana jest zasada ze zdefiniowanymi ustawieniami szyfrowania dysku wymiennego. Dlatego też wynik deszyfrowania danych na dyskach wymiennych zależy od komputera, do którego podłączony został dysk wymienny.

W celu odszyfrowania dysków wymiennych:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
4. Jeśli chcesz odszyfrować wszystkie zaszyfrowane pliki przechowywane na dyskach wymiennych, z listy rozwijalnej **Tryb szyfrowania** wybierz **Odszyfruj cały dysk wymienny**.

5. Aby odszyfrować dane przechowywane na pojedynczych dyskach wymiennych, zmodyfikuj reguły szyfrowania dla dysków wymiennych, których dane chcesz odszyfrować. W tym celu:

   a. Na liście nośników wymiennych, dla których skonfigurowano reguły szyfrowania, wybierz wpis odpowiadający żądanemu nośnikowi wymiennemu.

   b. Kliknij przycisk **Określ regułę**, aby zmodyfikować regułę szyfrowania dla wybranego dysku wymiennego.

   c. Z menu kontekstowego przycisku **Określ regułę** wybierz element **Odszyfruj cały dysk wymienny**.

6. Zapisz swoje zmiany.

W rezultacie, jeśli użytkownik podłącza dysk wymienny lub jest już podłączony, Kaspersky Endpoint Security odszyfrowuje dysk wymienny. Aplikacja ostrzega użytkownika, że proces deszyfrowania może zająć trochę czasu. Jeśli użytkownik zainicjuje bezpieczne usuwanie dysku wymiennego w trakcie deszyfrowania danych, Kaspersky Endpoint Security przerwie proces deszyfrowania i pozwoli na usunięcie dysku wymiennego przed zakończeniem procesu deszyfrowania. Deszyfrowanie danych będzie kontynuowane następnym razem, gdy dysk wymienny zostanie podłączony do komputera.

Jeśli deszyfrowanie nośnika wymiennego nie powiodło się, przejrzyj raport **Szyfrowanie danych** w interfejsie Kaspersky Endpoint Security. Dostęp do plików może być zablokowany przez inną aplikację. W tym przypadku spróbuj odłączyć nośnik wymienny od komputera i podłączyć go ponownie.

Przeglądanie informacji szczegółowych dotyczących szyfrowania danych

Podczas wykonywania procesu szyfrowania lub deszyfrowania program Kaspersky Endpoint Security wysyła do Kaspersky Security Center informacje o stanie parametrów szyfrowania zastosowanych na komputerach klienckich.

Sprawdzanie stanu szyfrowania

Możesz sprawdzić stan, aby monitorować szyfrowanie danych. Kaspersky Endpoint Security przypisuje następujące stany szyfrowania:

- **Nie spełnia zasad; anulowane przez użytkownika**. Użytkownik anulował szyfrowanie danych.
- **Nie jest zgodne z zasadą z powodu błędu**. Błąd szyfrowania danych, na przykład brak licencji.
- **Stosowanie zasady; wymagane jest ponowne uruchomienie**. Na komputerze przeprowadzane jest szyfrowanie danych. Uruchom ponownie komputer, aby zakończyć szyfrowanie danych.
- **Nie określono zasady szyfrowania**. Szyfrowanie danych jest wyłączone w ustawieniach zasad.
- **Brak obsługi**. Komponenty szyfrowania danych nie są zainstalowane na komputerze.
- **Trwa stosowanie zasady**. Na komputerze przeprowadzane jest szyfrowanie i / lub deszyfrowanie danych.

W celu wyświetlenia stanu szyfrowania danych komputera:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zarządzane urządzenia**.
3. W zakładce **Urządzenia** w obszarze roboczym przesuń suwak w prawą stronę, do samego końca. Jeśli kolumna **Stan szyfrowania** nie jest wyświetlana, dodaj tę kolumnę w ustawieniach konsoli Kaspersky Security Center.

   Kolumna **Stan szyfrowania** wyświetla stan szyfrowania danych na komputerach w wybranej grupie administracyjnej. Ten stan jest tworzony w oparciu o informacje o szyfrowaniu plików na dyskach lokalnych komputera oraz o szyfrowaniu całego dysku.
4. Jeśli stan szyfrowania danych na komputerze to **Stosowanie zasad**, możesz monitorować panel postępu szyfrowania:
   a. Otwórz właściwości komputera w stanie **Stosowanie zasad**, klikając go dwukrotnie.
   b. W oknie ustawień komputera wybierz sekcję **Aplikacje**.
   c. Na liście aplikacji Kaspersky zainstalowanych na komputerze wybierz **Kaspersky Endpoint Security for Windows**.
   d. Kliknij **Statystyka**.
   e. W sekcji **Szyfrowanie urządzeń** możesz zobaczyć aktualny postęp szyfrowania danych w procentach.

Przeglądanie statystyk szyfrowania dotyczących pulpitów nawigacyjnych Kaspersky Security Center

W celu przejrzenia statystyk szyfrowania dotyczących pulpitów nawigacyjnych Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
3. W obszarze roboczym po prawej stronie drzewa Konsoli administracyjnej, wybierz zakładkę **Statystyki**.
4. Utwórz nową stronę z panelami szczegółów zawierającą statystyki szyfrowania danych. W tym celu:
   a. Na zakładce **Statystyki** kliknij przycisk **Dostosuj widok**.
   b. W otwartym oknie kliknij przycisk **Dodaj**.
   c. To spowoduje otwarcie okna; w tym oknie, w sekcji **Ogólne** wprowadź nazwę strony.
   d. W sekcji **Panele informacyjne** kliknij przycisk **Dodaj**.
   e. W otwartym oknie, w grupie **Stan ochrony** wybierz element **Szyfrowanie urządzeń**.
   f. Kliknij **OK**.
   g. Jeśli to konieczne, edytuj ustawienia panelu szczegółów. Aby to zrobić, skorzystaj z sekcji **Widok** i **Urządzenia**.

h. Kliknij **OK**.

i. Powtórz czynności z kroków d – h, wybierając element **Szyfrowanie dysków wymiennych** w sekcji **Stan ochrony**.

Dodane panele szczegółów pojawią się na liście **Panele informacyjne**.

j. Kliknij **OK**.

Nazwa strony z panelami szczegółów utworzona w poprzednich krokach pojawi się na liście **Strony**.

k. Kliknij przycisk **Zamknij**.

5. Na zakładce **Statystyki** otwórz stronę utworzoną w poprzednich krokach instrukcji.

Pojawią się panele szczegółów wyświetlające stan szyfrowania komputerów i dysków wymiennych.

Przeglądanie błędów szyfrowania plików na lokalnych dyskach komputera

W celu wyświetlenia błędów szyfrowania plików na lokalnych dyskach komputera:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zarządzane urządzenia**.
3. W zakładce **Urządzenia** wybierz nazwę komputera z listy i kliknij go prawym przyciskiem myszy, aby otworzyć menu kontekstowe.
4. Z menu kontekstowego komputera wybierz element **Właściwości**. W otwartym oknie wybierz sekcję **Ochrona**.
5. Kliknij odnośnik **Wyświetl błędy szyfrowania danych**, aby otworzyć okno **Błędy szyfrowania danych**.

To okno wyświetla szczegółowe informacje dotyczące błędów szyfrowania plików na lokalnych dyskach komputera. Po naprawieniu błędu, Kaspersky Security Center usunie szczegóły dotyczące błędu z okna **Błędy szyfrowania danych**.

Przeglądanie raportu z szyfrowania danych

Kaspersky Security Center umożliwia tworzenie raportów dotyczących szyfrowania danych:

- **Raport o stanie szyfrowania zarządzanych urządzeń**. Raport zawiera informacje o tym, czy stan szyfrowania komputera jest zgodny z zasadą szyfrowania.
- **Raport o stanie szyfrowania urządzeń pamięci masowej**. Raport zawiera informacje o stanie szyfrowania urządzeń zewnętrznych i urządzeń pamięci masowej.
- **Raport o prawach dostępu do zaszyfrowanych dysków**. Raport zawiera informacje o stanie kont, które mają dostęp do zaszyfrowanych dysków.

- **Raport o błędach podczas szyfrowania plików**. Raport zawiera informacje o błędach, które wystąpiły podczas wykonywania zadań szyfrowania lub odszyfrowywania danych na komputerach.
- **Raport o zablokowanym dostępie do zaszyfrowanych plików**. Raport zawiera informacje o blokowaniu aplikacjom dostępu do zaszyfrowanych plików.

W celu wyświetlenia raportu z szyfrowania danych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Raporty**.
3. Kliknij przycisk **Nowy szablon raportu**.

   Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu.
4. Postępuj zgodnie z instrukcjami Kreatora szablonu raportu. W oknie **Wybieranie typu szablonu raportu** w sekcji **Inne** wybierz jeden z raportów z szyfrowania danych.

   Po zakończeniu pracy Kreatora tworzenia nowego szablonu raportu, nowy szablon raportu pojawi się w tabeli, na zakładce **Raporty**.
5. Wybierz szablon raportu, który został utworzony w poprzednich krokach instrukcji.
6. Z menu kontekstowego szablonu wybierz **Pokaż raport**.

Zostanie rozpoczęty proces tworzenia raportu. Raport zostanie wyświetlony w nowym oknie.

Praca z zaszyfrowanymi urządzeniami, gdy nie ma dostępu do nich

Uzyskiwanie dostępu do zaszyfrowanych urządzeń

Prośba o dostęp do zaszyfrowanych urządzeń może być konieczna w następujących przypadkach:

- Dysk twardy został zaszyfrowany na innym komputerze.
- Klucz szyfrowania dla urządzenia nie znajduje się na komputerze (na przykład, po pierwszej próbie dostępu do zaszyfrowanego nośnika wymiennego na komputerze), a komputer nie jest połączony z Kaspersky Security Center.

  Jeśli użytkownik zastosuje klucz dostępu do zaszyfrowanego urządzenia, Kaspersky Endpoint Security zapisze klucz szyfrowania na komputerze użytkownika i zezwoli na dostęp do tego urządzenia po kolejnych próbach uzyskania dostępu nawet wtedy, gdy nie ma połączenia z Kaspersky Security Center.

Dostęp do zaszyfrowanych urządzeń można uzyskać w następujący sposób:

1. Użytkownik wykorzystuje interfejs aplikacji Kaspersky Endpoint Security do utworzenia pliku żądania dostępu z rozszerzeniem kesdc i wysyła go do administratora firmowej sieci LAN.
2. Administrator wykorzystuje Konsolę administracyjną Kaspersky Security Center do utworzenia pliku klucza dostępu z rozszerzeniem kesdr i wysyła go do użytkownika.
3. Użytkownik stosuje klucz dostępu.

Odzyskiwanie danych na zaszyfrowanych urządzeniach

Do pracy z zaszyfrowanymi urządzeniami użytkownik może wykorzystać Narzędzie przywracania zaszyfrowanego urządzenia (zwane dalej Narzędziem przywracania). Taka sytuacja może mieć miejsce w następujących przypadkach:

- Procedura wykorzystania klucza dostępu do uzyskania dostępu nie powiodła się.
- Moduły szyfrujące nie zostały zainstalowane na zaszyfrowanym urządzeniu.

Dane niezbędne do przywrócenia dostępu do zaszyfrowanych urządzeń przy użyciu Narzędzia przywracania znajdują się od jakiegoś czasu w pamięci komputera użytkownika w postaci niezaszyfrowanej. Aby zmniejszyć ryzyko nieautoryzowanego dostępu do tych danych, zalecane jest przywrócenie dostępu do zaszyfrowanych urządzeń na zaufanych komputerach.

Dane na zaszyfrowanych urządzeniach można odzyskać w następujący sposób:

1. Użytkownik wykorzystuje Narzędzie przywracania do utworzenia pliku żądania dostępu z rozszerzeniem fdertc i wysyła go do administratora firmowej sieci LAN.
2. Administrator wykorzystuje Konsolę administracyjną Kaspersky Security Center do utworzenia pliku klucza dostępu z rozszerzeniem fdertr i wysyła go do użytkownika.
3. Użytkownik stosuje klucz dostępu.

Aby przywrócić dane na zaszyfrowanych dyskach twardych, użytkownik może także określić dane uwierzytelniające konta Agenta autoryzacji w Narzędziu przywracania. Jeśli metadane konta Agenta autoryzacji zostały uszkodzone, użytkownik musi zakończyć procedurę przywracania przy użyciu pliku żądania dostępu.

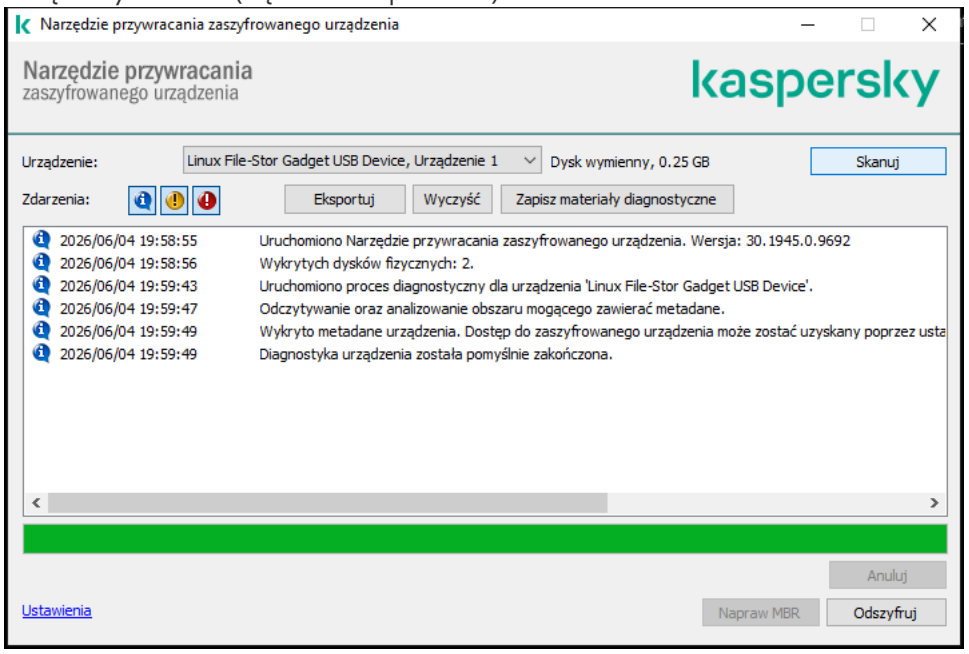
Przed przywróceniem danych na zaszyfrowanych urządzeniach zalecane jest anulowanie profilu Kaspersky Security Center lub wyłączenie szyfrowania w ustawieniach profilu Kaspersky Security Center na komputerze, na którym została wykonana procedura. Zapobiega to ponownemu zaszyfrowaniu urządzenia.

Odzyskiwanie danych za pomocą narzędzia przywracania FDERT

Jeśli dysk twardy ulegnie awarii, system plików może być uszkodzony. W takim przypadku dane chronione przez technologię Kaspersky Disk Encryption będą niedostępne. Możesz odszyfrować dane i skopiować je na nowy dysk.

Odzyskiwanie danych na dysku chronionym przez technologię Kaspersky Disk Encryption składa się z następujących kroków:

1. Utwórz autonomiczne narzędzie przywracania (patrz rysunek poniżej).
2. Podłącz dysk do komputera, na którym nie są zainstalowane komponenty szyfrujące Kaspersky Endpoint Security.
3. Uruchom narzędzie przywracania i zdiagnozuj dysk twardy.
4. Uzyskaj dostęp do danych na dysku. Aby to zrobić, wprowadź dane uwierzytelniające Agenta autoryzacji lub rozpocznij procedurę odzyskiwania (Żądanie-Odpowiedź).



Narzędzie przywracania FDERT

Tworzenie autonomicznego narzędzia przywracania

W celu utworzenia pliku wykonywalnego Narzędzia przywracania zaszyfrowanego urządzenia:

1. W oknie głównym aplikacji kliknij przycisk .
2. W otwartym oknie kliknij przycisk **Przywróć zaszyfrowane urządzenie**.

   Zostanie uruchomione Narzędzie do przywracania zaszyfrowanego urządzenia.

3. W oknie Narzędzia przywracania kliknij przycisk **Utwórz wersję autonomiczną Narzędzia przywracania**.

4. Zapisz autonomiczne narzędzie przywracania do pamięci komputera.

   W rezultacie plik wykonywalny narzędzia przywracania (fdert.exe) zostanie zapisany w określonym folderze. Skopiuj narzędzie przywracania na komputer, na którym nie są zainstalowane komponenty szyfrujące Kaspersky Endpoint Security. Zapobiega to ponownemu zaszyfrowaniu dysku.

Dane niezbędne do przywrócenia dostępu do zaszyfrowanych urządzeń przy użyciu Narzędzia przywracania znajdują się od jakiegoś czasu w pamięci komputera użytkownika w postaci niezaszyfrowanej. Aby zmniejszyć ryzyko nieautoryzowanego dostępu do tych danych, zalecane jest przywrócenie dostępu do zaszyfrowanych urządzeń na zaufanych komputerach.

Odzyskiwanie danych na dysku twardym

W celu przywrócenia dostępu do zaszyfrowanego urządzenia przy użyciu Narzędzia przywracania zaszyfrowanego urządzenia:

1. Uruchom plik o nazwie fdert.exe, który jest plikiem wykonywalnym narzędzia przywracania. Ten plik jest tworzony przez Kaspersky Endpoint Security.

2. W oknie Narzędzie przywracające wybierz zaszyfrowane urządzenie, do którego dostęp chcesz odzyskać.

3. Kliknij przycisk **Skanuj**, aby umożliwić narzędziu określenie akcji, jakie powinny zostać podjęte na urządzeniu: czy powinno zostać odblokowane, czy odszyfrowane.

   Jeśli komputer posiada dostęp do funkcji szyfrowania programu Kaspersky Endpoint Security, Narzędzie przywracania wyświetli okno z pytaniem o odblokowanie urządzenia. Mimo, że odblokowanie urządzenia nie odszyfrowuje go, w wyniku odblokowania urządzenie staje się bezpośrednio dostępne. Jeśli komputer nie posiada dostępu do funkcji szyfrowania programu Kaspersky Endpoint Security, Narzędzie przywracania wyświetli okno z pytaniem o odszyfrowanie urządzenia.

4. Jeśli chcesz zaimportować informacje diagnostyczne, kliknij przycisk **Zapisz materiały diagnostyczne**.

   Narzędzie zapisze archiwum z plikami zawierającymi informacje diagnostyczne.

5. Kliknij przycisk **Napraw MBR**, jeśli diagnostyka zaszyfrowanego systemowego dysku twardego zwróciła wiadomość o problemach związanych z głównym rekordem rozruchowym (MBR) urządzenia.

   Naprawienie głównego rekordu rozruchowego urządzenia może przyśpieszyć proces uzyskiwania informacji niezbędnych do odblokowywania lub deszyfrowania urządzenia.

6. W zależności od wyników diagnostyki kliknij przycisk **Odblokuj** lub **Odszyfruj**.

7. Jeśli chcesz przywrócić dane przy użyciu konta Agenta autoryzacji, wybierz opcję **Użyj ustawień konta Agenta autoryzacji** i wprowadź dane uwierzytelniające Agenta autoryzacji.

   Ta metoda jest możliwa tylko podczas przywracania danych na systemowym dysku twardym. Jeśli systemowy dysk twardy został uszkodzony, a dane konta Agenta autoryzacji zostały utracone, przywrócenie danych na zaszyfrowanym urządzeniu będzie możliwe po uzyskaniu klucza dostępu od administratora firmowej sieci LAN.

8. Jeśli chcesz rozpocząć procedurę odzyskiwania, wykonaj następujące czynności:

   a. Wybierz opcję **Określ ręcznie klucz dostępu do urządzenia**.

   b. Kliknij przycisk **Pobierz klucz dostępu** i zapisz plik żądania dostępu do pamięci komputera (plik z rozszerzeniem FDERTC).

   c. Wyślij plik żądania dostępu do administratora firmowej sieci LAN.

   > Nie zamykaj okna **Pobierz klucz dostępu do urządzenia**, dopóki nie otrzymasz klucza dostępu. Jeśli to okno zostanie otwarte ponownie, nie będziesz mógł zastosować klucza dostępu, który wcześniej został utworzony przez administratora.

   d. Pobierz i zapisz plik dostępu (plik z rozszerzeniem FDERTR) utworzony i wysłany przez administratora korporacyjnej sieci LAN (patrz instrukcje poniżej).

   e. Pobierz plik dostępu w oknie **Pobierz klucz dostępu do urządzenia**.

9. Jeśli odszyfrowujesz urządzenie, musisz skonfigurować dodatkowe ustawienia odszyfrowywania:

   - Określ deszyfrowany obszar:
     - Jeśli chcesz odszyfrować całe urządzenie, zaznacz opcję **Odszyfruj całe urządzenie**.
     - Jeśli chcesz odszyfrować część danych na urządzeniu, zaznacz opcję **Odszyfruj określone obszary urządzenia** i określ granice obszaru deszyfrowania.
   - Wybierz miejsce zapisu odszyfrowanych danych:
     - Jeśli chcesz, żeby dane na oryginalnym urządzeniu były nadpisane odszyfrowanymi danymi, odznacz pole **Odszyfruj do pliku obrazu dysku**.
     - Jeśli chcesz zapisać odszyfrowane dane w innym miejscu niż oryginalne, zaszyfrowane dane, zaznacz pole **Odszyfruj do pliku obrazu dysku** i użyj przycisku **Przeglądaj**, aby określić miejsce zapisu pliku VHD.

10. Kliknij **OK**.

Proces odblokowania / deszyfrowania urządzenia zostanie uruchomiony.

Jak utworzyć zaszyfrowany plik dostępu do danych w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz folder **Zaawansowane → Ochrona i szyfrowanie danych → Zaszyfrowane dyski**.
3. W obszarze roboczym wybierz zaszyfrowane urządzenie, dla którego chcesz utworzyć plik klucza dostępu, a z menu kontekstowego urządzenia wybierz **Uzyskaj dostęp do urządzenia w Kaspersky Endpoint Security**.

> Jeżeli masz wątpliwości, dla którego komputera został wygenerowany plik żądania dostępu, w drzewie Konsoli administracyjnej wybierz folder **Zaawansowane → Ochrona i szyfrowanie danych**, a następnie w obszarze roboczym kliknij **Uzyskaj klucz szyfrowania urządzenia w Kaspersky Endpoint Security**.

4. W oknie, które zostanie otwarte, wybierz algorytm szyfrowania, którego chcesz użyć: AES256 lub AES56.

   Algorytm szyfrowania danych zależy od biblioteki szyfrowania AES zawartej w pakiecie dystrybucyjnym: *Silne szyfrowanie (AES256)* lub *Uproszczone szyfrowanie (AES56)*. Biblioteka szyfrowania AES jest instalowana wraz z aplikacją.

5. Kliknij przycisk **Przeglądaj**, aby otworzyć okno; w tym oknie określ ścieżkę do pliku żądania z rozszerzeniem fdertc, które zostało otrzymane od użytkownika.

6. Kliknij **Odblokuj**.

Zobaczysz informacje o żądaniu użytkownika. Kaspersky Security Center wygeneruje plik klucza. Wyślij do użytkownika wygenerowany plik klucza dostępu do zaszyfrowanych danych. Lub zapisz plik dostępu i użyj dowolnej dostępnej metody, aby przenieść plik.

Jak utworzyć zaszyfrowany plik dostępu do danych w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Operacje → Ochrona i szyfrowanie danych → Zaszyfrowane dyski**.

2. Zaznacz pole wyboru obok nazwy komputera, na którym chcesz odzyskać dane.

3. Kliknij **Udziel dostępu do urządzenia w trybie offline**.

   Spowoduje to uruchomienie Kreatora umożliwiającego uzyskanie dostępu do urządzenia.

4. Postępuj zgodnie z instrukcjami Kreatora, aby przyznać dostęp do urządzenia:

   a. Wybierz wtyczkę Kaspersky Endpoint Security for Windows.

   b. Wybierz algorytm szyfrowania, którego chcesz użyć: AES256 lub AES56.

      Algorytm szyfrowania danych zależy od biblioteki szyfrowania AES zawartej w pakiecie dystrybucyjnym: *Silne szyfrowanie (AES256)* lub *Uproszczone szyfrowanie (AES56)*. Biblioteka szyfrowania AES jest instalowana wraz z aplikacją.

   c. Wybierz plik żądania dostępu otrzymany od użytkownika (plik z rozszerzeniem FDERTC).

   d. Wybierz folder, aby zapisać plik klucza dostępu do zaszyfrowanych danych (plik z rozszerzeniem FDERTR).

W rezultacie będziesz mógł uzyskać klucz dostępu do zaszyfrowanych danych, który będziesz musiał przekazać użytkownikowi.

Tworzenie dysku ratunkowego systemu operacyjnego

Dysk ratunkowy systemu operacyjnego może być przydatny, gdy z jakiegoś powodu nie można uzyskać dostępu do zaszyfrowanego dysku twardego, a system operacyjny nie może zostać załadowany.

Użytkownik może załadować obraz systemu operacyjnego Windows przy użyciu dysku ratunkowego oraz przywrócić dostęp do zaszyfrowanego dysku twardego przy pomocy Narzędzia przywracania zaszyfrowanego urządzenia, załączonego do obrazu systemu operacyjnego.

W celu utworzenia dysku ratunkowego systemu operacyjnego:

1. Utwórz plik wykonywalny Narzędzia przywracania zaszyfrowanego urządzenia.

2. Utwórz niestandardowy obraz środowiska pre-boot systemu Windows. Podczas tworzenia niestandardowego obrazu środowiska pre-boot systemu Windows dodaj do obrazu plik wykonywalny Narzędzia przywracania zaszyfrowanego urządzenia.

3. Zapisz niestandardowy obraz środowiska preinstalacyjnego systemu Windows na dysku rozruchowym, takim jak CD lub nośnik wymienny.

   Instrukcje dotyczące tworzenia niestandardowego obrazu środowiska preinstalacyjnego systemu Windows można znaleźć w plikach pomocy Microsoft (na przykład w zasobach Microsoft TechNet).

Rozwiązania Detection and Response

Rozwiązania Kaspersky Detection and Response to systemy bezpieczeństwa do wykrywania zaawansowanych zagrożeń i wskaźników ataku na różnych poziomach infrastruktury organizacji. Rozwiązania Detection and Response dostarczają informacji o wykrytym zagrożeniu oraz pozwalają zarządzać akcjami Threat Response.

W związku z tym rozwiązanie Detection and Response wykonuje następujące czynności:

- Otrzymywanie informacji o działaniu komputera, serwera lub innych urządzeń (telemetria).
- Automatyczna analiza informacji w celu wykrycia zagrożeń.
- Generowanie szczegółów alertów jako kolumny łańcucha rozwoju zagrożeń do analizy i wybierania działań reakcji na zagrożenia.
- Wykonywanie działań związanych z odpowiedzią na zagrożenie (na przykład izolację komputera od sieci).

Kaspersky Endpoint Security obsługuje rozwiązania Detection and Response, korzystając z agenta wbudowanego. Wbudowany agent wysyła dane telemetryczne do serwerów rozwiązań i przeprowadza akcje Threat Response. Agent wbudowany obsługuje:

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)
- Kaspersky Anti Targeted Attack Platform:
  - Endpoint Detection and Response (EDR) w wersji 7.1 lub starszej
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

Rozwiązanie Kaspersky Endpoint Security z funkcją Detection and Response można stosować w różnych konfiguracjach, na przykład: [EDR Optimum+MDR].

Licencje MDR i EDR Optimum

Kaspersky Endpoint Security obsługuje rozwiązania Kaspersky Managed Detection and Response (MDR) i Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). Możesz używać Kaspersky Endpoint Security z tymi rozwiązaniami w różnych konfiguracjach i zbudować niestandardowy system ochrony, który spełni Twoje szczególne wymagania. W tym celu należy zakupić licencję na każde z tych rozwiązań. Licencja może obejmować prawo do korzystania z jednego rozwiązania (np. tylko dodatku MDR) lub kilku rozwiązań, dodatku [EDR Optimum+MDR].

Rozwiązania MDR i EDR Optimum obsługują następujące metody licencjonowania:

- Funkcja MDR lub EDR Optimum jest dostępna w ramach licencji Kaspersky Endpoint Security for Windows.

  Funkcja będzie dostępna natychmiast po aktywacji Kaspersky Endpoint Security for Windows. Wystarczy tylko dodać jeden klucz.

- Oddzielne licencje dla MDR lub EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  Funkcja staje się dostępna po dodaniu osobnego klucza dla dodatku MDR, EDR Optimum lub [EDR Optimum+MDR]. W rezultacie na komputerze zostają dodane dwa klucze: klucz dla Kaspersky Endpoint Security i klucz dla MDR lub EDR Optimum. Klucz Kaspersky Endpoint Security należy dodać w pierwszej kolejności.

Kaspersky Endpoint Security umożliwia dodanie tylko jednego *aktywnego klucza* licencji MDR i EDR Optimum. Dlatego aby aktywować oba te rozwiązania, należy dodać jeden klucz [EDR Optimum+MDR] Add-on zamiast osobnego klucza dla każdego rozwiązania. Można także dodać jeden *klucz zapasowy*.

Jeśli podczas wdrażania rozwiązania MDR użyto pliku BLOB, do jego aktywowania nie potrzeba osobnego klucza. Plik BLOB zawiera już informacje o licencji.

Wstępne licencjonowanie rozwiązań

Podczas pierwszej instalacji rozwiązania MDR i EDR Optimum są aktywowane w taki sam sposób, jak aplikacja Kaspersky Endpoint Security. Możesz dodać klucz za pomocą zadania *Dodaj klucz* lub skorzystać z funkcji automatycznego przydziału kluczy. Klucz licencyjny zostanie dodany do aplikacji jako drugi aktywny klucz lub jako klucz zapasowy po zaznaczeniu odpowiedniego pola wyboru.

Przejście z jednej licencji na drugą

Jeśli w Twojej organizacji wdrożono już jedno z tych rozwiązań, a do aplikacji dodano odpowiedni klucz, należy wziąć pod uwagę pewne szczególne kwestie związane z licencjonowaniem nowej konfiguracji. Podczas przechodzenia na inną licencję aplikacja nie dodaje nowego klucza do aplikacji, ale zastępuje bieżący klucz nowym. Jest to spowodowane ograniczeniem, które pozwala aplikacji dodać tylko jeden klucz w celu aktywowania rozwiązania MDR i EDR Optimum.

Załóżmy na przykład, że w Twojej organizacji wdrożono rozwiązanie [EDR Optimum+MDR] i chcesz przejść na konfigurację dodatku MDR. Aby przejść na nową konfigurację, należy zastąpić klucz dodatku [EDR Optimum+MDR] Add-on kluczem dodatku MDR.

Oddzielna licencja na EDR Optimum i MDR (dodatek [EDR Optimum+MDR]) nie jest już dostępna. Jeśli chcesz używać obu tych rozwiązań, musisz aktywować MDR za pomocą pliku BLOB, a EDR Optimum za pomocą klucza licencyjnego.

Dzięki funkcji automatycznego przydzielania kluczy aplikacja odrzuca klucze licencyjne obejmujące tę samą liczbę rozwiązań. Oznacza to, że jeśli masz dodany klucz dodatku EDR Optimum, nie możesz zastąpić tego klucza kluczem dodatku MDR. Można jednak zastąpić klucz dodatku EDR Optimum kluczem dodatku [EDR Optimum+MDR]. Aplikacja odrzuca także klucze w przypadku próby zastąpienia klucza dodatku MDR kluczem dodatku EDR. Aby zastąpić klucz, możesz uruchomić zadanie *Dodaj klucz*. Zadanie *Dodaj klucz* pozwala zastępować klucze licencyjne dowolną liczbą rozwiązań.

Jeśli masz dodany klucz rezerwowy dodatku [EDR Optimum+MDR] Add-on, aby poprawnie dodać aktywny klucz dodatku EDR Optimum lub dodatku MDR, musisz najpierw wymienić klucz rezerwowy na klucz dodatku EDR Optimum lub dodatku MDR. Możesz także usunąć klucz rezerwowy, a następnie zastąpić aktywny klucz.

Kompatybilność z rozwiązaniami EDR innych firm

Za pomocą Kaspersky Endpoint Security możesz chronić stacje robocze i serwery w połączeniu z rozwiązaniami EDR innych firm. Aby wyeliminować fałszywe alarmy, zalecamy dodanie plików wykonywalnych Kaspersky Endpoint Security i Network Agent do strefy zaufanej rozwiązania EDR innej firmy.

Strefa zaufana zapewniająca zgodność z rozwiązaniami EDR innych firm

	Kaspersky Endpoint Security for Windows	Agent sieciowy Kaspersky Security Center
Folder roboczy	`C:\Program Files (x86)\Kaspersky Lab\KES.14.1.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Pliki wykonywalne	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent obsługuje interakcję między aplikacją a innymi rozwiązaniami firmy Kaspersky w celu wykrywania zaawansowanych zagrożeń (np. Kaspersky Sandbox). Rozwiązania Kaspersky są kompatybilne z określonymi wersjami Kaspersky Endpoint Agent.

Aby użyć Kaspersky Endpoint Agent jako części rozwiązań Kaspersky, musisz aktywować te rozwiązania przy użyciu odpowiedniego klucza licencyjnego.

W celu uzyskania kompletnych informacji o Kaspersky Endpoint Agent zawartych w używanym rozwiązaniu oprogramowania oraz w celu uzyskania kompletnych informacji o rozwiązaniu autonomicznym zapoznaj się z pomocą dla odpowiedniego produktu:

- Pomoc dla Kaspersky Anti Targeted Attack Platform
- Pomoc dla Kaspersky Sandbox
- Pomoc dla Kaspersky Endpoint Detection and Response Optimum
- Pomoc dla Kaspersky Managed Detection and Response

Pakiet dystrybucyjny dla Kaspersky Endpoint Security w wersjach 11.2.0–11.8.0 zawiera Kaspersky Endpoint Agent. Możesz wybrać Kaspersky Endpoint Agent podczas instalacji Kaspersky Endpoint Security for Windows. W rezultacie na twoim komputerze zostaną zainstalowane dwie aplikacje: KEA i KES. W programie Kaspersky Endpoint Security 11.9.0 pakiet dystrybucyjny Kaspersky Endpoint Agent nie jest już częścią zestawu dystrybucyjnego Kaspersky Endpoint Security.

Zgodność wersji KEA (w ramach KES) z wersjami KES

Kaspersky Endpoint Security for Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

Kaspersky przełącza wszystkie funkcje Detection and Response na działanie z wbudowanym agentem Kaspersky Endpoint Security zamiast z Kaspersky Endpoint Agent. Firma Kaspersky stopniowo dodaje obsługę tych rozwiązań i wycofuje Kaspersky Endpoint Agent (patrz tabela poniżej). Począwszy od wersji 12.1 aplikacja obsługuje wszystkie rozwiązania Detection and Response. Ponadto, począwszy od wersji 12.1, aplikacja nie jest już kompatybilna z Kaspersky Endpoint Agent, a zainstalowanie obu aplikacji obok siebie na tym samym komputerze nie jest już możliwe.

Wersji Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (komponent Endpoint Detection and Response)	Kaspersky Anti Targeted Attack Platform (komponent Network Detection and Response)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Wbudowany agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	Kaspersky Endpoint Agent
12.6	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**	**Wbudowany agent**

Migracja konfiguracji [KES+KEA] do konfiguracji [KES+wbudowany agent]

Kaspersky Endpoint Security zawiera wbudowanego agenta współpracującego z rozwiązaniami Detection and Response. Nie potrzebujesz już oddzielnej aplikacji Kaspersky Endpoint Agent do pracy z tymi rozwiązaniami. Podczas wdrażania Kaspersky Endpoint Security na komputerach, na których jest zainstalowany Kaspersky Endpoint Agent, rozwiązania Detection and Response będą nadal działać z Kaspersky Endpoint Security. Dodatkowo, Kaspersky Endpoint Agent zostanie usunięty z komputera.

Pakiet dystrybucyjny dla Kaspersky Endpoint Security w wersjach 11.2.0–11.8.0 zawiera Kaspersky Endpoint Agent. Możesz wybrać Kaspersky Endpoint Agent podczas instalacji Kaspersky Endpoint Security for Windows. W rezultacie na twoim komputerze zostaną zainstalowane dwie aplikacje: KEA i KES. W programie Kaspersky Endpoint Security 11.9.0 pakiet dystrybucyjny Kaspersky Endpoint Agent nie jest już częścią zestawu dystrybucyjnego Kaspersky Endpoint Security.

Migrowanie konfiguracji [KES+KEA] do [KES+wbudowany agent] obejmuje następujące etapy:

1. **Aktualizowanie Kaspersky Security Center**

   Zaktualizuj wszystkie komponenty Kaspersky Security Center do wersji 13.2 lub wyższej, w tym Agenta sieciowego, na komputerach użytkowników i Web Console.

2. **Aktualizowanie wtyczki webowej Kaspersky Endpoint Security**

W Kaspersky Security Center Web Console uaktualnij wtyczkę sieciową Kaspersky Endpoint Security do wersji 11.7.0 lub wyższej. Aby zarządzać komponentami EDR Optimum i Kaspersky Sandbox, musisz korzystać z Web Console.

Aby korzystać z Kaspersky Anti Targeted Attack Platform (EDR), będziesz potrzebować wtyczki sieciowej dla Kaspersky Endpoint Security w wersji 12.1 lub nowszej.

Aby korzystać z Kaspersky Anti Targeted Attack Platform (NDR), będziesz potrzebować wtyczki sieciowej dla Kaspersky Endpoint Security w wersji 12.7 lub nowszej.

3. **Migrowanie zasady i zadań**

   Użyj Kreatora migracji zadań i zasad Kaspersky Endpoint Agent, aby przenieść ustawienia Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows.

   To spowoduje utworzenie nowej zasady Kaspersky Endpoint Security. Nowa zasada posiada stan *Nieaktywny*. Aby zastosować zasadę, otwórz właściwości zasady, zaakceptuj Oświadczenie Kaspersky Security Network i ustaw stan na *Aktywny*.

4. **Funkcjonalność licencjonowania**

   Jeśli do aktywowania Kaspersky Endpoint Security for Windows i Kaspersky Endpoint Agent używasz wspólnej licencji dla Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security, funkcjonalność EDR Optimum zostanie aktywowana automatycznie po zaktualizowaniu aplikacji do wersji 11.7.0. Nie musisz robić nic innego.

   Jeśli do aktywowania funkcjonalności EDR Optimum używasz autonomicznej licencji Kaspersky Endpoint Detection and Response Optimum Add-on, musisz upewnić się, że klucz EDR Optimum Add-on zostanie dodany do repozytorium Kaspersky Security Center, a funkcjonalność automatycznej dystrybucji klucza licencyjnego zostanie włączona. Po zaktualizowaniu aplikacji do wersji 11.7.0, funkcjonalność EDR Optimum zostanie aktywowana automatycznie.

   Jeśli do aktywowania Kaspersky Endpoint Agent użyjesz licencji dla Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security, a do aktywowania Kaspersky Endpoint Security for Windows użyjesz innej licencji, musisz zastąpić klucz Kaspersky Endpoint Security for Windows standardowym kluczem Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security. Możesz zastąpić klucz przy użyciu zadania *Dodaj klucz*.

   Nie musisz aktywować funkcjonalności Kaspersky Sandbox. Funkcjonalność Kaspersky Sandbox będzie dostępna natychmiast po zaktualizowaniu i aktywowaniu Kaspersky Endpoint Security for Windows.

   Tylko licencja Kaspersky Anti Targeted Attack Platform może zostać użyta do aktywacji Kaspersky Endpoint Security w ramach rozwiązania Kaspersky Anti Targeted Attack Platform. Po zaktualizowaniu aplikacji do wersji 12.1, funkcjonalność EDR (KATA) zostanie aktywowana automatycznie. Nie musisz robić nic innego.

5. **Aktualizowanie aplikacji Kaspersky Endpoint Security**

   Aby zaktualizować aplikację i migrować funkcję EDR Optimum i Kaspersky Sandbox, zalecane jest wykonanie zadania zdalnej instalacji.

   W celu zaktualizowania aplikacji przy użyciu zadania zdalnej instalacji, musisz edytować następujące ustawienia:

   - Wybierz komponenty dla rozwiązań Detection and Response w ustawieniach pakietu instalacyjnego.
   - Wyklucz komponent Kaspersky Endpoint Agent w ustawieniach pakietu instalacyjnego (w przypadku Kaspersky Endpoint Security for Windows w wersjach 11.2.0–11.8.0).
   - Jeśli włączona jest funkcja Ochrona hasłem, która ogranicza dostęp do Kaspersky Endpoint Agent, wprowadź hasło dezinstalacyjne w ustawieniach zadania *Zdalna instalacja aplikacji*. Hasło dezinstalacyjne można wprowadzać, począwszy od Kaspersky Security Center Linux 15.1.

Możesz także zaktualizować aplikację za pomocą następujących metod:

- Przy użyciu usługi aktualizacji Kaspersky (Seamless Update – SMU).
- Lokalnie, za pomocą Kreatora instalacji.

Kaspersky Endpoint Security obsługuje automatyczne wybieranie komponentów podczas aktualizacji aplikacji na komputerze z zainstalowaną aplikacją Kaspersky Endpoint Agent. Automatyczne wybieranie komponentów zależy od uprawnień konta użytkownika, które aktualizuje aplikację.

Jeśli aktualizujesz Kaspersky Endpoint Security przy użyciu pliku EXE lub MSI z poziomu konta systemowego (SYSTEM), Kaspersky Endpoint Security uzyskuje dostęp do bieżących licencji rozwiązań firmy Kaspersky. Dlatego też, jeśli na komputerze jest, na przykład, zainstalowany Kaspersky Endpoint Agent i aktywowane rozwiązanie EDR Optimum, instalator Kaspersky Endpoint Security automatycznie konfiguruje zestaw komponentów i wybiera komponent EDR Optimum. To powoduje przełączenie Kaspersky Endpoint Security na używanie wbudowanego agenta i usunięcie Kaspersky Endpoint Agent. Uruchomienie instalatora MSI z poziomu konta systemowego (SYSTEM) jest zazwyczaj wykonywane podczas aktualizacji za pośrednictwem usługi aktualizacji Kaspersky (SMU) lub podczas wdrażania pakietu instalacyjnego za pośrednictwem Kaspersky Security Center.

Jeśli aktualizujesz Kaspersky Endpoint Security przy użyciu pliku MSI z poziomu konta użytkownika bez uprawnień, Kaspersky Endpoint Security nie ma dostępu do bieżących licencji dla rozwiązań Kaspersky. W tym przypadku Kaspersky Endpoint Security automatycznie wybiera komponenty w oparciu o konfigurację Kaspersky Endpoint Agent. Następnie Kaspersky Endpoint Security przełączy się na korzystanie z wbudowanego agenta i usunie Kaspersky Endpoint Agent.

6. **Ponowne uruchomienie komputera**

   Uruchom ponownie komputer, aby zakończyć aktualizowanie aplikacji za pomocą wbudowanego agenta. Podczas aktualizowania aplikacji instalator usuwa Kaspersky Endpoint Agent przed ponownym uruchomieniem komputera. Po ponownym uruchomieniu komputera instalator dodaje wbudowanego agenta. Oznacza to, że Kaspersky Endpoint Security nie będzie pełnił funkcji EDR i Kaspersky Sandbox do momentu ponownego uruchomienia komputera.

7. **Sprawdzanie zdrowia Kaspersky Endpoint Detection and Response Optimum i Kaspersky Sandbox**

   Jeśli po aktualizacji, komputer posiada stan *Krytyczny* w konsoli Kaspersky Security Center:

   - Upewnij się, że na komputerze jest zainstalowany Agent sieciowy w wersji 13.2 lub wyższej.
   - Sprawdź stan działania komponentów, przeglądając *Raport o stanie składników aplikacji*. Jeśli komponent ma stan *Nie zainstalowano*, zainstaluj komponent przy użyciu zadania *Zmiana składników aplikacji*.
   - Upewnij się, że akceptujesz Oświadczenie Kaspersky Security Network w nowej zasadzie Kaspersky Endpoint Security for Windows.
   - Upewnij się, że funkcja EDR Optimum została aktywowana za pomocą opcji *Raport o stanie składników aplikacji*. Jeśli komponent posiada stan *Nieobjęte licencją*, upewnij się, że funkcjonalność automatycznej dystrybucji klucza licencyjnego EDR Optimum jest włączona.

Migracja zasad i zadań dla Kaspersky Endpoint Agent

Kaspersky Endpoint Security for Windows zawiera kreator migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security. Możesz migrować ustawienia zasady i zadania dla następujących rozwiązań:

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

Kreator migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security działa tylko w usługach Web Console i Cloud Console. W Konsoli administracyjnej (MMC) możesz migrować ustawienia dla rozwiązania Kaspersky Anti Targeted Attack Platform (EDR) tylko za pomocą standardowego Kreatora migracji zasad i zadań Kaspersky Security Center.

Zalecane jest rozpoczęcie migracji Kaspersky Endpoint Agent do Kaspersky Endpoint Security na pojedynczym komputerze, następnie zrób to na grupie komputerów, a następnie zakończ migrację na wszystkich komputerach w organizacji.

W celu migracji ustawień zasady i zadania z Kaspersky Endpoint Agent do Kaspersky Endpoint Security:

w oknie głównym Web Console wybierz **Operacje** → **Migracja z Kaspersky Endpoint Agent**.

To spowoduje uruchomienie Kreatora migracji zasad i zadań. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Migracja zasady

Kreator migracji tworzy nową zasadę, która scala ustawienia zasad Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Na liście zasad wybierz zasady Kaspersky Endpoint Agent, których ustawienia chcesz scalić z zasadą Kaspersky Endpoint Security. Kliknij zasadę Kaspersky Endpoint Agent, aby wybrać zasadę Kaspersky Endpoint Security, z którą chcesz scalić ustawienia. Upewnij się, że wybrałeś poprawne zasady i przejdź do następnego kroku.

Krok 2. Migracja zadania

Kreator migracji tworzy nowe zadania dla Kaspersky Endpoint Security. Na liście zadań wybierz zadania Kaspersky Endpoint Agent, które chcesz utworzyć dla zasady Kaspersky Endpoint Security. Kreator obsługuje zadania dla Kaspersky Endpoint Detection and Response i dla Kaspersky Sandbox. Przejdź do następnego kroku.

Krok 3. Kończenie działania kreatora

Zakończ działanie Kreatora. W rezultacie kreator wykona następujące czynności:

- Utworzy nową zasadę Kaspersky Endpoint Security.

  Zasada scala ustawienia z Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Zasada zostaje nazwana *<Nazwa zasady Kaspersky Endpoint Security> & <Nazwa zasady Kaspersky Endpoint Agent>*. Nowa zasada posiada stan *Nieaktywny*. Aby kontynuować, zmień stany zasad Kaspersky Endpoint Agent i Kaspersky Endpoint Security na *Nieaktywny* i aktywuj nową scaloną zasadę.

  Po migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows upewnij się, że nowa zasada posiada funkcjonalność przesyłania danych do Serwera administracyjnego (dane pliku poddanego kwarantannie oraz dane łańcucha rozwoju zagrożeń). Wartości parametrów przesyłania danych nie zostają przeniesione z zasady Kaspersky Endpoint Agent.

  Podczas migracji z programu Kaspersky Endpoint Agent do Kaspersky Endpoint Security dla rozwiązania Kaspersky Anti Targeted Attack Platform (EDR) mogą wystąpić błędy z połączeniem komputera do serwerów Central Node. Dzieje się tak, ponieważ kreator migracji w usłudze Web Console pomija następujące ustawienia reguł i nie migruje ich:

  - Zakaz modyfikacji ustawień **Połączenie z serwerami KATA** („blokada").

    Domyślnie ustawienia można modyfikować („blokada" jest otwarta). Dlatego ustawienia nie są stosowane na komputerze. Należy zakazać modyfikacji ustawień i zamknąć „blokadę".

  - Kontener szyfrowania.

    Jeśli do łączenia się z serwerami Central Node używasz uwierzytelniania dwuskładnikowego, należy dodać kontener szyfrowania. Kreator migracji poprawnie migruje certyfikat TLS serwera.

  Kreator migracji reguł i zadań w Konsoli administracyjnej (MMC) migruje wszystkie ustawienia rozwiązania Kaspersky Anti Targeted Attack Platform (EDR).

- Utworzy nowe zadania Kaspersky Endpoint Security.

  Nowe zadania są kopiami zadań Kaspersky Endpoint Agent dla Kaspersky Endpoint Detection and Response i Kaspersky Sandbox. Jednocześnie kreator pozostawia zadania Kaspersky Endpoint Agent niezmienione.

Jak dokonać migracji ustawień zasady i zadania z Kaspersky Endpoint Agent do Kaspersky Endpoint Security w Konsoli administracyjnej (MMC) – tylko w przypadku KATA (EDR)

1. W Konsoli administracyjnej wybierz Serwer administracyjny i kliknij go prawym klawiszem myszy, aby otworzyć menu kontekstowe.
2. Wybierz **Wszystkie zadania → Kreator konwersji zasad i zadań**.

Uruchomi się Kreator konwersji zasad i zadań. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie aplikacji, dla której konieczna jest konwersja zasad i zadań

Na tym etapie należy wybrać Kaspersky Endpoint Security for Windows. Przejdź do następnego kroku.

Krok 2. Konwersja zasad

Kreator migracji utworzy nową zasadę Kaspersky Endpoint Security, do której zostaną przeniesione ustawienia zasad Kaspersky Endpoint Agent. Na liście zasad wybierz zasady Kaspersky Endpoint Agent, których ustawienia chcesz przenieść do zasady Kaspersky Endpoint Security. Przejdź do następnego kroku.

Następnie Kreator migracji rozpocznie konwertowanie zasad. Podczas konwersji zasady Kreator migracji poprosi o zaakceptowanie Oświadczenia Kaspersky Security Network. Nowe zasady będą miały nazwę *<Nazwa zasady> (przekonwertowane)*.

Krok 3. Konwersja zadań

Pomiń ten krok. Kreator obsługuje zadania tylko dla Kaspersky Endpoint Detection and Response Optimum i dla Kaspersky Sandbox. Zarządzanie tymi komponentami jest dostępne tylko w usłudze Web Console. Przejdź do następnego kroku.

Krok 4. Kończenie działania kreatora

Zakończ działanie Kreatora. W wyniku działania kreatora zostanie utworzona nowa zasada Kaspersky Endpoint Security.

Endpoint Detection and Response Agent (EDR Agent)

Począwszy od wersji Kaspersky Endpoint Security 12.3 for Windows, aplikacja zawiera konfigurację Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* to aplikacja instalowana na poszczególnych stacjach roboczych i serwerach w infrastrukturze informatycznej organizacji w celu obsługi następujących rozwiązań Detection and Response firmy Kaspersky:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (od wersji 12.6)
- Kaspersky Anti Targeted Attack Platform (NDR) (od wersji 12.7)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (od wersji 12.11)

EDR Agent nie obsługuje integracji z rozwiązaniem Kaspersky Endpoint Detection and Response Expert (cloud).

EDR Agent stale monitoruje procesy uruchomione na tych komputerach, otwarte połączenia sieciowe i modyfikowane pliki. Komponenty ochrony i kontroli aplikacji nie są dostępne dla EDR Agent.

EDR Agent jest kompatybilny z aplikacjami EPP innych firm. Dzięki temu możesz korzystać z zabezpieczeń infrastruktury innych firm wraz z funkcją Detection and Response firmy Kaspersky.

Aby wdrożyć EDR Agent, na komputerze musi być zainstalowany Agent sieciowy, a komputer musi zostać dodany w konsoli Kaspersky Security Center. Aby umożliwić interakcję EDR Agent z Kaspersky Security Center, musisz zainstalować wtyczkę zarządzającą Kaspersky Endpoint Security for Windows. Możesz określić ustawienia EDR Agent przy pomocy zasad grupy. Aby zintegrować EDR Agent, należy skonfigurować integrację w odpowiednich sekcjach zasad.

Aby wspierać rozwiązania Kaspersky Detection and Response, w infrastrukturze należy zainstalować następujące aplikacje firmy Kaspersky:

	• Agent sieciowy • EDR Agent
Endpoint	
	Informacje o wtyczce zarządzającej Kaspersky Endpoint Security for Windows
Kaspersky Security Center	
	
Rozwiązania Detection and Response: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

Instalowanie EDR Agent

Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent (EDR Agent) dla rozwiązań Kaspersky Detection and Response instaluje się w ten sam sposób.

EDR Agent można zainstalować na komputerze stosując jeden z poniższych sposobów:

- Zdalnie, przy użyciu Kaspersky Security Center.
- Lokalnie, przy pomocy Kreatora Setup.
- Lokalnie, w wierszu poleceń (tylko dla KATA (EDR) i EDR Expert (on-premises)).

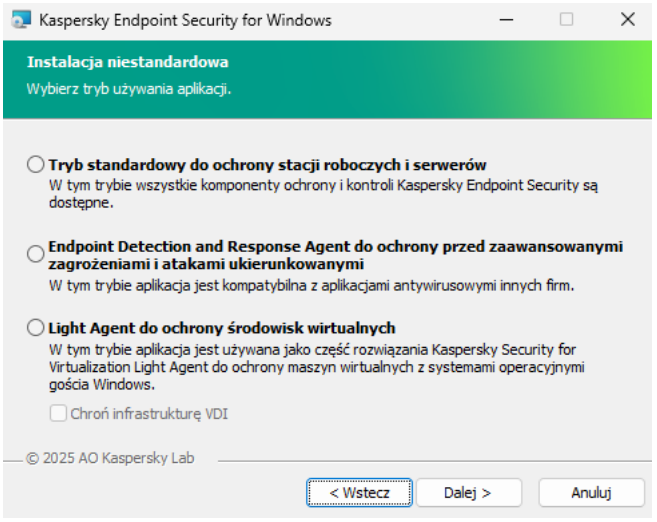
Aby zainstalować EDR Agent, należy wybrać odpowiednią konfigurację w ustawienia pakietu instalacyjnego lub w Kreatorze Setup.

Instalacja EDR Agent przy pomocy Kreatora Setup.

1. Skopiuj folder pakietu dystrybucyjnego na komputer użytkownika.
2. Uruchom setup_kes.exe.

   Zostanie uruchomiony Kreator instalacji.

Konfiguracja Kaspersky Endpoint Security



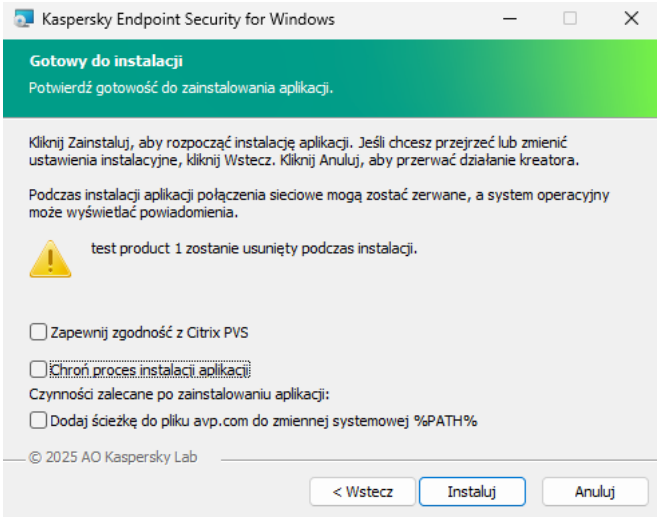
Wybór konfiguracji aplikacji

Wybierz konfigurację **Endpoint Detection and Response Agent**. W tej konfiguracji można zainstalować wyłącznie komponenty zapewniające obsługę rozwiązań wykrywania i reagowania: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), jak również KUMA. Ta konfiguracja jest wymagana, jeśli w Twojej organizacji wdrożona jest platforma Endpoint Protection Platform (EPP) innej firmy wraz z rozwiązaniem Kaspersky Detection and Response. Dzięki temu Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent jest kompatybilny z aplikacjami EPP innych firm.

Komponenty Kaspersky Endpoint Security

Wybierz składniki, które chcesz zainstalować. Możesz zmienić dostępne komponenty aplikacji po zainstalowaniu aplikacji. Aby to zrobić, musisz ponownie uruchomić Kreatora instalacji i wybrać zmianę dostępnych składników.

Ustawienia zaawansowane



Zaawansowane ustawienia instalacji aplikacji

Chroń proces instalacji aplikacji. Ochrona instalacji obejmuje ochronę przed zastąpieniem pakietu dystrybucyjnego szkodliwymi aplikacjami, blokowaniem dostępu do folderu instalacyjnego Kaspersky Endpoint Security, a także blokowaniem dostępu do sekcji rejestru systemu zawierającego klucze aplikacji. Jeżeli aplikacja nie może zostać zainstalowana (na przykład podczas zdalnej instalacji przy użyciu Windows Remote Desktop), zalecane jest wyłączenie ochrony procesu instalacji.

Zapewnij zgodność z Citrix PVS. Możesz włączyć obsługę Citrix Provisioning Services, aby zainstalować Kaspersky Endpoint Security na maszynie wirtualnej.

Dodaj ścieżkę do pliku avp.com do zmiennej systemowej %PATH%. Możesz dodać ścieżkę instalacji do zmiennej %PATH% dla wygodnego korzystania z interfejsu wiersza poleceń.

Instalacja EDR Agent z wiersza poleceń (tylko dla KATA (EDR) i EDR Expert (on-premises))

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się pakiet dystrybucyjny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
   ```

   LUB

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
   ```

   W rezultacie na komputerze instalowana jest aplikacja EDR Agent do integracji z Kaspersky Anti Targeted Attack Platform (EDR) lub Kaspersky Endpoint Detection and Response Expert (on-premises). Możesz potwierdzić, że aplikacja jest zainstalowana i sprawdzić ustawienia aplikacji, publikując polecenie `status`.

Instalacja EDR Agent przy pomocy Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz folder **Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

   Spowoduje to otwarcie listy pakietów instalacyjnych, które zostały pobrane do Kaspersky Security Center.
3. Otwórz właściwości pakietu instalacyjnego.

   Jeśli to konieczne, utwórz nowy pakiet instalacyjny.
4. Przejdź do sekcji **Składniki ochrony**.
5. Wybierz konfigurację **Endpoint Detection and Response Agent do ochrony przed zaawansowanymi zagrożeniami i atakami ukierunkowanymi**. W tej konfiguracji można zainstalować wyłącznie komponenty zapewniające obsługę rozwiązań wykrywania i reagowania: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), jak również KUMA. Ta konfiguracja jest wymagana, jeśli w Twojej organizacji wdrożona jest platforma Endpoint Protection Platform (EPP) innej firmy wraz z rozwiązaniem Kaspersky Detection and Response. Dzięki temu Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent jest kompatybilny z aplikacjami EPP innych firm.
6. Wybierz składniki, które chcesz zainstalować.

   Możesz zmienić dostępne komponenty aplikacji po zainstalowaniu aplikacji.

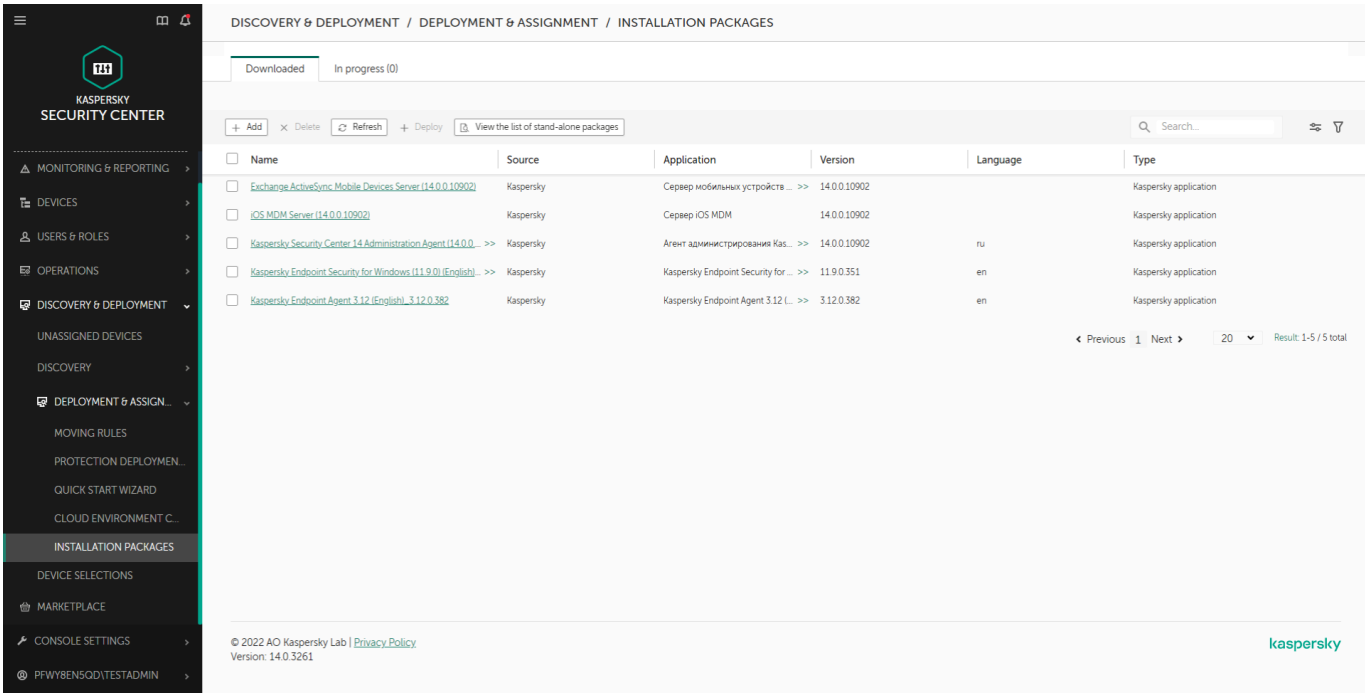
7. Zapisz swoje zmiany.

8. Utwórz zadanie zdalnej instalacji. We właściwościach zadania wybierz utworzony pakiet instalacyjny.

Instalacja EDR Agent przy użyciu Web Console

1. W oknie głównym Web Console wybierz **Wykrywanie i wdrażanie → Wdrażanie i przypisywanie → Pakiety instalacyjne**.

   Spowoduje to otwarcie listy pakietów instalacyjnych, które zostały pobrane do Kaspersky Security Center.



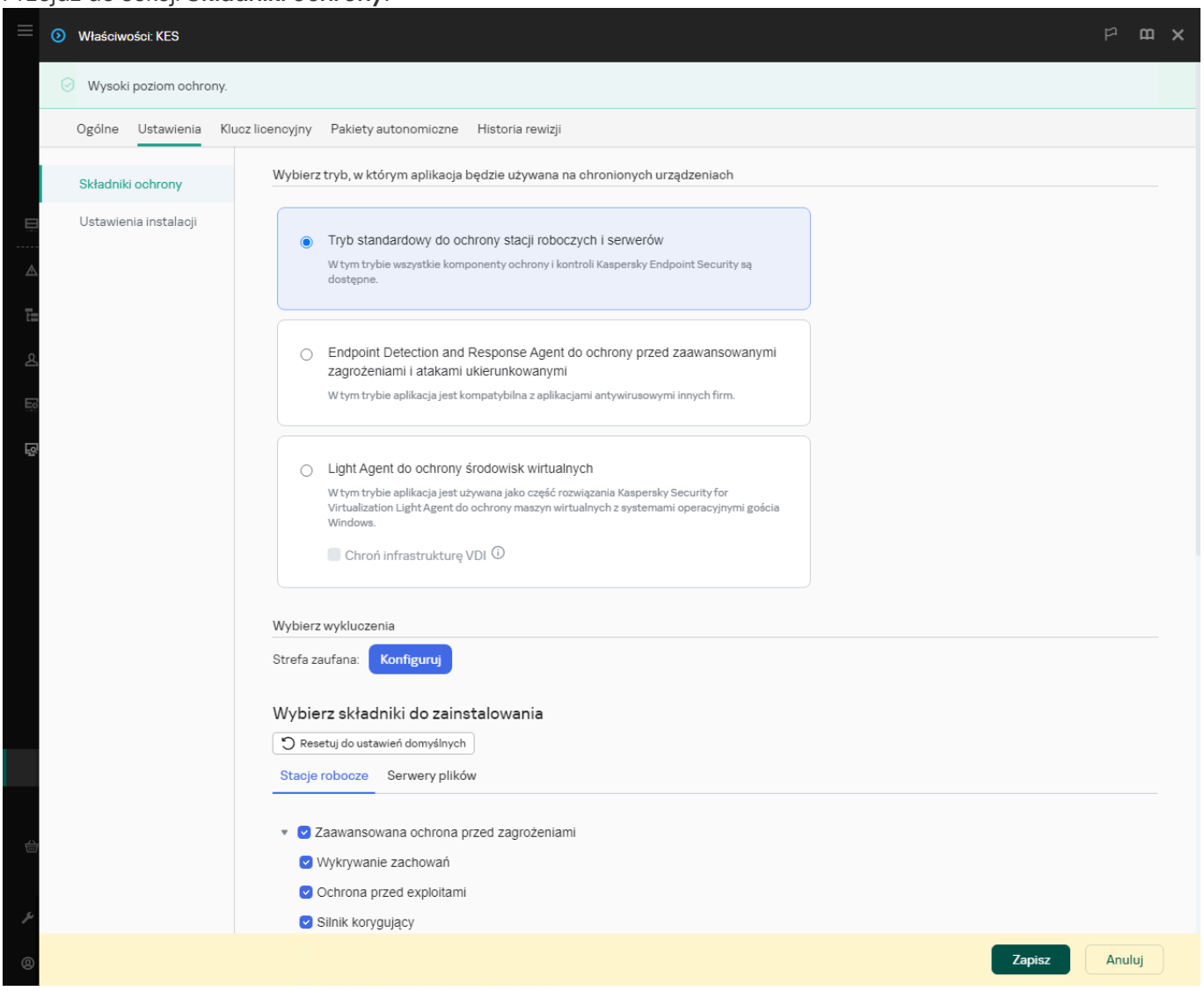
Lista pakietów instalacyjnych

2. Otwórz właściwości pakietu instalacyjnego.

   Jeśli to konieczne, utwórz nowy pakiet instalacyjny.

3. Wybierz zakładkę **Ustawienia**.

4. Przejdź do sekcji **Składniki ochrony**.



Komponenty zawarte w pakiecie instalacyjnym

5. Wybierz konfigurację **Endpoint Detection and Response Agent do ochrony przed zaawansowanymi zagrożeniami i atakami ukierunkowanymi**. W tej konfiguracji można zainstalować wyłącznie komponenty zapewniające obsługę rozwiązań wykrywania i reagowania: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), jak również KUMA. Ta konfiguracja jest wymagana, jeśli w Twojej organizacji wdrożona jest platforma Endpoint Protection Platform (EPP) innej firmy wraz z rozwiązaniem Kaspersky Detection and Response. Dzięki temu Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent jest kompatybilny z aplikacjami EPP innych firm.

6. Wybierz składniki, które chcesz zainstalować.

   Możesz zmienić dostępne komponenty aplikacji po zainstalowaniu aplikacji.

7. Zapisz swoje zmiany.

8. Utwórz zadanie zdalnej instalacji. We właściwościach zadania wybierz utworzony pakiet instalacyjny.

W efekcie EDR Agent zostanie zainstalowany na komputerze użytkownika. Możesz skorzystać z interfejsu aplikacji, a w obszarze powiadomień wyświetlana jest ikona aplikacji .

W Kaspersky Security Center komputer z zainstalowaną aplikacją w konfiguracji EDR Agent posiada stan *Krytyczny* – . Komputer ma ten stan, ponieważ brakuje składnika Ochrona plików. Nie musisz podejmować żadnych dodatkowych działań.

Jeśli nie mogłeś zainstalować EDR Agent na komputerze z aplikacją EPP innej firmy, ponieważ instalator znalazł na komputerze niekompatybilne oprogramowanie, możesz pomiń sprawdzanie niezgodnego oprogramowania.



Główne okno EDR Agent

Teraz musisz skonfigurować integrację z rozwiązaniem Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) lub Kaspersky Anti Targeted Attack (NDR). Możesz także określić zaawansowane ustawienia aplikacji i np. utwórz strefę zaufaną Lub ukryj interfejs aplikacji. Dostępne są ustawienia w następujących sekcjach:

- Kaspersky Security Network
- Ustawienia aplikacji
- Ustawienia sieci
- Wykluczenia
- Raporty

- Interfejs
- Zarządzaj ustawieniami

Integracja EDR Agent z MDR

EDR Agent instalowany jest na stacjach roboczych i serwerach w infrastrukturze informatycznej organizacji. EDR Agent przetwarza dane i wysyła je poprzez strumienie Kaspersky Security Network do Kaspersky Managed Detection and Response.

Aby rozwiązanie Kaspersky Managed Detection and Response działało z Serwerem administracyjnym poprzez Kaspersky Security Center Web Console, należy nawiązać nowe bezpieczne połączenie – *połączenie w tle*. Kaspersky Managed Detection and Response wyświetla pytanie o nawiązanie połączenia w tle po wdrożeniu rozwiązania. Upewnij się, że połączenie w tle zostało nawiązane.

Nawiązywanie połączenia w tle w Web Console

1. W oknie głównym Web Console wybierz **Ustawienia** → **Integracja**.
2. Przejdź do sekcji **Integracja**.
3. Włącz przełącznik **Połączenie w tle w celu integracji Włączone**.
4. Zapisz swoje zmiany.

Integracja z Kaspersky Managed Detection and Response obejmuje następujące kroki:

1. **Instalacja komponentu Managed Detection and Response**

   Możesz wybrać składnik MDR podczas instalacji lub aktualizacji, a także przy użyciu zadania *Zmiana składników aplikacji*.

   > Aby zainstalować składnik Managed Detection and Response bez ponownego uruchamiania komputera przy użyciu zadania *Zmiana składników aplikacji*, należy wyłączyć opcję **Usuń niekompatybilne aplikacje innych firm** w ustawieniach zadania.

2. **Konfiguracja Kaspersky Private Security Network**

   > Pomiń ten krok, jeśli używasz Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console automatycznie konfiguruje lokalną sieć Kaspersky Private Security Network podczas instalowania wtyczki MDR.

   Kaspersky Private Security Network (KPSN) to rozwiązanie, które umożliwia użytkownikom komputerów z zainstalowanym programem Kaspersky Endpoint Security lub innymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów.

   Wczytaj plik konfiguracyjny Kaspersky Security Network we właściwościach Serwera administracyjnego. Plik konfiguracyjny Kaspersky Security Network znajduje się w archiwum ZIP pliku konfiguracyjnego MDR. Archiwum ZIP możesz uzyskać w Kaspersky Managed Detection and Response Console. Więcej informacji na temat konfigurowania prywatnej sieci Kaspersky Private Security Network można znaleźć w pomocy dla Kaspersky Security Center. Plik konfiguracyjny Kaspersky Security Network możesz wczytać także z poziomu wiersza polecenia (zapoznaj się z poniższymi instrukcjami).

Jak skonfigurować prywatną sieć Kaspersky Private Security Network z poziomu wiersza polecenia?

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:

   ```
   avp.com KSN /private <file name>
   ```

   gdzie `<file name>` to nazwa pliku konfiguracyjnego zawierającego ustawienia sieci Kaspersky Private Security Network (format pliku PKCS7 lub PEM).

   Na przykład:
   `avp.com KSN /private C:\kpsn_config.pkcs7`

W rezultacie Kaspersky Endpoint Security użyje Kaspersky Private Security Network do określenia reputacji plików, aplikacji i stron internetowych. W sekcji ustawień zasady **Kaspersky Security Network** zostanie wyświetlony następujący stan operacyjny: *Infrastruktura: Kaspersky Private Security Network*.

Musisz włączyć rozszerzony tryb KSN dla Managed Detection and Response, aby działało.

3 Aktywowanie Kaspersky Managed Detection and Response

Począwszy od wersji 12.10 Kaspersky Endpoint Security for Windows, aby aktywować funkcję Managed Detection and Response, jako alternatywę dla kodu aktywacyjnego możesz również użyć pliku kluczowego.

Musisz zakupić osobną licencję dla MDR (dodatek Kaspersky Managed Detection and Response).

Funkcja będzie dostępna po dodaniu oddzielnego klucza dla dodatku Kaspersky Managed Detection and Response. Licencjonowanie dla autonomicznej funkcjonalności Managed Detection and Response jest takie samo, jak w przypadku licencjonowania Kaspersky Endpoint Security.

Upewnij się, że funkcja MDR jest w licencji i jest uruchomiona w lokalnym interfejsie aplikacji.

4 Włączanie komponentu Managed Detection and Response

Załaduj plik konfiguracyjny BLOB w zasadzie Kaspersky Endpoint Security (zapoznaj się z poniższymi instrukcjami). Plik BLOB zawiera ID klienta oraz informacje o licencji dla Kaspersky Managed Detection and Response. Plik BLOB znajduje się w archiwum ZIP pliku konfiguracyjnego MDR. Archiwum ZIP możesz uzyskać w Kaspersky Managed Detection and Response Console. Więcej informacji o pliku BLOB można znaleźć w pomocy dla Kaspersky Managed Detection and Response.

Począwszy od Kaspersky Endpoint Security 12.6 for Windows, dodanie pliku BLOB jest opcjonalne dla Kaspersky Managed Detection and Response bez dzierżawców, jeśli posiadasz aktualną licencję.

Jak włączyć komponent Managed Detection and Response w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.
4. Zaznacz pole **Managed Detection and Response (Industrial CyberSecurity)**.

5. W sekcji **Ustawienia** kliknij **Przekaż** i wybierz plik BLOB pobrany w Kaspersky Managed Detection and Response Console. Plik posiada rozszerzenie P7.

   Domyślnie użytkownik może zarządzać ustawieniami aplikacji (kłódka jest otwarta)). Aby zastosować zasady na komputerach, zamknij kłódki .

6. Zapisz swoje zmiany.

Jak włączyć komponent Managed Detection and Response w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Managed Detection and Response**.
5. Włącz przełącznik **Managed Detection and Response WŁĄCZONO**.
6. Kliknij **Wczytaj** i wybierz plik BLOB, który został uzyskany w Kaspersky Managed Detection and Response Console. Plik posiada rozszerzenie P7.

   Domyślnie użytkownik ma możliwość zarządzania ustawieniami zasad (kłódka jest otwarta)). Aby zastosować zasady na komputerach, zamknij kłódki .

7. Zapisz swoje zmiany.

Jak włączyć komponent Managed Detection and Response z poziomu wiersza polecenia?

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   Aby wykonać to polecenie, Ochrona hasłem musi być włączona. Użytkownik musi mieć uprawnienie **Konfiguracja ustawień aplikacji**.

W wyniku tego program Kaspersky Endpoint Security będzie sprawdzał plik BLOB. Weryfikacja pliku BLOB obejmuje sprawdzanie podpisu cyfrowego i okresu licencjonowania. Jeśli plik BLOB został pomyślnie zweryfikowany, Kaspersky Endpoint Security pobierze plik i wyśle go do komputera podczas kolejnej synchronizacji z Kaspersky Security Center. Sprawdź stan działania komponentu, przeglądając *Raport o stanie składników aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Managed Detection and Response** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

5 Konfigurowanie innych komponentów aplikacji w celu odbierania danych telemetrycznych

Musisz włączyć następujące komponenty dla Managed Detection and Response w celu zapewnienia działania:

- Kaspersky Security Network (tryb rozszerzony).
- Wykrywanie zachowań.
- Ochrona przed exploitami.
- Ochrona WWW.
- Ochrona poczty.
- Ochrona plików.
- Ochrona sieci
- Zapora sieciowa.
- Ochrona AMSI.
- Skanowanie w tle.

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Managed Detection and Response**.
5. Włącz przełącznik **Managed Detection and Response WŁĄCZONO**.
6. Zapisz swoje zmiany.

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Zaznacz pole **Managed Detection and Response (Industrial CyberSecurity)**.
5. Zapisz swoje zmiany.

Integracja EDR Agent z EDR (KATA)

EDR Agent instalowany jest na stacjach roboczych i serwerach w infrastrukturze informatycznej organizacji. Na tych komputerach EDR Agent stale monitoruje procesy, otwarte połączenia sieciowe i modyfikowane pliki oraz wysyła dane monitorujące do serwera za pomocą komponentu Central Node.

Aby zintegrować się z EDR (KATA), należy dodać komponent Endpoint Detection and Response (KATA) oraz skonfigurować EDR Agent.

W celu zapewnienia działania Endpoint Detection and Response (KATA) muszą być spełnione następujące warunki:

- Kaspersky Anti Targeted Attack Platform w wersji 5.0–7.1.
- Kaspersky Security Center w wersji 14.2 lub nowszej. We wcześniejszych wersjach Kaspersky Security Center nie ma możliwości aktywowania funkcji Endpoint Detection and Response (KATA).

https://www.youtube.com/watch?v=cZzgtBoeC7k

Integracja z Endpoint Detection and Response (KATA) obejmuje następujące etapy:

1. **Aktywowanie Endpoint Detection and Response (KATA)**

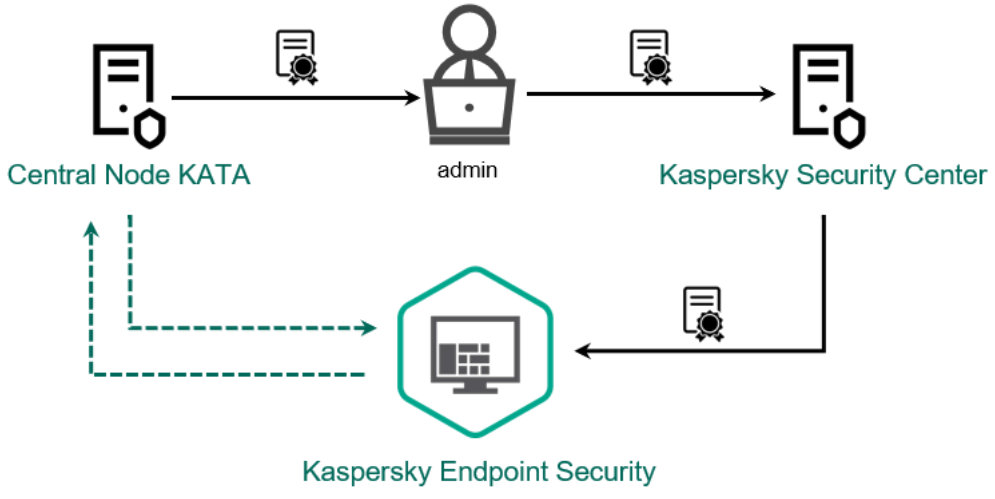
   Musisz zakupić osobną licencję dla korzystania z EDR (KATA) (dodatek Kaspersky Endpoint Detection and Response (KATA)).

   Funkcja będzie dostępna po dodaniu oddzielnego klucza dla Kaspersky Endpoint Detection and Response (KATA). Zasady udzielania licencji dla autonomicznej funkcjonalności Endpoint Detection and Response (KATA) są takie same jak w przypadku udzielania licencji dla Kaspersky Endpoint Security.

   Upewnij się, że funkcja EDR (KATA) znajduje się w licencji i jest uruchomiona w lokalnym interfejsie aplikacji.

2. **Łączenie z węzłem centralnym**

   Kaspersky Anti Targeted Attack Platform wymaga ustanowienia zaufanego połączenia między Kaspersky Endpoint Security a komponentem Central Node. Aby skonfigurować zaufane połączenie, musisz użyć certyfikatu TLS. Możesz uzyskać certyfikat TLS w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w Pomoc Kaspersky Anti Targeted Attack Platform). Następnie musisz dodać certyfikat TLS do Kaspersky Endpoint Security (zobacz instrukcje poniżej).



Dodanie certyfikatu TLS do Kaspersky Endpoint Security

Domyślnie Kaspersky Endpoint Security sprawdza tylko certyfikat TLS węzła centralnego. Aby połączenie było bezpieczniejsze, możesz dodatkowo włączyć weryfikację komputera na Węźle Centralnym (uwierzytelnianie dwukierunkowe). Aby włączyć tę weryfikację, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach węzła centralnego i Kaspersky Endpoint Security. Aby korzystać z uwierzytelniania dwukierunkowego, potrzebujesz również kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform).

Jak połączyć komputer Kaspersky Endpoint Security z Węzłem centralnym przy użyciu Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Detection and Response → Endpoint Detection and Response Expert (on-premises)**.
5. Zaznacz pole **Endpoint Detection and Response Expert (on-premises)**.
6. Kliknij **Ustawienia połączenia z serwerem**.
7. Skonfiguruj połączenie z serwerem:
   - **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera węzła centralnego. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem węzła centralnego.
   - **Certyfikat TLS serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem Central Node. Możesz uzyskać certyfikat TLS w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w Pomoc Kaspersky Anti Targeted Attack Platform).
   - **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem Central Node. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera Central Node, a następnie uzyskać kontener szyfrowania i ustawić hasło chroniące kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform). Po skonfigurowaniu ustawień węzła centralnego należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny.

     Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.
8. Kliknij **OK**.
9. Dodaj serwery węzła centralnego. W tym celu należy określić adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.

   Można dodać wiele adresów serwera węzła centralnego. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.

10. W razie potrzeby skonfiguruj telemetrię.

11. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak połączyć komputer Kaspersky Endpoint Security z węzłem centralnym przy użyciu Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Konfiguracja wbudowanych agentów** → **Endpoint Detection and Response Expert (on-premise)**.

5. Włącz przełącznik **Endpoint Detection and Response Expert (on-premise) WŁĄCZONO**.

6. Aby skonfigurować EDR (KATA), wybierz **Endpoint Detection and Response Expert (wersja 7.1 lub starsze)** z listy rozwiązań.

7. Kliknij **Ustawienia połączenia**.

8. Skonfiguruj połączenie z serwerem:

   - **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera węzła centralnego. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem węzła centralnego.

   - **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem Central Node. Możesz uzyskać certyfikat TLS w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w Pomoc Kaspersky Anti Targeted Attack Platform).

   - **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem Central Node. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera Central Node, a następnie uzyskać kontener szyfrowania i ustawić hasło chroniące kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform). Po skonfigurowaniu ustawień węzła centralnego należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny.

     Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.

9. Kliknij **OK**.

10. Dodaj serwery węzła centralnego. W tym celu należy określić adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.

    Można dodać wiele adresów serwera węzła centralnego. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.

11. W razie potrzeby skonfiguruj telemetrię.

12. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

W rezultacie komputer zostanie dodany do konsoli Kaspersky Anti Targeted Attack Platform. Sprawdź stan działania komponentu, przeglądając *Raport o stanie składników aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Endpoint Detection and Response Expert (on-premises)** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

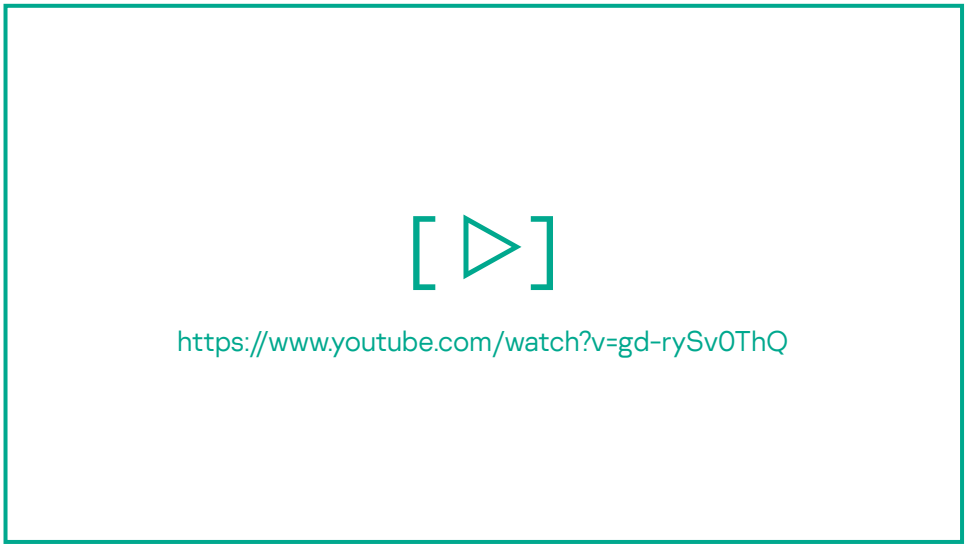
Integracja EDR Agent z NDR (KATA)

EDR Agent instalowany jest na stacjach roboczych i serwerach w infrastrukturze informatycznej organizacji. Na tych komputerach EDR Agent stale monitoruje procesy, otwarte połączenia sieciowe i modyfikowane pliki oraz wysyła dane monitorujące do serwera za pomocą komponentu Central Node.

Aby zintegrować się z NDR (KATA), należy dodać komponent Network Detection and Response (KATA) oraz skonfigurować EDR Agent.

W celu zapewnienia działania Network Detection and Response (KATA) muszą być spełnione następujące warunki:

- Kaspersky Anti Targeted Attack Platform w wersji 7.0 lub nowszej.
- Kaspersky Security Center w wersji 14.2 lub nowszej. We wcześniejszych wersjach Kaspersky Security Center nie ma możliwości aktywowania funkcji Network Detection and Response (KATA).



https://www.youtube.com/watch?v=gd-rySv0ThQ

Integracja z Network Detection and Response (KATA) obejmuje następujące etapy:

1. **Aktywowanie Network Detection and Response (KATA)**

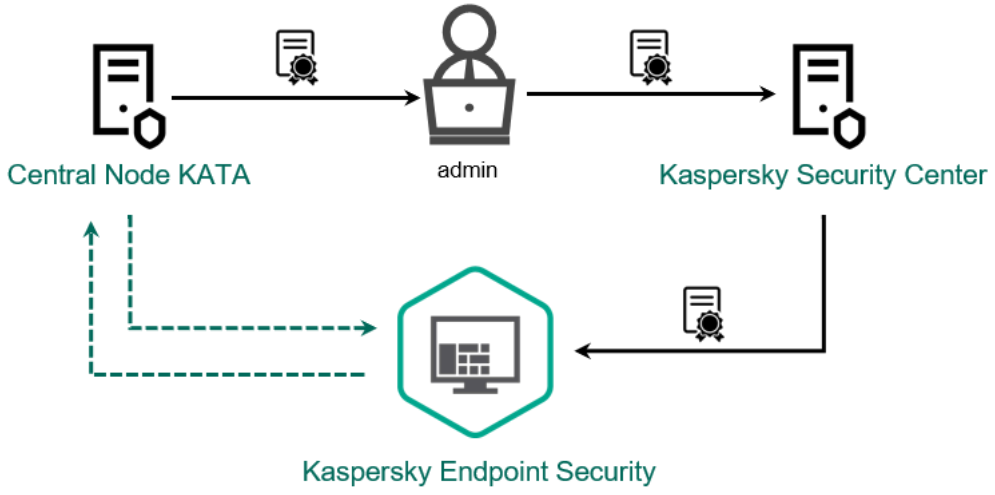
   Musisz zakupić osobną licencję dla korzystania z NDR (KATA) (dodatek Kaspersky Network Detection and Response (KATA)).

   Funkcja będzie dostępna po dodaniu oddzielnego klucza dla Kaspersky Network Detection and Response (KATA). Zasady udzielania licencji dla autonomicznej funkcjonalności Network Detection and Response (KATA) są takie same jak w przypadku udzielania licencji dla Kaspersky Endpoint Security.

   Upewnij się, że funkcja NDR (KATA) znajduje się w licencji i jest uruchomiona w lokalnym interfejsie aplikacji.

2. **Łączenie z węzłem centralnym**

Kaspersky Anti Targeted Attack Platform wymaga ustanowienia zaufanego połączenia między Kaspersky Endpoint Security a komponentem Central Node. Aby skonfigurować zaufane połączenie, musisz użyć certyfikatu TLS. Możesz uzyskać certyfikat TLS w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w Pomoc Kaspersky Anti Targeted Attack Platform). Następnie musisz dodać certyfikat TLS do Kaspersky Endpoint Security (zobacz instrukcje poniżej).



Dodanie certyfikatu TLS do Kaspersky Endpoint Security

Domyślnie Kaspersky Endpoint Security sprawdza tylko certyfikat TLS węzła centralnego. Aby połączenie było bezpieczniejsze, możesz dodatkowo włączyć weryfikację komputera na Węźle Centralnym (uwierzytelnianie dwukierunkowe). Aby włączyć tę weryfikację, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach węzła centralnego i Kaspersky Endpoint Security. Aby korzystać z uwierzytelniania dwukierunkowego, potrzebujesz również kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform).

Jak połączyć komputer Kaspersky Endpoint Security z Węzłem centralnym przy użyciu Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Detection and Response → Network Detection and Response (KATA)**.
4. Zaznacz pole **Network Detection and Response (KATA)**.
5. Kliknij **Ustawienia połączenia**.
6. Skonfiguruj połączenie z serwerem:
   - **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera węzła centralnego. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem węzła centralnego.
   - **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem Central Node. Możesz uzyskać certyfikat TLS w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w Pomoc Kaspersky Anti Targeted Attack Platform).

- **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem Central Node. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera Central Node, a następnie uzyskać kontener szyfrowania i ustawić hasło chroniące kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform). Po skonfigurowaniu ustawień węzła centralnego należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny.

  Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.

7. Kliknij **OK**.
8. Dodaj serwery węzła centralnego. W tym celu należy określić adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.
9. Można dodać wiele adresów serwera węzła centralnego. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.
10. W razie potrzeby skonfiguruj telemetrię.
11. Zapisz swoje zmiany.

Jak połączyć komputer Kaspersky Endpoint Security z węzłem centralnym przy użyciu Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów → Network Detection and Response (KATA)**.
5. Włącz przełącznik **Network Detection and Response (KATA) WŁĄCZONE**.
6. Kliknij **Ustawienia połączenia**.
7. Skonfiguruj połączenie z serwerem:

   - **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera węzła centralnego. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem węzła centralnego.
   - **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem Central Node. Możesz uzyskać certyfikat TLS w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w Pomoc Kaspersky Anti Targeted Attack Platform).

- **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem Central Node. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera Central Node, a następnie uzyskać kontener szyfrowania i ustawić hasło chroniące kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform). Po skonfigurowaniu ustawień węzła centralnego należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny.

  Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.

8. Kliknij **OK**.
9. Dodaj serwery węzła centralnego. W tym celu należy określić adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.
10. Można dodać wiele adresów serwera węzła centralnego. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.
11. W razie potrzeby skonfiguruj telemetrię.
12. Zapisz swoje zmiany.

W rezultacie komputer zostanie dodany do konsoli Kaspersky Anti Targeted Attack Platform. Sprawdź stan działania komponentu, przeglądając *Raport o stanie składników aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Network Detection and Response (KATA)** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

Integracja agenta EDR z EDR Expert (on-premises)

EDR Agent instalowany jest na stacjach roboczych i serwerach w infrastrukturze informatycznej organizacji. Na tych komputerach EDR Agent stale monitoruje procesy, otwarte połączenia sieciowe i modyfikowane pliki oraz wysyła dane monitorujące do serwera EDR Expert (on-premises).

Aby zintegrować się z EDR Expert (on-premises), należy dodać komponent Endpoint Detection and Response Expert (on-premises) oraz skonfigurować EDR Agent.

Integracja z Endpoint Detection and Response Expert (on-premises) obejmuje następujące etapy:

1. **Aktywowanie Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Należy zakupić osobną licencję w celu korzystania z EDR Expert (on-premises) (dodatek Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Funkcja będzie dostępna po dodaniu oddzielnego klucza dla Kaspersky Endpoint Detection and Response Expert (on-premises). Licencjonowanie dla autonomicznej funkcjonalności Endpoint Detection and Response Expert (on-premises) jest takie samo jak w przypadku licencjonowania Kaspersky Endpoint Security.

   Upewnij się, że funkcja EDR Expert (on-premises) znajduje się w licencji i jest uruchomiona w lokalnym interfejsie aplikacji.

2. **Nawiązywanie połączenia z serwerem gromadzącym dane telemetryczne i serwerem odpowiedzi**

Kaspersky Endpoint Detection and Response Expert (on-premises) wymaga zaufanego połączenia między rozwiązaniem Kaspersky Endpoint Security a dwoma serwerami:

- *Serwer gromadzenia danych telemetrycznych* jest serwerem stanowiącym część rozwiązania SIEM, które zbiera, normalizuje, koreluje, analizuje i przechowuje informacje o zdarzeniach mających miejsce na komputerze.

- *Serwer odpowiedzi* jest serwerem służącym do odbierania i skanowania danych, badania zachowań obiektów i publikowania wyników tych badań.

Aby skonfigurować zaufane połączenie, musisz użyć certyfikatu TLS. Certyfikat TLS można uzyskać na platformie Open Single Management Platform (instrukcje można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)). Następnie musisz dodać certyfikat TLS do Kaspersky Endpoint Security (zobacz instrukcje poniżej).

Domyślnie Kaspersky Endpoint Security sprawdza tylko certyfikat TLS serwerów. Aby połączenie było bezpieczniejsze, możesz dodatkowo włączyć weryfikację komputera na serwerze (uwierzytelnianie dwukierunkowe). Aby włączyć tę weryfikację, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera i Kaspersky Endpoint Security. Aby korzystać z uwierzytelniania dwukierunkowego, potrzebujesz również kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać na platformie Open Single Management Platform (instrukcje znajdują się w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)).

Jak połączyć komputer Kaspersky Endpoint Security z platformą EDR Expert (on-premises) przy użyciu Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Konfiguracja wbudowanych agentów → Endpoint Detection and Response Expert (on-premise)**.

5. Włącz przełącznik **Endpoint Detection and Response Expert (on-premise) WŁĄCZONO**.

6. Aby skonfigurować EDR Expert (on-premises), wybierz **Endpoint Detection and Response Expert (wersja 8.0 lub nowsze)** z listy rozwiązań.

7. Skonfiguruj połączenie z *serwerami gromadzącymi dane telemetryczne*:

   a. W sekcji **Połączenie z serwerami gromadzenia danych telemetrycznych** kliknij odnośnik **Ustawienia połączenia**.

   b. Skonfiguruj połączenie z serwerami gromadzącymi dane telemetryczne:

   - **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem.

   - **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem. Certyfikat TLS można uzyskać na platformie Open Single Management Platform (instrukcje można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera, a następnie uzyskać kontener kryptograficzny i ustawić hasło chroniące kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać na platformie Open Single Management Platform (instrukcje znajdują się w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)). Po skonfigurowaniu ustawień serwera należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener szyfrowania.

  Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.

c. Kliknij **OK**.

d. Dodaj serwery gromadzące dane telemetryczne. W tym celu należy określić adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.

Można dodać wiele adresów serwerów gromadzących dane telemetryczne. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.

e. W razie potrzeby skonfiguruj telemetrię.

8. Skonfiguruj połączenie z *serwerami odpowiedzi*:

a. W sekcji **Połączenie z serwerami odpowiedzi** skonfiguruj połączenie **Wysyłaj żądanie synchronizacji do serwera co (min)**. Częstotliwość żądań synchronizacji wysyłanych do serwera. Podczas synchronizacji program Kaspersky Endpoint Security odbiera zadania reagowania na zagrożenia i wysyła wyniki zadań.

b. Kliknij odnośnik **Ustawienia połączenia**.

c. Skonfiguruj połączenie z serwerami odpowiedzi:

- **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem.

- **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem. Certyfikat TLS można uzyskać na platformie Open Single Management Platform (instrukcje można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera, a następnie uzyskać kontener kryptograficzny i ustawić hasło chroniące kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać na platformie Open Single Management Platform (instrukcje znajdują się w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)). Po skonfigurowaniu ustawień serwera należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener szyfrowania.

  Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.

d. Kliknij **OK**.

e. Dodaj serwery odpowiedzi. W tym celu należy określić adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.

Można dodać wiele adresów serwerów odpowiedzi. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.

9. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

W rezultacie komputer zostaje dodany do Open Single Management Platform (OSMP). Sprawdź stan działania komponentu, przeglądając *Raport o stanie składników aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Endpoint Detection and Response Expert (on-premises)** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

Kompatybilność z aplikacjami EPP innych firm

EDR Agent obsługuje funkcjonalność rozwiązań Detection and Response firmy Kaspersky. Komponenty ochrony i kontroli nie są dostępne dla EDR Agent. Ta konfiguracja umożliwia instalowanie aplikacji EPP innych firm i wdrażanie rozwiązań Kaspersky Detection and Response w infrastrukturze organizacji. EDR Agent obsługuje pracę z Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack Platform (EDR) i Kaspersky Anti Targeted Attack Platform (NDR).

EDR Agent jest kompatybilny z aplikacjami EPP następujących dostawców:

- **Dr.Web**

  EDR Agent jest kompatybilny z Dr.Web Agent dla systemu Windows w wersji 13.0.1 lub nowszej i Dr.Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  EDR Agent jest kompatybilny z Dallas Lock 8.0-C wersja 11.4.2.843 lub nowsza.

  Aby umożliwić działanie EDR Agent na komputerze z zainstalowanym oprogramowaniem Dallas Lock, należy zezwolić na połączenie z zewnętrznymi usługami Kaspersky w ustawieniach modułu Zapora sieciowa.

- **Secret Net Studio**

  EDR Agent jest kompatybilny z Secret Net Studio w wersji 8.11 lub nowszej.

Aplikacja nie może zostać zainstalowana na komputerze, na którym jest wdrożony program Secret Net Studio z komponentem Antivirus. Aby umożliwić interoperacyjność, musisz usunąć komponent Antivirus z Secret Net Studio.

- **Trend Micro**

  EDR Agent jest kompatybilny z Trend Micro Apex One wersja 14.0.12994 lub nowszą wersją (w tym Security Agent).

  EDR Agent jest kompatybilny z Trend Micro Deep Security w wersji 20.0.2-4960 lub nowszej (w tym Security Agent).

- **Windows Defender**

- **Sophos**

  EDR Agent jest kompatybilny z Sophos Intercept X w wersji 2024.1.2 lub nowszej (w tym Endpoint Agent) i Sophos Core Agent w wersji 2024.3.2.3.

- **Bitdefender**

  EDR Agent jest kompatybilny z Bitdefender Endpoint Security Tools wersja 7.9.21.523 lub nowsza.

- **ESET**

  EDR Agent jest kompatybilny z ESET Endpoint Security w wersji 12.0.2049.0 lub nowszej i ESET Management Agent w wersji 12.0 lub nowszej.

Na komputerach z systemem Windows 11 dla architektury Arm64 agent EDR Agent nie jest zgodny z Bitdefender Endpoint Security Tools.

Aplikacje należy zainstalować w następującej kolejności: najpierw zainstaluj aplikację EPP, następnie Agenta sieciowego Kaspersky Security Center, a następnie EDR Agent. Jest to konieczne, ponieważ instalator aplikacji EPP może wykryć EDR Agent i Agenta sieciowego jako oprogramowanie niekompatybilne i je usunąć. Działanie EDR Agent i Agenta sieciowego należy sprawdzić także po aktualizacji aplikacji EPP innej firmy, ponieważ jej instalator może ponownie przeskanować komputer w poszukiwaniu niekompatybilnego oprogramowania i usunąć aplikacje.

Jeśli nie mogłeś zainstalować EDR Agent na komputerze z aplikacją EPP innej firmy, ponieważ instalator znalazł na komputerze niekompatybilne oprogramowanie, możesz pomiń sprawdzanie niezgodnego oprogramowania.

Managed Detection and Response



Kaspersky Endpoint Security for Windows obsługuje integrację z rozwiązaniem Managed Detection and Response. Rozwiązanie *Kaspersky Managed Detection and Response (MDR)* automatycznie wykrywa i analizuje incydenty naruszenia bezpieczeństwa w Twojej infrastrukturze. W tym celu MDR używa danych telemetrycznych, otrzymanych z punktów końcowych i uczenia maszynowego. MDR wysyła dane incydentu do ekspertów z Kaspersky. Eksperci mogą następnie przetworzyć incydent i, na przykład, dodać nowy wpis do antywirusowych baz danych. Zamiast tego eksperci mogą opublikować zalecenia odnośnie przetwarzania incydentu i, na przykład, zasugerować odizolowanie komputera od sieci. Szczegółowe informacje dotyczące sposobu działania rozwiązania można znaleźć w pomocy do Kaspersky Managed Detection and Response.

Konfiguracje Kaspersky Endpoint Security do integracji z MDR

Do pracy z MDR można stosować następujące konfiguracje:

- **[KES+wbudowany agent]**. W tej konfiguracji Kaspersky Endpoint Security działa zarówno jako aplikacja zapewniająca bezpieczeństwo komputera, jak i aplikacja do pracy z MDR. Wbudowany agent jest dostępny w Kaspersky Endpoint Security 11.6.0 for Windows lub nowszym.

- **[zewnętrzny agent EPP+EDR]**. W tej konfiguracji bezpieczeństwo infrastruktury IT zapewnia zewnętrzna platforma Endpoint Protection Platform (EPP). Interakcja z MDR jest zapewniana przez Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent (EDR Agent). W tej konfiguracji EDR Agent jest kompatybilny z aplikacjami EPP innych firm. EDR Agent jest dostępny w Kaspersky Endpoint Security 12.3 for Windows lub nowszym.

Obsługa poprzednich wersji Kaspersky Endpoint Security

Kaspersky Endpoint Security w wersji 11 i nowszej obsługuje rozwiązanie MDR. Kaspersky Endpoint Security w wersjach 11 – 11.5.0 tylko wysyła dane telemetryczne Kaspersky Managed Detection and Response, aby włączyć wykrywanie zagrożeń. Kaspersky Endpoint Security w wersji 11.6.0 posiada pełną funkcjonalność agenta wbudowanego (Kaspersky Endpoint Agent).

Jeśli korzystasz z Kaspersky Endpoint Security 11 – 11.5.0, musisz zaktualizować bazy danych do najnowszej wersji w celu pracy z rozwiązaniem MDR. Musisz także zainstalować Kaspersky Endpoint Agent.

Jeśli korzystasz z Kaspersky Endpoint Security w wersji 11.6.0 lub nowszej, nie musisz instalować Kaspersky Endpoint Agent, aby używać rozwiązania MDR.

> Jeśli zasada Kaspersky Endpoint Security także jest stosowana także do komputerów, na których nie jest zainstalowany program Kaspersky Endpoint Security 11 – 11.5.0, w pierwszej kolejności musisz utworzyć oddzielną zasadę Kaspersky Endpoint Agent dla tych komputerów. W nowej zasadzie skonfiguruj integrację z Kaspersky Managed Detection and Response.

Integracja wbudowanego agenta z MDR

Aby skonfigurować integrację z Kaspersky Managed Detection and Response, musisz włączyć komponent Managed Detection and Response i skonfigurować Kaspersky Endpoint Security.

Aby rozwiązanie Kaspersky Managed Detection and Response działało z Serwerem administracyjnym poprzez Kaspersky Security Center Web Console, należy nawiązać nowe bezpieczne połączenie – *połączenie w tle*. Kaspersky Managed Detection and Response wyświetla pytanie o nawiązanie połączenia w tle po wdrożeniu rozwiązania. Upewnij się, że połączenie w tle zostało nawiązane.

Nawiązywanie połączenia w tle w Web Console

1. W oknie głównym Web Console wybierz **Ustawienia** → **Integracja**.

2. Przejdź do sekcji **Integracja**.

3. Włącz przełącznik **Połączenie w tle w celu integracji Włączone**.

4. Zapisz swoje zmiany.

Integracja z Kaspersky Managed Detection and Response obejmuje następujące kroki:

1. **Instalacja komponentu Managed Detection and Response**

   Możesz wybrać składnik MDR podczas instalacji lub aktualizacji, a także przy użyciu zadania *Zmiana składników aplikacji*.

   > Aby zainstalować składnik Managed Detection and Response bez ponownego uruchamiania komputera przy użyciu zadania *Zmiana składników aplikacji*, należy wyłączyć opcję **Usuń niekompatybilne aplikacje innych firm** w ustawieniach zadania.

2. **Konfiguracja Kaspersky Private Security Network**

   > Pomiń ten krok, jeśli używasz Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console automatycznie konfiguruje lokalną sieć Kaspersky Private Security Network podczas instalowania wtyczki MDR.

   Kaspersky Private Security Network (KPSN) to rozwiązanie, które umożliwia użytkownikom komputerów z zainstalowanym programem Kaspersky Endpoint Security lub innymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów.

   Wczytaj plik konfiguracyjny Kaspersky Security Network we właściwościach Serwera administracyjnego. Plik konfiguracyjny Kaspersky Security Network znajduje się w archiwum ZIP pliku konfiguracyjnego MDR. Archiwum ZIP możesz uzyskać w Kaspersky Managed Detection and Response Console. Więcej informacji na temat konfigurowania prywatnej sieci Kaspersky Private Security Network można znaleźć w pomocy dla Kaspersky Security Center. Plik konfiguracyjny Kaspersky Security Network możesz wczytać także z poziomu wiersza polecenia (zapoznaj się z poniższymi instrukcjami).

   Jak skonfigurować prywatną sieć Kaspersky Private Security Network z poziomu wiersza polecenia?

   1. Uruchom wiersz poleceń (cmd.exe) jako administrator.

   2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

   3. Uruchom następujące polecenie:

      ```
      avp.com KSN /private <file name>
      ```

      gdzie `<file name>` to nazwa pliku konfiguracyjnego zawierającego ustawienia sieci Kaspersky Private Security Network (format pliku PKCS7 lub PEM).

      Na przykład:
      ```
      avp.com KSN /private C:\kpsn_config.pkcs7
      ```

   W rezultacie Kaspersky Endpoint Security użyje Kaspersky Private Security Network do określenia reputacji plików, aplikacji i stron internetowych. W sekcji ustawień zasady **Kaspersky Security Network** zostanie wyświetlony następujący stan operacyjny: *Infrastruktura: Kaspersky Private Security Network*.

   > Musisz włączyć rozszerzony tryb KSN dla Managed Detection and Response, aby działało.

3 Aktywowanie Kaspersky Managed Detection and Response

Począwszy od wersji 12.10 Kaspersky Endpoint Security for Windows, aby aktywować funkcję Managed Detection and Response, jako alternatywę dla kodu aktywacyjnego możesz również użyć pliku kluczowego.

Rozwiązanie Kaspersky Managed Detection and Response obsługuje następujące metody licencjonowania:

- Funkcjonalność Managed Detection and Response jest dostępna w licencji dla Kaspersky Endpoint Security for Windows.

  Funkcja będzie dostępna natychmiast po aktywacji Kaspersky Endpoint Security for Windows.

- MDR (dodatek Kaspersky Managed Detection and Response) używa osobnej licencji.

  Funkcja będzie dostępna po dodaniu oddzielnego klucza dla dodatku Kaspersky Managed Detection and Response. W rezultacie na komputerze zostają dodane dwa klucze: klucz dla Kaspersky Endpoint Security i klucz dla Kaspersky Managed Detection and Response.

  Licencjonowanie dla autonomicznej funkcjonalności Managed Detection and Response jest takie samo, jak w przypadku licencjonowania Kaspersky Endpoint Security.

Upewnij się, że funkcja MDR jest w licencji i jest uruchomiona w lokalnym interfejsie aplikacji.

4 Włączanie komponentu Managed Detection and Response

Załaduj plik konfiguracyjny BLOB w zasadzie Kaspersky Endpoint Security (zapoznaj się z poniższymi instrukcjami). Plik BLOB zawiera ID klienta oraz informacje o licencji dla Kaspersky Managed Detection and Response. Plik BLOB znajduje się w archiwum ZIP pliku konfiguracyjnego MDR. Archiwum ZIP możesz uzyskać w Kaspersky Managed Detection and Response Console. Więcej informacji o pliku BLOB można znaleźć w pomocy dla Kaspersky Managed Detection and Response.

Począwszy od Kaspersky Endpoint Security 12.6 for Windows, dodanie pliku BLOB jest opcjonalne dla Kaspersky Managed Detection and Response bez dzierżawców, jeśli posiadasz aktualną licencję.

Jak włączyć komponent Managed Detection and Response w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.
4. Zaznacz pole **Managed Detection and Response (Industrial CyberSecurity)**.
5. W sekcji **Ustawienia** kliknij **Przekaż** i wybierz plik BLOB pobrany w Kaspersky Managed Detection and Response Console. Plik posiada rozszerzenie P7.

   Domyślnie użytkownik może zarządzać ustawieniami aplikacji (kłódka jest otwarta ). Aby zastosować zasady na komputerach, zamknij kłódki  .

6. Zapisz swoje zmiany.

Jak włączyć komponent Managed Detection and Response w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Managed Detection and Response**.
5. Włącz przełącznik **Managed Detection and Response WŁĄCZONO**.
6. Kliknij **Wczytaj** i wybierz plik BLOB, który został uzyskany w Kaspersky Managed Detection and Response Console. Plik posiada rozszerzenie P7.

   Domyślnie użytkownik ma możliwość zarządzania ustawieniami zasad (kłódka jest otwarta). Aby zastosować zasady na komputerach, zamknij kłódki.
7. Zapisz swoje zmiany.

Jak włączyć komponent Managed Detection and Response z poziomu wiersza polecenia?

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   Aby wykonać to polecenie, Ochrona hasłem musi być włączona. Użytkownik musi mieć uprawnienie **Konfiguracja ustawień aplikacji**.

W wyniku tego program Kaspersky Endpoint Security będzie sprawdzał plik BLOB. Weryfikacja pliku BLOB obejmuje sprawdzanie podpisu cyfrowego i okresu licencjonowania. Jeśli plik BLOB został pomyślnie zweryfikowany, Kaspersky Endpoint Security pobierze plik i wyśle go do komputera podczas kolejnej synchronizacji z Kaspersky Security Center. Sprawdź stan działania komponentu, przeglądając *Raport o stanie składników aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Managed Detection and Response** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

5. **Konfigurowanie innych komponentów aplikacji w celu odbierania danych telemetrycznych**

   Musisz włączyć następujące komponenty dla Managed Detection and Response w celu zapewnienia działania:

   - Kaspersky Security Network (tryb rozszerzony).
   - Wykrywanie zachowań.
   - Ochrona przed exploitami.
   - Ochrona WWW.

- Ochrona poczty.
- Ochrona plików.
- Ochrona sieci
- Zapora sieciowa.
- Ochrona AMSI.
- Skanowanie w tle.

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Managed Detection and Response**.
5. Włącz przełącznik **Managed Detection and Response WŁĄCZONO**.
6. Zapisz swoje zmiany.

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Zaznacz pole **Managed Detection and Response (Industrial CyberSecurity)**.
5. Zapisz swoje zmiany.

Przewodnik migracji z KEA do KES dla MDR

Kaspersky Endpoint Security for Windows zawiera wbudowanego agenta dla rozwiązania Managed Detection and Response. Nie potrzebujesz już oddzielnej aplikacji Kaspersky Endpoint Agent do pracy z MDR. Wszystkie funkcje Kaspersky Endpoint Agent będą wykonywane przez Kaspersky Endpoint Security.

Podczas wdrażania Kaspersky Endpoint Security na komputerach, na których jest zainstalowany Kaspersky Endpoint Agent, rozwiązanie Kaspersky Managed Detection and Response będzie nadal działać z Kaspersky Endpoint Security. Dodatkowo, Kaspersky Endpoint Agent zostanie usunięty z komputera. To samo zachowanie w systemie wystąpi podczas aktualizacji Kaspersky Endpoint Security do wersji 11.6.0 lub nowszej.

Kaspersky Endpoint Security nie jest kompatybilny z Kaspersky Endpoint Agent. Obu tych aplikacji nie można zainstalować na tym samym komputerze.

Aby aplikacja Kaspersky Endpoint Security działała w ramach Kaspersky Managed Detection and Response, muszą być spełnione następujące warunki:

- Kaspersky Security Center w wersji 13.2 lub nowszej (w tym Agent sieciowy). We wcześniejszych wersjach Kaspersky Security Center nie ma możliwości aktywowania funkcji Managed Detection and Response.
- Połączenia w tle między Kaspersky Security Center Web Console a Serwerem administracyjnym zostało nawiązane. Aby rozwiązanie MDR działało z Serwerem administracyjnym poprzez Kaspersky Security Center Web Console, należy nawiązać nowe bezpieczne połączenie – *połączenie w tle*.

Kroki migracji konfiguracji [KES+KEA] do [KES+wbudowanego agenta] dla MDR

1. **Aktualizowanie wtyczki zarządzającej Kaspersky Endpoint Security**

   Komponentem MDR można zarządzać przy użyciu wtyczki zarządzającej Kaspersky Endpoint Security w wersji 11.6 lub nowszej. W zależności od typu konsoli Kaspersky Security Center, której używasz, zaktualizuj wtyczkę zarządzającą w Konsoli administracyjnej (MMC) lub wtyczkę webową w Web Console.

2. **Migrowanie zasad i zadań**

   Przenieś ustawienia Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows. Dostępne są następujące opcje:

   - Kreator migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security. Kreator migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security działa tylko w usłudze Web Console.

     Jak dokonać migracji ustawień zasady i zadania z Kaspersky Endpoint Agent do Kaspersky Endpoint Security w Web Console:

     W oknie głównym Web Console wybierz **Operacje** → **Migracja z Kaspersky Endpoint Agent**.

     To spowoduje uruchomienie Kreatora migracji zasad i zadań. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Migracja zasady

Kreator migracji tworzy nową zasadę, która scala ustawienia zasad Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Na liście zasad wybierz zasady Kaspersky Endpoint Agent, których ustawienia chcesz scalić z zasadą Kaspersky Endpoint Security. Kliknij zasadę Kaspersky Endpoint Agent, aby wybrać zasadę Kaspersky Endpoint Security, z którą chcesz scalić ustawienia. Upewnij się, że wybrałeś poprawne zasady i przejdź do następnego kroku.

Krok 2. Migracja zadania

Kreator migracji nie obsługuje zadań MDR. Pomiń ten krok.

Krok 3. Kończenie działania kreatora

Zakończ działanie Kreatora. W wyniku działania kreatora zostanie utworzona nowa zasada Kaspersky Endpoint Security. Zasada scala ustawienia z Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Zasada zostaje nazwana *<Nazwa zasady Kaspersky Endpoint Security> & <Nazwa zasady Kaspersky Endpoint Agent>*. Nowa zasada posiada stan *Nieaktywny*. Aby kontynuować, zmień stany zasad Kaspersky Endpoint Agent i Kaspersky Endpoint Security na *Nieaktywny* i aktywuj nową scaloną zasadę.

- Standardowy kreator konwersji zasad i zadań. Kreator konwersji zasad i zadań jest dostępny tylko w Konsoli administracyjnej (MMC). Więcej informacji o kreatorze konwersji zasad i zadań można znaleźć w pomocy Kaspersky Security Center.

3. **Udzielanie licencji funkcjonalności MDR**

Aby aktywować Kaspersky Endpoint Security jako część rozwiązania Kaspersky Managed Detection and Response, potrzebujesz osobnej licencji na dodatek Kaspersky Managed Detection and Response. Możesz dodać klucz przy użyciu zadania *Dodaj klucz*. W rezultacie do aplikacji zostaną dodane dwa klucze: *Kaspersky Endpoint Security* i *Kaspersky Managed Detection and Response*.

4. **Instalacja / aktualizacja aplikacji Kaspersky Endpoint Security**

Aby przeprowadzić migrację funkcjonalności MDR podczas instalacji lub aktualizacji aplikacji, zaleca się użycie zadania zdalnej instalacji. Podczas tworzenia zadania zdalnej instalacji należy wybrać komponent MDR w ustawieniach pakietu instalacyjnego.

Możesz także zaktualizować aplikację za pomocą następujących metod:

- Przy użyciu usługi aktualizacji Kaspersky.
- Lokalnie, za pomocą Kreatora instalacji.

Kaspersky Endpoint Security obsługuje automatyczne wybieranie komponentów podczas aktualizacji aplikacji na komputerze z zainstalowaną aplikacją Kaspersky Endpoint Agent. Automatyczne wybieranie komponentów zależy od uprawnień konta użytkownika, które aktualizuje aplikację.

Jeśli aktualizujesz Kaspersky Endpoint Security przy użyciu pliku EXE lub MSI z poziomu konta systemowego (SYSTEM), Kaspersky Endpoint Security uzyskuje dostęp do bieżących licencji rozwiązań firmy Kaspersky. Dlatego też, jeśli na komputerze jest zainstalowany Kaspersky Endpoint Agent i aktywowane rozwiązanie MDR, instalator Kaspersky Endpoint Security automatycznie konfiguruje zestaw komponentów i wybiera komponent MDR. To powoduje przełączenie Kaspersky Endpoint Security na używanie wbudowanego agenta i usunięcie Kaspersky Endpoint Agent. Uruchomienie instalatora MSI z poziomu konta systemowego (SYSTEM) jest zazwyczaj wykonywane podczas aktualizacji za pośrednictwem usługi aktualizacji Kaspersky lub podczas wdrażania pakietu instalacyjnego za pośrednictwem Kaspersky Security Center.

Jeśli aktualizujesz Kaspersky Endpoint Security przy użyciu pliku MSI z poziomu konta użytkownika bez uprawnień, Kaspersky Endpoint Security nie ma dostępu do bieżących licencji dla rozwiązań Kaspersky. W takim przypadku Kaspersky Endpoint Security automatycznie wybiera komponenty na podstawie zestawu komponentów Kaspersky Endpoint Agent. Następnie Kaspersky Endpoint Security przełączy się na korzystanie z wbudowanego agenta i usunie Kaspersky Endpoint Agent.

Kaspersky Endpoint Security obsługuje aktualizację bez ponownego uruchamiania komputera. Możesz wybrać tryb aktualizacji aplikacji we właściwościach zasad.

5. **Sprawdzanie działania aplikacji**

Jeśli po instalacji lub aktualizacji aplikacji komputer posiada stan *Krytyczny* w konsoli Kaspersky Security Center:

- Upewnij się, że na komputerze jest zainstalowany Agent sieciowy w wersji 13.2 lub wyższej.
- Sprawdź stan działania komponentów, przeglądając *Raport o stanie składników aplikacji*. Jeśli komponent ma stan *Nie zainstalowano*, zainstaluj komponent przy użyciu zadania *Zmiana składników aplikacji*. Jeśli komponent ma stan *Nieobjęte licencją*, upewnij się, że aktywowano wbudowaną funkcję agenta.
- Upewnij się, że akceptujesz Oświadczenie Kaspersky Security Network w nowej zasadzie Kaspersky Endpoint Security for Windows.

Endpoint Detection and Response



Kaspersky Endpoint Security for Windows zawiera wbudowanego agenta dla rozwiązania Kaspersky Endpoint Detection and Response Optimum (zwanego dalej również „EDR Optimum"). Począwszy od wersji 11.8.0 Kaspersky Endpoint Security for Windows zawiera wbudowanego agenta dla rozwiązania Kaspersky Endpoint Detection and Response Expert (zwanego dalej również „EDR Expert"). *Kaspersky Endpoint Detection and Response* to szereg rozwiązań do ochrony infrastruktury IT korporacji przed zaawansowanymi cyberzagrożeniami. Funkcjonalność rozwiązań łączy automatyczne wykrywanie zagrożeń z możliwością reagowania na te zagrożenia w celu przeciwdziałania zaawansowanym atakom, w tym nowym exploitom, oprogramowaniu ransomware, atakom bezplikowym, a także metodom z użyciem legalnych narzędzi systemowych. EDR Expert oferuje więcej funkcji monitorowania zagrożeń i reakcji na nie niż EDR Optimum. Więcej informacji o rozwiązaniach można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Optimum oraz w pomocy do Kaspersky Endpoint Detection and Response Expert.

Narzędzia analizy zagrożeń

Kaspersky Endpoint Detection and Response używa następujących narzędzi Threat Intelligence:

- Integracja z portalem Kaspersky Threat Intelligence Portal, który zawiera i wyświetla informacje o reputacji plików i adresów sieciowych.
- Baza danych Kaspersky Threats.
- Infrastruktura usługi chmury Kaspersky Security Network (zwana dalej również „KSN"), która zapewnia dostęp do informacji o reputacji pliku, strony internetowej i oprogramowania w czasie rzeczywistym z bazy wiedzy Kaspersky. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji firmy Kaspersky na zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie prawdopodobieństwa wystąpienia fałszywych alarmów.
- Technologia Cloud Sandbox, która pozwala uruchamiać wykryte pliki w izolowanym środowisku i sprawdzać ich reputację.

Zasada działania rozwiązania

Kaspersky Endpoint Detection and Response monitoruje i analizuje rozwój zagrożeń i zapewnia *personel ds. bezpieczeństwa* lub *Administratora* z informacjami o potencjalnym ataku, które są niezbędne do reagowania w odpowiednim momencie. Kaspersky Endpoint Detection and Response wyświetla szczegóły wykrycia w oddzielnym oknie. *Wykrycie* to zdarzenie w korporacyjnej infrastrukturze IT, które aplikacja zidentyfikowała jako nietypowe lub podejrzane i które może stanowić zagrożenie dla bezpieczeństwa korporacyjnej infrastruktury IT. *Szczegóły wykrycia* to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Optimum oraz w pomocy do Kaspersky Endpoint Detection and Response Expert.

Obsługa poprzednich wersji Kaspersky Endpoint Security

Jeśli używasz Kaspersky Endpoint Security 11.2.0–11.6.0 do współdziałania z Kaspersky Endpoint Detection and Response Optimum, aplikacja zawiera Kaspersky Endpoint Agent. Możesz zainstalować Kaspersky Endpoint Agent wraz z Kaspersky Endpoint Security. W programie Kaspersky Endpoint Security 11.9.0 pakiet dystrybucyjny Kaspersky Endpoint Agent nie jest już częścią zestawu dystrybucyjnego Kaspersky Endpoint Security.

Rozwiązanie Kaspersky Endpoint Detection and Response Expert nie obsługuje współdziałania z Kaspersky Endpoint Agent. Rozwiązanie Kaspersky Endpoint Detection and Response Expert używa Kaspersky Endpoint Security z wbudowanym agentem (wersja 11.8.0 i nowsza).

Integracja wbudowanego agenta z EDR Optimum / EDR Expert

Aby skonfigurować integrację z Kaspersky Managed Detection and Response, musisz dodać komponent Endpoint Detection and Response Optimum lub komponent Endpoint Detection and Response Expert (cloud) i skonfigurować Kaspersky Endpoint Security.

Komponenty Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) i Endpoint Detection and Response Expert (on-premises) nie są ze sobą kompatybilne.

W celu zapewnienia działania Endpoint Detection and Response muszą być spełnione następujące warunki:

- Kaspersky Security Center w wersji 13.2 lub nowszej. We wcześniejszych wersjach Kaspersky Security Center nie ma możliwości aktywowania funkcji Endpoint Detection and Response.
- Wtyczka zarządzająca Kaspersky Endpoint Detection and Response.

  Począwszy od Kaspersky Endpoint Security w wersji 12.6 wyświetlanie szczegółów alertów zostało przeniesione z wtyczki zarządzającej Kaspersky Endpoint Security do wtyczki zarządzającej EDR. Wtyczka zarządzająca EDR to pojedyncza wtyczka do pracy z agentami w systemach operacyjnych Windows, Mac i Linux. Teraz, pracując z EDR Optimum, będziesz potrzebować wtyczki zarządzającej Kaspersky Endpoint Security do tworzenia zadań Threat Response oraz wtyczki zarządzającej EDR do przeglądania szczegółów alertów.

- Komponent Endpoint Detection and Response Optimum jako część Kaspersky Endpoint Security obsługuje interakcję z rozwiązaniem Kaspersky Endpoint Detection and Response Optimum 2.0. Interakcja z Kaspersky Endpoint Detection and Response Optimum w wersji 1.0 nie jest obsługiwana.
- EDR Optimum może być zarządzany w Kaspersky Security Center Web Console i Kaspersky Security Center Cloud Console.

  EDR Expert może być zarządzany tylko przy użyciu konsoli Kaspersky Security Center Cloud Console. Nie możesz zarządzać tą funkcjonalnością przy użyciu Konsoli administracyjnej (MMC).
- Aplikacja jest aktywowana, a funkcjonalność jest objęta licencją.
- Komponent Endpoint Detection and Response jest włączony.
- Składniki aplikacji, od których zależy Endpoint Detection and Response, są włączone i działają. Endpoint Detection and Response zależy od następujących komponentów:
  - Ochrona plików.
  - Ochrona WWW.
  - Ochrona poczty.
  - Ochrona przed exploitami.
  - Wykrywanie zachowań.
  - Ochrona przed włamaniami.
  - Silnik korygujący.
  - Adaptacyjna kontrola anomalii.

Integracja z Kaspersky Endpoint Detection and Response obejmuje następujące etapy:

1. **Instalowanie komponentów Endpoint Detection and Response**

   Możesz wybrać komponent Endpoint Detection and Response Optimum lub komponent Endpoint Detection and Response Expert (cloud) podczas instalacji lub aktualizacji, a także w przypadku korzystania z zadania *Zmiana składników aplikacji*.

   > Musisz ponownie uruchomić komputer, aby dokończyć aktualizację aplikacji o nowe komponenty.

2. **Aktywowanie Kaspersky Endpoint Detection and Response**

   Możesz uzyskać licencję do korzystania z Kaspersky Endpoint Detection and Response na następujące sposoby:

   - Funkcjonalność Endpoint Detection and Response znajduje się w licencji dla Kaspersky Endpoint Security for Windows.

     Funkcja będzie dostępna natychmiast po aktywacji Kaspersky Endpoint Security for Windows.

- Zakupienie licencji dla korzystania z EDR Optimum lub EDR Expert (dodatek Kaspersky Endpoint Detection and Response).

  Funkcja będzie dostępna po dodaniu oddzielnego klucza dla Kaspersky Endpoint Detection and Response. W rezultacie na komputerze zostają dodane dwa klucze: klucz dla Kaspersky Endpoint Security i klucz dla Kaspersky Endpoint Detection and Response.

  Licencjonowanie dla autonomicznej funkcjonalności Endpoint Detection and Response jest takie samo jak w przypadku licencjonowania Kaspersky Endpoint Security.

Upewnij się, że funkcja EDR Optimum lub EDR Expert znajduje się w licencji i jest uruchomiona w lokalnym interfejsie aplikacji.

Więcej informacji o umowie licencyjnej EDR Optimum znajdziesz w Kaspersky Endpoint Detection and Response Optimum Help.

3. **Włączanie komponentów Endpoint Detection and Response**

Możesz włączyć lub wyłączyć komponent w ustawieniach zasady Kaspersky Endpoint Security for Windows.

Jak włączyć lub wyłączyć komponent Endpoint Detection and Response w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Endpoint Detection and Response**.
5. Włącz przełącznik **Endpoint Detection and Response WŁĄCZONY**.
6. Zapisz swoje zmiany.

Komponent Kaspersky Endpoint Detection and Response jest włączony. Sprawdź stan działania komponentu, przeglądając *Raport o stanie składników aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Endpoint Detection and Response Optimum** lub **Endpoint Detection and Response Expert (cloud)** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

4. **Włączanie przesyłania danych do Serwera administracyjnego**

W celu włączenia wszystkich funkcji Endpoint Detection and Response, przesyłanie danych powinno być włączone dla następujących typów danych:

- Dane pliku poddanego kwarantannie.

  Dane są wymagane do uzyskania informacji o plikach poddanych kwarantannie na komputerze za pośrednictwem Web Console i Cloud Console. Na przykład, możesz pobrać plik z kwarantanny do analizy w Web Console i Cloud Console.

- Dane łańcucha rozwoju zagrożeń.

  Dane są wymagane do uzyskania informacji o zagrożeniach wykrytych na komputerze w Web Console i Cloud Console. Możesz przejrzeć szczegóły wykrycia i podjąć działanie w Web Console i Cloud Console.

Jak włączyć przesyłanie danych do Serwera administracyjnego w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Integracja KSC**.
5. W sekcji **Przesyłanie danych do Serwera administracyjnego** kliknij odnośnik **Ustawienia zaawansowane**.
6. W otwartym oknie zaznacz następujące pola wyboru:
   - **Informacje o plikach Kwarantanny**.
   - **Informacje o łańcuchu rozprzestrzeniania się zagrożeń**.
7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa (zadanie standardowe)

Wskaźnik naruszeń bezpieczeństwa (IOC) to zestaw danych dotyczących obiektu lub aktywności, która wskazuje nieautoryzowany dostęp do komputera (naruszenie bezpieczeństwa danych). Na przykład, wiele niepomyślnych prób zalogowania do systemu może stanowić wskaźnik naruszeń bezpieczeństwa. Zadanie *Skanowanie IOC* umożliwia odszukanie wskaźników naruszeń bezpieczeństwa na komputerze i podejmują środki reakcji na zagrożenia.

Kaspersky Endpoint Security wyszukuje wskaźniki zagrożenia za pomocą plików IOC. *Pliki IOC* to pliki zawierające zestawy wskaźników, które aplikacja próbuje dopasować do licznika wykrywania. Pliki IOC muszą pasować do standardu OpenIOC.

Tryb uruchamiania zadania Skanowanie IOC

Kaspersky Endpoint Detection and Response umożliwia utworzenie standardowych zadań Skanowanie IOC do wykrywania danych, których bezpieczeństwo zostało naruszone. *Standardowe zadanie skanowania IOC* to zadanie grupowe lub lokalne, które jest tworzone i skonfigurowane ręcznie w konsoli Web Console. Zadania są uruchamiane przy użyciu plików IOC przygotowanych przez użytkownika. Jeśli chcesz ręcznie dodać wskaźnik naruszenia bezpieczeństwa, zapoznaj się z wymaganiami plików IOC.

Plik, który możesz pobrać, klikając poniższy odnośnik, zawiera tabelę z pełną listą warunków IOC standardu OpenIOC.

POBIERZ PLIK IOC_TERMS.XLSX

Kaspersky Endpoint Security także obsługuje autonomiczne zadania skanowania IOC, gdy aplikacja jest używana jako część rozwiązania Kaspersky Sandbox.

Tworzenie pliku IOC

Począwszy od wersji Kaspersky Endpoint Security 12.10 for Windows pliki IOC można tworzyć bezpośrednio w ustawieniach zadania. Aby utworzyć plik IOC, należy przygotować plik TXT zawierający listę wskaźników naruszeń bezpieczeństwa. Można dodać listy następujących obiektów jako wskaźniki naruszeń bezpieczeństwa:

- Skróty plików (MD5 / SHA256).

  Aplikacja przygotowuje plik IOC z zakresem skanowania FileItem/Md5sum lub FileItem/Sha256sum.

- Adresy IP (IPv4, IPv6).

  Aplikacja przygotowuje plik IOC z zakresem skanowania PortItem/RemoteIP.

- Nazwy DNS.

  Aplikacja przygotowuje plik IOC z zakresem skanowania DnsEntryItem/RecordName.

Jak utworzyć plik IOC w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zadania**.

   Zostanie otwarta lista zadań.

2. Wybierz zadanie **Skanowanie IOC**.

   Zostanie otwarte okno właściwości zadania. W razie konieczności utwórz zadanie **Skanowanie IOC**.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Przejdź do sekcji **Skanowanie zagrożeń**.

5. Kliknij **Ponownie zdefiniuj pliki IOC**.

6. Otwiera się formularz umożliwiający utworzenie pliku IOC:

   a. W obszarze **Źródło pliku IOC** wybierz **Wygeneruj z pliku**.

   b. Wprowadź nazwę pliku IOC.

   c. Wybierz plik TXT zawierający listę wskaźników naruszeń bezpieczeństwa.

   d. Wybierz typ pliku IOC: **Nazwy DNS**, **Sumy kontrolne plików**, **Adresy IP**.

   e. Kliknij **Wygeneruj**.

   Kaspersky Endpoint Security dodaje pliki IOC do kolekcji IOC. W razie potrzeby można tymczasowo wykluczyć pliki IOC z zakresu zadania.

7. Zapisz swoje zmiany.

Tworzenie zadania Skanowanie IOC

Możesz ręcznie utworzyć zadania *Skanowanie IOC*:

- W szczegółach alertów (tylko dla EDR Optimum).

  Szczegóły wykrycia to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Optimum oraz w pomocy do Kaspersky Endpoint Detection and Response Expert.

- Korzystanie z Kreatora tworzenia zadania.

Możesz skonfigurować zadanie dla EDR Optimum w Web Console i Cloud Console. Ustawienia zadania dla EDR Expert są dostępne tylko w Cloud Console.

Aby utworzyć zadanie Skanowanie IOC:

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Skanowanie IOC**.

   c. W polu **Nazwa zadania** wpisz krótki opis.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Przejdź do następnego kroku.

5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Przejdź do następnego kroku.

   Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

   Konto systemowe (SYSTEM) nie posiada uprawnienia do wykonywania zadania *Skanowanie IOC* na dyskach sieciowych. Jeśli chcesz uruchomić zadanie dla dysku sieciowego, wybierz konto użytkownika, który posiada dostęp do tego dysku.

   W przypadku autonomicznych zadań Skanowanie IOC na dyskach sieciowych, we właściwościach zadania należy ręcznie wybrać konto użytkownika, które ma dostęp do tego dysku.

6. Zakończ działanie kreatora.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij nowe zadanie.

   Zostanie otwarte okno właściwości zadania.

8. Wybierz zakładkę **Ustawienia aplikacji**.

9. Przejdź do sekcji **Skanowanie zagrożeń**.

10. Prześlij pliki IOC, aby wyszukać wskaźniki naruszeń bezpieczeństwa.

    Po przesłaniu plików IOC aplikacja wyświetla podsumowanie informacji o pliku, włącznie z listą wskaźników, które nie przeszły kontroli. Po przesłaniu plików IOC możesz ręcznie edytować pliki we wbudowanym edytorze bezpośrednio we właściwościach zadania. Kaspersky Endpoint Security obsługuje edycję plików IOC zgodnych ze standardem OpenIOC 1.1. Nie można modyfikować zawartości plików IOC zgodnych z wersją OpenIOC 1.0.

    Kaspersky Endpoint Security dodaje pliki IOC do kolekcji IOC. W razie potrzeby można tymczasowo wykluczyć pliki IOC z zakresu zadania.

    > Dodanie lub usunięcie plików IOC po uruchomieniu zadania nie jest zalecane. To może spowodować niepoprawne wyświetlenie wyników skanowania IOC przed wcześniejszymi uruchomieniami zadania. Aby wyszukać wskaźniki naruszeń bezpieczeństwa przez nowe pliki IOC, zalecane jest dodanie nowych zadań.

11. Jeśli to konieczne, zaznacz pole wyboru **Retrospektywne skanowanie IOC**. *Retrospektywne skanowanie IOC* jest trybem zadania *Skanowanie IOC*, w ramach którego Kaspersky Endpoint Security skanuje dane w poszukiwaniu oznak naruszenia bezpieczeństwa przez określony czas. Tryb ten jest przeznaczony do wyszukiwania wskaźników zagrożenia na podstawie danych telemetrycznych chronionego komputera, takich jak aktywność sieciowa, procesy, pliki i inne dane telemetryczne. Kaspersky Endpoint Security analizuje dane w dziennikach systemu operacyjnego i dziennikach przeglądarki na komputerze. Retrospektywne skanowanie IOC analizuje logi następujących przeglądarek: Google Chrome, Mozilla Firefox, Microsoft Edge (wersja 79 lub nowsza).

12. Skonfiguruj akcje po wykryciu IOC:

    - **Odizoluj urządzenie od sieci**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security odizoluje komputer od sieci, aby zapobiec rozprzestrzenianiu się zagrożenia. Możesz skonfigurować czas trwania izolacji w ustawieniach komponentu Endpoint Detection and Response.

      Jeśli to pole wyboru jest odznaczone, możesz odizolować komputer od sieci po ręcznym uruchomieniu zadania. Jeśli zadanie *Skanowanie IOC* wykryje wskaźnik naruszeń bezpieczeństwa, możesz odizolować komputer od sieci bezpośrednio z poziomu wskaźnika naruszeń bezpieczeństwa (właściwości *Skanowanie IOC* → **Ustawienia aplikacji** → zadanie **Wyniki skanowania IOC**). Kaspersky Endpoint Security umożliwia również natychmiastowe zarządzanie dodatkowymi ustawieniami: Okresem wyłączenia izolacji sieciowej oraz Wykluczeniami izolacji sieciowej.

- **Przenieś kopię do Kwarantanny, usuń obiekt**. Jeśli ta opcja została zaznaczona, Kaspersky Endpoint Security usunie szkodliwy obiekt wykryty na komputerze. Przed usunięciem obiektu Kaspersky Endpoint Security utworzy kopię zapasową w przypadku, gdy obiekt musi zostać przywrócony w późniejszym czasie. Kaspersky Endpoint Security przeniesie kopię zapasową do Kwarantanny.

  Jeśli to pole wyboru jest odznaczone, możesz poddać plik kwarantannie ręcznie po ręcznym uruchomieniu zadania. Jeśli zadanie *Skanowanie IOC* wykryje plik, który może naruszyć dane, możesz poddać ten plik kwarantannie bezpośrednio z wyników skanowania IOC (**Ustawienia aplikacji → Wyniki skanowania IOC**). W wyniku tego działania Kaspersky Endpoint Security uruchamia kreator tworzenia zadania z predefiniowanymi danymi wykrytego pliku. Musisz jedynie zarządzać dodatkowymi ustawieniami zadań, na przykład skonfigurować harmonogram zadań.

- **Uruchom skanowanie obszarów krytycznych**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security uruchamia zadanie *Skanowanie obszarów krytycznych*. Domyślnie, Kaspersky Endpoint Security skanuje pamięć jądra, uruchomione procesy i sektory startowe dysku.

13. Przejdź do sekcji **Zaawansowane**.

14. Wybierz typy danych (dokumenty IOC), które muszą zostać przeanalizowane jako część zadania.

    Kaspersky Endpoint Security automatycznie wybiera typy danych (dokumenty IOC) dla zadania *Skanowanie IOC* zgodnie z zawartością załadowanych plików IOC. Nie jest zalecane odznaczenie typów danych.

    Dodatkowo możesz skonfigurować obszary skanowania dla następujących typów danych:

    - **Pliki - FileItem**. Ustaw obszar skanowania IOC na komputerze przy użyciu predefiniowanych obszarów.

      Domyślnie, Kaspersky Endpoint Security skanuje pod kątem wskaźników naruszeń bezpieczeństwa tylko ważne obszary komputera, takie jak folder Pobrane, pulpit, folder z tymczasowymi plikami systemu operacyjnego itd. Możesz także ręcznie dodać obszar skanowania.

    - **Dziennik zdarzeń Windows - EventLogItem**. Wprowadź czas zarejestrowania zdarzeń. Możesz także wybrać, które dzienniki zdarzeń systemu Windows muszą być użyte dla skanowania IOC. Domyślnie, wybrane są następujące dzienniki zdarzeń: dziennik zdarzeń aplikacji, dziennik zdarzeń systemu oraz dziennik zdarzeń ochrony.

    - **Rejestr Windowsa - RegistryItem**. Skonfiguruj zakres skanowania IOC w rejestrze.

      Domyślnie Kaspersky Endpoint Security skanuje zestaw kluczy rejestru.

15. W oknie właściwości zadania wybierz zakładkę **Terminarz**.

16. Skonfiguruj terminarz zadania.

    Wake-on-LAN nie jest dostępne dla tego zadania. Upewnij się, że komputer jest włączony do uruchomienia zadania.

17. Zapisz swoje zmiany.

18. Zaznacz pole obok zadania.

19. Kliknij **Uruchom**.

    W rezultacie Kaspersky Endpoint Security uruchamia wyszukiwanie wskaźników naruszeń bezpieczeństwa na komputerze. Możesz przejrzeć wyniki zadania we właściwościach zadania, w sekcji **Wyniki**. Informacje o

wykrytych wskaźnikach naruszeń bezpieczeństwa możesz przejrzeć we właściwościach zadania: **Ustawienia aplikacji** → **Wyniki skanowania IOC**. W wynikach skanowania IOC można również ręcznie poddać wykryty plik kwarantannie lub odizolować komputer od sieci.

Kaspersky Endpoint Security wyszukuje duplikaty wśród rekordów utworzonych dla tego samego pliku IOC, a w wynikach zadania zachowuje tylko unikatowe rekordy. Duplikaty to rekordy tego samego typu, które mają takie same wartości wszystkich porównywanych pól. Aplikacja może również nie utworzyć rekordu, jeśli w jednym lub kilku polach brakuje wartości (patrz tabela poniżej).

Typ	Porównywane pola	Warunek nieutworzenia rekordu
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• Brak wartości pól FullPath, Md5sum, Sha256sum. • Brakujące wartości pola FullPath i identyczne wartości pola Md5sum, Sha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Brak wartości co najmniej jednego z następujących pól: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	Brakujące wartości pól startTime lub PID.

W oknie **Szczegóły alertu** mogą być wyświetlane rekordy RegistryItem z identycznymi wartościami pól. Takie rekordy nie są duplikatami, ponieważ zawierają różne wartości pola Tekst, które nie jest wyświetlane w interfejsie.

Wyniki skanowania IOC są przechowywane 30 dni. Po tym czasie Kaspersky Endpoint Security automatycznie usuwa najstarsze wpisy.

Rozszerzona telemetria dla Skanowania IOC

Zalecamy włączenie rozszerzonej telemetrii na komputerze w celu retrospektywnego skanowania IOC. Rozszerzona telemetria poprawia dokładność wykrywania IOC, ale wykorzystuje więcej zasobów komputera.

Rozszerzona telemetria obejmuje obsługę następujących dodatkowych warunków:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed

- FileItem/Accessed
- FileItem/FileAttributes

Jeśli rozszerzona telemetria jest wyłączona, Kaspersky Endpoint Security może wymieniać informacje o wykrytych wskaźnikach naruszeń bezpieczeństwa.

Aby włączyć rozszerzoną telemetrię:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Endpoint Detection and Response**.
5. Zaznacz pole **Włącz zaawansowane rejestrowanie aktywności systemu**.
6. Zapisz swoje zmiany.

Przenieś plik do Kwarantanny

Podczas reagowania na zagrożenia Kaspersky Endpoint Detection and Response może utworzyć zadania *Przenieś plik do Kwarantanny*. To jest niezbędne do zminimalizowania konsekwencji wystąpienia zagrożenia. *Kwarantanna* to specjalny lokalny magazyn na komputerze. Użytkownik może poddać kwarantannie pliki, które użytkownik uznaje za niebezpieczne dla komputera. Pliki poddane kwarantannie są przechowywane w postaci zaszyfrowanej i nie zagrażają bezpieczeństwu urządzenia. Kaspersky Endpoint Security używa Kwarantanny tylko w przypadku integracji z rozwiązaniami Kaspersky Detection and Response. W innych przypadkach Kaspersky Endpoint Security umieszcza odpowiedni plik w Kopii zapasowej. Więcej informacji na temat zarządzania Kwarantanną jako częścią rozwiązań można znaleźć w pomocy dla Kaspersky Sandbox, pomocy dla Kaspersky Endpoint Detection and Response Optimum, pomocy dla Kaspersky Endpoint Detection and Response Expert, pomocy dla Kaspersky Anti Targeted Attack Platform i pomocy dla Kaspersky Endpoint Detection and Response Expert (on-premises).

Możesz utworzyć zadania *Przenieś plik do Kwarantanny* na następujące sposoby:

- W szczegółach alertów (tylko dla EDR Optimum).

  Szczegóły wykrycia to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Optimum oraz w pomocy do Kaspersky Endpoint Detection and Response Expert.
- Korzystanie z Kreatora tworzenia zadania.

  Musisz wprowadzić ścieżkę do pliku lub sumę kontrolną pliku (SHA256 lub MD5), albo obie te wartości.

- W ustawienia zadania *Skanowanie IOC*.

  Jeśli zadanie *Skanowanie IOC* wykryje plik, który może naruszyć dane, możesz poddać ten plik kwarantannie bezpośrednio z wyników skanowania IOC (**Ustawienia aplikacji** → **Wyniki skanowania IOC**). W wyniku tego działania Kaspersky Endpoint Security uruchamia kreator tworzenia zadania z predefiniowanymi danymi wykrytego pliku. Musisz jedynie zarządzać dodatkowymi ustawieniami zadań, na przykład skonfigurować harmonogram zadań.

Istnieją następujące ograniczenia zadania *Przenieś plik do Kwarantanny*.

1. Rozmiar pliku nie może przekraczać 100 MB.
2. Krytyczny obiekt systemowy (SCO) nie może zostać poddany kwarantannie. Krytyczne obiekty systemowe to pliki, które są wymagane przez system operacyjny i aplikację Kaspersky Endpoint Security for Windows do działania.
3. Możesz skonfigurować zadanie dla EDR Optimum w Web Console i Cloud Console. Ustawienia zadania dla EDR Expert są dostępne tylko w Cloud Console.
4. Nie możesz przeskanować obiektu poddanego kwarantannie w wyniku działania zadania *Przenieś plik do Kwarantanny*.

Aby utworzyć zadanie Przenieś plik do Kwarantanny:

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.
3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Przenieś plik do Kwarantanny**.

   c. W polu **Nazwa zadania** wpisz krótki opis.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.
4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij **Dalej**.
5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Kliknij **Dalej**.

   Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).
6. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

   Nowe zadanie zostanie wyświetlone na liście zadań.
7. Kliknij nowe zadanie.

   Zostanie otwarte okno właściwości zadania.
8. Wybierz zakładkę **Ustawienia aplikacji**.

9. Na liście plików kliknij **Dodaj**.

   Zostanie uruchomiony kreator dodawania plików.

10. Aby dodać plik, należy wprowadzić pełną ścieżkę do pliku lub zarówno sumę kontrolną, jak i ścieżkę.

    > Jeśli plik znajduje się na dysku sieciowym, wprowadź ścieżkę do pliku, począwszy od `\\`, a nie od litery dysku. Na przykład, `\\server\shared_folder\file.exe`. Jeśli ścieżka do pliku zawiera literę dysku sieciowego, możesz uzyskać błąd *Nie odnaleziono pliku*.

11. W oknie właściwości zadania wybierz zakładkę **Terminarz**.

12. Skonfiguruj terminarz zadania.

    > Wake-on-LAN nie jest dostępne dla tego zadania. Upewnij się, że komputer jest włączony do uruchomienia zadania.

13. Zapisz swoje zmiany.

14. Zaznacz pole obok zadania.

15. Kliknij **Uruchom**.

    W rezultacie, Kaspersky Endpoint Security przeniesie plik do Kwarantanny.

Jeśli plik jest zablokowany przez inny proces, zadanie jest wyświetlany jako *Zakończone*, ale sam plik jest poddawany kwarantannie tylko po ponownym uruchomieniu komputera. Po ponownym uruchomieniu komputera potwierdź usunięcie pliku.

Zadanie *Przenieś plik do Kwarantanny* może zostać zakończone błędem *Dostęp zabroniony*, jeśli próbujesz zagwarantować plik wykonywalny, który jest aktualnie uruchomiony. Utwórz zadanie kończenia procesu dla pliku i spróbuj ponownie.

Zadanie *Przenieś plik do Kwarantanny* może zostać zakończone błędem *Brak wystarczającej ilości miejsca w magazynie Kwarantanny*, jeśli próbujesz zagwarantować plik, który jest za duży. Opróżnij Kwarantannę lub zwiększ rozmiar Kwarantanny. Następnie spróbuj ponownie.

Możesz przywrócić plik z Kwarantanny lub opróżnić Kwarantannę przy użyciu konsoli Web Console. Możesz przywrócić obiekty lokalnie na komputerze przy użyciu wiersza polecenia.

Uzyskaj plik

Możesz uzyskać pliki z komputerów użytkowników. Na przykład, możesz skonfigurować uzyskiwanie pliku dziennika zdarzeń, utworzonego przez aplikację innej firmy. W wyniku wykonywania zadania plik zostanie zapisany w Kwarantannie. *Kwarantanna* to specjalny lokalny magazyn na komputerze. Możesz pobrać plik z Kwarantanny na swój komputer przy użyciu Web Console (**Operacje** → **Magazyny** → **Kwarantanna**). Na komputerze użytkownika plik pozostanie w oryginalnym folderze.

Rozmiar pliku nie może przekraczać 100 MB.

Możesz skonfigurować zadanie dla EDR Optimum w Web Console i Cloud Console. Ustawienia zadania dla EDR Expert są dostępne tylko w Cloud Console.

Aby utworzyć zadanie Uzyskaj plik:

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Uzyskaj plik**.

   c. W polu **Nazwa zadania** wpisz krótki opis.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij **Dalej**.

5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Kliknij **Dalej**.

   Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

6. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij nowe zadanie.

   Zostanie otwarte okno właściwości zadania.

8. Wybierz zakładkę **Ustawienia aplikacji**.

9. Na liście plików kliknij **Dodaj**.

   Zostanie uruchomiony kreator dodawania plików.

10. Aby dodać plik, należy wprowadzić pełną ścieżkę do pliku lub zarówno sumę kontrolną, jak i ścieżkę.

    Jeśli plik znajduje się na dysku sieciowym, wprowadź ścieżkę do pliku, począwszy od `\\`, a nie od litery dysku. Na przykład, `\\server\shared_folder\file.exe`. Jeśli ścieżka do pliku zawiera literę dysku sieciowego, możesz uzyskać błąd *Nie odnaleziono pliku*.

11. W oknie właściwości zadania wybierz zakładkę **Terminarz**.

12. Skonfiguruj terminarz zadania.

    Wake-on-LAN nie jest dostępne dla tego zadania. Upewnij się, że komputer jest włączony do uruchomienia zadania.

13. Zapisz swoje zmiany.

14. Zaznacz pole obok zadania.

15. Kliknij **Uruchom**.

    W rezultacie Kaspersky Endpoint Security tworzy kopię pliku i przenosi tę kopię do Kwarantanny. Plik możesz pobrać z Kwarantanny w Web Console.

Usuń plik

Możesz zdalnie usunąć pliki przy użyciu zadania *Usuń plik*. Na przykład, podczas reagowania na zagrożenie możesz zdalnie usunąć plik.

Istnieją następujące ograniczenia zadania *Usuń plik*:

- System Critical Object (SCO) nie może zostać usunięty. Krytyczne obiekty systemowe to pliki, które są wymagane przez system operacyjny i aplikację Kaspersky Endpoint Security do działania.
- Możesz skonfigurować zadanie dla EDR Optimum w Web Console i Cloud Console. Ustawienia zadania dla EDR Expert są dostępne tylko w Cloud Console.

Aby utworzyć zadanie Usuń plik:

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Usuń plik**.

   c. W polu **Nazwa zadania** wpisz krótki opis.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij **Dalej**.

5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Kliknij **Dalej**.

   Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

6. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij nowe zadanie.

   Zostanie otwarte okno właściwości zadania.

8. Wybierz zakładkę **Ustawienia aplikacji**.

9. Na liście plików kliknij **Dodaj**.

   Zostanie uruchomiony kreator dodawania plików.

10. Aby dodać plik, należy wprowadzić pełną ścieżkę do pliku lub zarówno sumę kontrolną, jak i ścieżkę.

    Jeśli plik znajduje się na dysku sieciowym, wprowadź ścieżkę do pliku, począwszy od `\\`, a nie od litery dysku. Na przykład, `\\server\shared_folder\file.exe`. Jeśli ścieżka do pliku zawiera literę dysku sieciowego, możesz uzyskać błąd *Nie odnaleziono pliku*.

11. W oknie właściwości zadania wybierz zakładkę **Terminarz**.

12. Skonfiguruj terminarz zadania.

    Wake-on-LAN nie jest dostępne dla tego zadania. Upewnij się, że komputer jest włączony do uruchomienia zadania.

13. Zapisz swoje zmiany.

14. Zaznacz pole obok zadania.

15. Kliknij **Uruchom**.

W rezultacie, Kaspersky Endpoint Security usunie plik z komputera. Jeśli plik jest zablokowany przez inny proces, zadanie jest wyświetlany jako *Gotowe*, ale sam plik jest usuwany tylko po ponownym uruchomieniu komputera. Po ponownym uruchomieniu komputera potwierdź usunięcie pliku.

Zadanie *Usuń plik* może zostać zakończone błędem *Brak dostępu lub plik nie został odnaleziony*, jeśli próbujesz usunąć plik wykonywalny, który jest aktualnie uruchomiony. Utwórz zadanie kończenia procesu dla pliku i spróbuj ponownie.

Rozpoczęcie procesu

Możesz zdalnie uruchomić pliki przy użyciu zadania *Rozpoczęcie procesu*. Na przykład, możesz zdalnie uruchomić narzędzie, które tworzy plik konfiguracyjny komputera. Następnie możesz użyć zadania *Odbierz plik z urządzenia*, aby otrzymać utworzony plik w konsoli Kaspersky Security Center Web Console.

Możesz skonfigurować zadanie dla EDR Optimum w Web Console i Cloud Console. Ustawienia zadania dla EDR Expert są dostępne tylko w Cloud Console.

Aby utworzyć zadanie Rozpoczęcie procesu:

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Rozpoczęcie procesu**.

   c. W polu **Nazwa zadania** wpisz krótki opis.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij **Dalej**.

5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Kliknij **Dalej**.

   Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

6. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij nowe zadanie.

8. Zostanie otwarte okno właściwości zadania.

9. Wybierz zakładkę **Ustawienia aplikacji**.

10. Wpisz polecenie rozpoczęcia procesu.

Na przykład, jeśli chcesz uruchomić narzędzie (`utility.exe`), które zapisuje informacje o konfiguracji komputera do pliku `conf.txt` w bieżącym folderze (domyślnie). Narzędzie znajduje się w folderze `C:\Users\admin\Diagnostic\`. Musisz zapisać plik konfiguracyjny w folderze `C:\Users\admin\Documents\Configuration`. Wprowadź następujące wartości:

- **Polecenie wykonywalne** – `C:\Users\admin\Diagnostic\utility.exe`
- **Argumenty wiersza polecenia (opcjonalne)** – `/R conf.txt`
- **Ścieżka do katalogu (opcjonalna)** – `C:\Users\admin\Documents\Configuration`

11. W oknie właściwości zadania wybierz zakładkę **Terminarz**.
12. Skonfiguruj terminarz zadania.

    Wake-on-LAN nie jest dostępne dla tego zadania. Upewnij się, że komputer jest włączony do uruchomienia zadania.

13. Zapisz swoje zmiany.
14. Zaznacz pole obok zadania.
15. Kliknij **Uruchom**.

    Kaspersky Endpoint Security uruchomi polecenie w trybie cichym i uruchomi proces. Możesz przejrzeć wyniki zadania we właściwościach zadania, w sekcji **Wyniki wykonania**.

Kończenie działania procesu

Możesz zdalnie zakończyć działanie procesu, korzystając z zadania *Zakończ proces*. Na przykład, możesz zdalnie zakończyć działanie narzędzia testującego prędkość internetu, które zostało uruchomione przy użyciu zadania *Uruchom proces*.

Jeśli chcesz zapobiec uruchomieniu pliku, możesz skonfigurować komponent Zapobieganie wykonywaniu. Możesz zabronić wykonaniu plików wykonywalnych, skryptów, plików formatów office.

Istnieją następujące ograniczenia zadania *Zakończ proces*:

- Procesy Krytycznego obiektu systemowego (SCO) nie mogą zostać zakończone. Krytyczne obiekty systemowe to pliki, które są wymagane przez system operacyjny i aplikację Kaspersky Endpoint Security do działania.
- Możesz skonfigurować zadanie dla EDR Optimum w Web Console i Cloud Console. Ustawienia zadania dla EDR Expert są dostępne tylko w Cloud Console.

Aby utworzyć zadanie Zakończ proces:

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

   a. Z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows 14.2.0**.

   b. Z listy rozwijalnej **Typ zadania** wybierz **Zakończ proces**.

   c. W polu **Nazwa zadania** wpisz krótki opis.

   d. W sekcji **Urządzenia, do których zostanie przypisane zadanie** wybierz żądany zakres zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij **Dalej**.

5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Kliknij **Dalej**.

   Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

6. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

   Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij nowe zadanie.

   Zostanie otwarte okno właściwości zadania.

8. Wybierz zakładkę **Ustawienia aplikacji**.

9. Aby zakończyć proces, musisz wybrać plik, którego działanie chcesz zakończyć. Możesz wybrać plik na jeden z następujących sposobów:

   - Wprowadź pełną nazwę pliku.
   - Wprowadź skrót pliku i ścieżkę do pliku.
   - Wprowadź PID procesu (dotyczy tylko zadań lokalnych).

   Jeśli plik znajduje się na dysku sieciowym, wprowadź ścieżkę do pliku, począwszy od `\\`, a nie od litery dysku. Na przykład, `\\server\shared_folder\file.exe`. Jeśli ścieżka do pliku zawiera literę dysku sieciowego, możesz uzyskać błąd *Nie odnaleziono pliku*.

10. W oknie właściwości zadania wybierz zakładkę **Terminarz**.

11. Skonfiguruj terminarz zadania.

    Wake-on-LAN nie jest dostępne dla tego zadania. Upewnij się, że komputer jest włączony do uruchomienia zadania.

12. Kliknij **Zapisz**.

13. Zaznacz pole obok zadania.

14. Kliknij **Uruchom**.

W rezultacie, Kaspersky Endpoint Security zakończy proces na komputerze. Jeśli na przykład aplikacja GAME jest uruchomiona, a użytkownik zakończy proces game.exe, aplikacja zostanie zamknięta bez zapisywania danych. Możesz przejrzeć wyniki zadania we właściwościach zadania, w sekcji **Wyniki**.

Zapobieganie wykonywaniu

Zapobieganie wykonywaniu umożliwia zarządzanie uruchamianiem plików wykonywalnych i skryptów, a także otwieraniem plików formatu office. W ten sposób możesz, na przykład, zapobiec wykonaniu aplikacji, które uważasz za niezabezpieczone. W wyniku tego działania można zatrzymać rozprzestrzenianie się zagrożenia. Zapobieganie wykonywaniu obsługuje zestaw rozszerzeń plików pakietu office oraz zestaw interpreterów skryptu.

Reguła zapobiegania wykonywaniu

Zapobieganie wykonywaniu zarządza dostępem użytkownika do plików z regułami zapobiegania wykonywaniu. *Reguły zapobiegania wykonywaniu* to zestaw kryteriów, które aplikacja bierze pod uwagę podczas reagowania na wykonanie obiektu, na przykład, podczas blokowania wykonania obiektu. Aplikacja identyfikuje pliki według ich ścieżek lub sum kontrolnych wyliczonych przy użyciu algorytmów haszowania MD5 i SHA256.

Możesz utworzyć reguły Zapobiegania wykonywaniu:

- W szczegółach alertów (tylko dla EDR Optimum).

  Szczegóły wykrycia to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Optimum oraz w pomocy do Kaspersky Endpoint Detection and Response Expert.

- Korzystając z zasad grupy lub lokalnych ustawień aplikacji.

  Musisz wprowadzić ścieżkę do pliku lub sumę kontrolną pliku (SHA256 lub MD5), albo obie te wartości.

Możesz także zarządzać Zapobieganiem wykonywaniu lokalnie przy użyciu wiersza polecenia.

Zapobieganie wykonywaniu posiada następujące ograniczenia:

1. Reguł zapobiegania nie obejmują plików na płytach CD lub obrazów ISO. Aplikacja nie blokuje wykonywania lub otwierania tych plików.

2. Nie jest możliwe zablokowanie uruchamiania obiektów krytycznych dla systemu (SCO). Krytyczne obiekty systemowe to pliki, które są wymagane przez system operacyjny i aplikację Kaspersky Endpoint Security do działania.

3. Nie jest zalecane utworzenie więcej niż 5 000 reguł zapobiegania uruchomieniu, gdyż może to spowodować niestabilność systemu.

Tryby reguły zapobiegania wykonywaniu

Komponent Zapobieganie wykonywaniu może działać w dwóch trybach:

- **Tylko statystyki**

  W tym trybie Kaspersky Endpoint Security publikuje zdarzenie dotyczące prób uruchomienia obiektów wykonywalnych lub otwarcia dokumentów, które odpowiadają kryteriom reguły blokowania, w Dzienniku zdarzeń Windows oraz w Kaspersky Security Center, ale nie blokują próby uruchomienia lub otwarcia obiektu lub dokumentu. Ten tryb jest wybrany domyślnie.

- **Aktywny**

  W tym trybie aplikacja blokuje wykonanie obiektów lub otwieranie dokumentów, które odpowiadają kryteriom reguły blokowania. Aplikacja publikuje także zdarzenie dotyczące prób wykonania obiektów lub otwarcia dokumentów w Dzienniku zdarzeń Windows oraz dzienniku zdarzeń Kaspersky Security Center.

Zarządzanie zapobieganiem wykonaniu

Możesz skonfigurować ustawienia komponentu tylko w Web Console.

W celu zapobiegania wykonywaniu:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Endpoint Detection and Response**.
5. Wybierz zakładkę **Zapobieganie wykonywaniu**.
6. Włącz przełącznik **Zapobieganie wykonywaniu WŁĄCZONE**.
7. W sekcji **Akcja podczas wykonywania lub otwierania zabronionego obiektu** wybierz tryb działania komponentu:

   - **Zablokuj i dodaj do dziennika zdarzeń**. W tym trybie aplikacja blokuje wykonanie obiektów lub otwieranie dokumentów, które odpowiadają kryteriom reguły blokowania. Aplikacja publikuje także zdarzenie dotyczące prób wykonania obiektów lub otwarcia dokumentów w Dzienniku zdarzeń Windows oraz dzienniku zdarzeń Kaspersky Security Center.

   - **Dodaj do dziennika zdarzeń**. W tym trybie Kaspersky Endpoint Security publikuje zdarzenie dotyczące prób uruchomienia obiektów wykonywalnych lub otwarcia dokumentów, które odpowiadają kryteriom reguły blokowania, w Dzienniku zdarzeń Windows oraz w Kaspersky Security Center, ale nie blokują próby uruchomienia lub otwarcia obiektu lub dokumentu. Ten tryb jest wybrany domyślnie.

8. Utwórz listę reguł zapobiegania wykonywaniu:

   a. Kliknij **Dodaj**.

   b. To spowoduje otwarcie okna; w tym oknie wprowadź nazwę reguły zapobiegania wykonywaniu (na przykład, *Aplikacja A*).

   c. Z listy rozwijalnej **Typ** wybierz obiekt, który chcesz zablokować: **Plik wykonywalny**, **Skrypt**, **Dokument Microsoft Office**.

   Jeśli wybrałeś zły typ obiektu, Kaspersky Endpoint Security nie blokuje pliku lub skryptu.

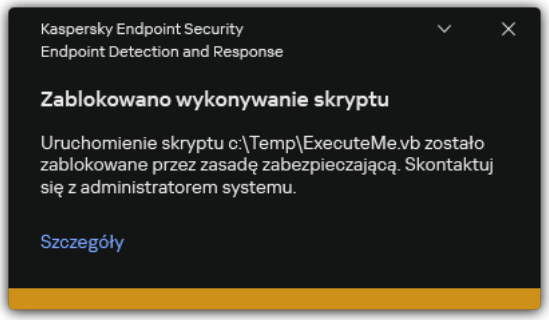
   d. Aby dodać plik, należy wprowadzić sumę kontrolną pliku (SHA256 lub MD5), pełną ścieżkę do pliku lub sumę kontrolną i ścieżkę.

   > Jeśli plik znajduje się na dysku sieciowym, wprowadź ścieżkę do pliku, począwszy od `\\`, a nie od litery dysku. Na przykład, `\\server\shared_folder\file.exe`. Jeśli ścieżka dostępu do pliku zawiera literę dysku sieciowego, Kaspersky Endpoint Security nie blokuje pliku lub skryptu.

   Zapobieganie wykonywaniu obsługuje zestaw rozszerzeń plików pakietu office oraz zestaw interpreterów skryptu.

9. Zapisz swoje zmiany.

W rezultacie Kaspersky Endpoint Security zablokuje wykonanie obiektów: uruchomienie skryptów i plików wykonywalnych, otwarcie plików formatów office. Jednakże możesz, na przykład, otworzyć plik skryptu w edytorze tekstu nawet wtedy, gdy uruchomienie skryptów zostanie uniemożliwione. Podczas blokowania wykonania obiektu Kaspersky Endpoint Security wyświetli standardowe powiadomienie (patrz rysunek poniżej), jeśli powiadomienia są włączone w ustawieniach aplikacji.



Powiadomienie o zapobieganiu wykonywania

Izolacja sieci komputerowej

Izolacja sieci komputerowej umożliwia automatyczne izolowanie komputera od sieci w odpowiedzi na wykrycie wskaźnika naruszeń bezpieczeństwa (IOC) – to jest *tryb automatyczny*. Możesz ręcznie włączyć Izolację od sieci, gdy analizujesz wykryte zagrożenie – to jest *tryb ręczny*.

Jeśli Izolacja sieci jest włączona, aplikacja zrywa wszystkie aktywne połączenia i blokuje wszystkie nowe połączenia sieciowe TCP/IP na komputerze, za wyjątkiem następujących połączeń:

- Połączenia znajdujące się w wykluczeniach Izolacji sieci.
- Połączenia zainicjowane przez usługi Kaspersky Endpoint Security.
- Połączenia zainicjowane przez agenta sieciowego Kaspersky Security Center.
- Połączenia z maszyną SVM i serwerem integracyjnym, jeśli aplikacja jest używana w trybie Light Agent.
- Połączenia z KSN podczas integracji aplikacji z Kaspersky Managed Detection and Response.

Możesz skonfigurować ustawienia komponentu tylko w Web Console.

Automatyczny tryb izolacji od sieci

Możesz skonfigurować Izolację sieci tak, aby była włączana automatycznie w odpowiedzi na wykrycie IOC. Możesz skonfigurować automatyczny tryb izolacji od sieci za pomocą zasad grupy.

Konfigurowanie Izolacji sieci tak, aby była włączana automatycznie w odpowiedzi na wykrycie IOC

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie **Skanowanie IOC** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

   W razie konieczności utworzyć zadanie *Skanowanie IOC*.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. W sekcji **Akcja po wykryciu IOC** zaznacz pola **Podejmij działania w odpowiedzi po znalezieniu IOC** i **Odizoluj komputer od sieci**.

5. Zapisz swoje zmiany.

   W wyniku tego działania, po wykryciu IOC, aplikacja odizoluje komputer od sieci, aby zapobiec rozprzestrzenianiu zagrożenia.

Można skonfigurować automatyczne wyłączanie izolacji od sieci po upływie określonego czasu. Domyślnie, aplikacja wyłącza Izolację sieci po 8 godzinach od czasu, gdy została włączona. Możesz także wyłączyć izolację od sieci ręcznie (patrz instrukcje poniżej). Po wyłączeniu Izolacji sieci komputer może używać sieci bez ograniczeń.

Konfigurowanie opóźnienia wyłączania Izolacji sieci dla komputera w trybie automatycznym

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów → Endpoint Detection and Response**.
5. Wybierz zakładkę **Izolacja od sieci**.
6. Wybierz opóźnienie wyłączenia Izolacji od sieci.
7. Zapisz swoje zmiany.

Ręczny tryb izolacji od sieci

Możesz także ręcznie włączyć i wyłączyć Izolację od sieci. Możesz skonfigurować ręczny tryb Izolacji od sieci, korzystając z właściwości komputera w konsoli Kaspersky Security Center.

Izolację sieci można włączyć:

- W szczegółach alertów (tylko dla EDR Optimum).

  Szczegóły wykrycia to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Optimum oraz w pomocy do Kaspersky Endpoint Detection and Response Expert.

- Przy pomocy lokalnych ustawień aplikacji.

- W ustawienia zadania *Skanowanie IOC*.

  Jeśli zadanie *Skanowanie IOC* wykryje wskaźnik naruszeń bezpieczeństwa, możesz odizolować komputer od sieci bezpośrednio z poziomu wskaźnika naruszeń bezpieczeństwa (właściwości *Skanowanie IOC* → **Ustawienia aplikacji** → zadanie **Wyniki skanowania IOC**). Kaspersky Endpoint Security umożliwia również natychmiastowe zarządzanie dodatkowymi ustawieniami: Okresem wyłączenia izolacji sieciowej oraz Wykluczeniami izolacji sieciowej.

Ręczne włączanie Izolacji sieci komputera

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasoby (urządzenia)**.
2. Wybierz komputer, dla którego chcesz skonfigurować lokalne ustawienia aplikacji.

   Spowoduje to otwarcie właściwości komputera.
3. Wybierz zakładkę **Aplikacje**.
4. Kliknij **Kaspersky Endpoint Security for Windows**.

   Spowoduje to otwarcie lokalnych ustawień aplikacji.
5. Wybierz zakładkę **Ustawienia aplikacji**.
6. Wybierz **Detection and Response → Endpoint Detection and Response**.
7. W sekcji **Izolacja od sieci** kliknij **Odizoluj komputer od sieci**.

Można skonfigurować automatyczne wyłączanie izolacji od sieci po upływie określonego czasu. Domyślnie, aplikacja wyłącza Izolację sieci po 8 godzinach od czasu, gdy została włączona. Po wyłączeniu Izolacji sieci komputer może używać sieci bez ograniczeń.

Konfigurowanie opóźnienia wyłączania Izolacji od sieci dla komputera w trybie ręcznym

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Wybierz komputer, dla którego chcesz skonfigurować lokalne ustawienia aplikacji.
   Spowoduje to otwarcie właściwości komputera.
3. Wybierz zakładkę **Zadania**.
   Spowoduje to wyświetlenie listy zadań dostępnych na komputerze.
4. Wybierz zadanie **Izolacja od sieci**.
5. Wybierz zakładkę **Ustawienia aplikacji**.
6. Spowoduje to otwarcie okna; w tym oknie wybierz opóźnienie wyłączenia Izolacji od sieci.
7. Zapisz swoje zmiany.

Ręczne wyłączanie Izolacji sieci komputera

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Wybierz komputer, dla którego chcesz skonfigurować lokalne ustawienia aplikacji.
   Spowoduje to otwarcie właściwości komputera.
3. Wybierz zakładkę **Aplikacje**.
4. Kliknij **Kaspersky Endpoint Security for Windows**.
   Spowoduje to otwarcie lokalnych ustawień aplikacji.
5. Wybierz zakładkę **Ustawienia aplikacji**.
6. Wybierz **Detection and Response** → **Endpoint Detection and Response**.
7. W sekcji **Izolacja od sieci** kliknij **Odblokuj izolację komputera od sieci**.

Możesz także wyłączyć Izolację sieci lokalnie przy użyciu wiersza polecenia.

Począwszy od wersji Kaspersky Endpoint Security 12.10 for Windows możesz zarządzać izolacją sieci w szczegółach alertów. Dodatkowo w szczegółach alertu można określić okres izolacji komputera od sieci. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Optimum oraz w pomocy do Kaspersky Endpoint Detection and Response Expert.

Wykluczenia Izolacji sieci

Możesz skonfigurować wykluczenia Izolacji sieci. Połączenia sieciowe, które odpowiadają regułom, nie są blokowane na komputerze, gdy Izolacja sieci jest włączona.

Aby skonfigurować wykluczenia izolacji sieci, możesz użyć listy *standardowych profili sieciowych*. Domyślnie, wykluczenia obejmują profile sieciowe zawierające reguły, które zapewniają nieprzerwane działanie urządzeń z rolami serwera DNS/DHCP i klienta DNS/DHCP. Możesz także ręcznie zmodyfikować ustawienia standardowych profili sieciowych lub zdefiniować wykluczenia (patrz instrukcja poniżej).

Wykluczenia określone we właściwościach zasady są stosowane tylko wtedy, gdy Izolacja sieci zostaje włączona automatycznie w odpowiedzi na wykryte zagrożenie. Wykluczenia określone we właściwościach komputera są stosowane tylko wtedy, gdy Izolacja od sieci zostanie włączona ręcznie we właściwościach komputera w konsoli Kaspersky Security Center lub w szczegółach alertu.

Aktywna zasada nie zapobiega stosowaniu wykluczeń z Izolacji sieci, skonfigurowanej we właściwościach komputera, ponieważ te parametry mają inne scenariusze korzystania.

Dodawanie wykluczenia Izolacji sieci w trybie automatycznym

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Endpoint Detection and Response**.
5. Wybierz zakładkę **Izolacja od sieci**.
6. W sekcji **Wykluczenia izolacji od sieci** kliknij **Wykluczenia**.
7. To spowoduje otwarcie okna; w tym oknie kliknij **Dodaj** → **Dodaj z profilu** i wybierz standardowe profile sieciowe do konfigurowania wykluczeń.

   Wykluczenia Izolacji sieci z profilu są dodawane do listy wykluczeń Izolacji sieci. Możesz przejrzeć właściwości połączenia sieciowego. Jeśli to konieczne, możesz zmodyfikować ustawienia połączenia sieciowego.
8. Jeśli to konieczne, ręcznie dodaj wykluczenie Izolacji sieci. Aby to zrobić, w oknie z listą wykluczeń kliknij **Dodaj** → **Dodaj** i ręcznie edytuj ustawienia połączenia sieciowego.
9. Zapisz swoje zmiany.

Dodawanie wykluczenia Izolacji sieci w trybie ręcznym

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Wybierz komputer, dla którego chcesz skonfigurować lokalne ustawienia aplikacji.

   Spowoduje to otwarcie właściwości komputera.
3. Wybierz zakładkę **Zadania**.

   Spowoduje to wyświetlenie listy zadań dostępnych na komputerze.
4. Wybierz zadanie **Izolacja od sieci**.
5. Wybierz zakładkę **Ustawienia aplikacji**.

6. To spowoduje otwarcie okna; w tym oknie kliknij **Wykluczenia**.

7. To spowoduje otwarcie okna; w tym oknie kliknij **Dodaj z profilu** i wybierz standardowe profile sieciowe do konfigurowania wykluczeń.

   Wykluczenia Izolacji sieci z profilu są dodawane do listy wykluczeń Izolacji sieci. Możesz przejrzeć właściwości połączenia sieciowego. Jeśli to konieczne, możesz zmodyfikować ustawienia połączenia sieciowego.

8. Jeśli to konieczne, ręcznie dodaj wykluczenie Izolacji sieci. Aby to zrobić, w oknie z listą wykluczeń kliknij **Dodaj** i ręcznie edytuj ustawienia połączenia sieciowego.

9. Zapisz swoje zmiany.

Możesz także przejrzeć listę wykluczenia Izolacji sieci lokalnie, korzystając z wiersza polecenia. W takim przypadku komputer musi zostać odizolowany.

Począwszy od wersji Kaspersky Endpoint Security 12.10 for Windows w szczegółach alertu można dodać Wykluczenia izolacji sieciowej. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Optimum oraz w pomocy do Kaspersky Endpoint Detection and Response Expert.

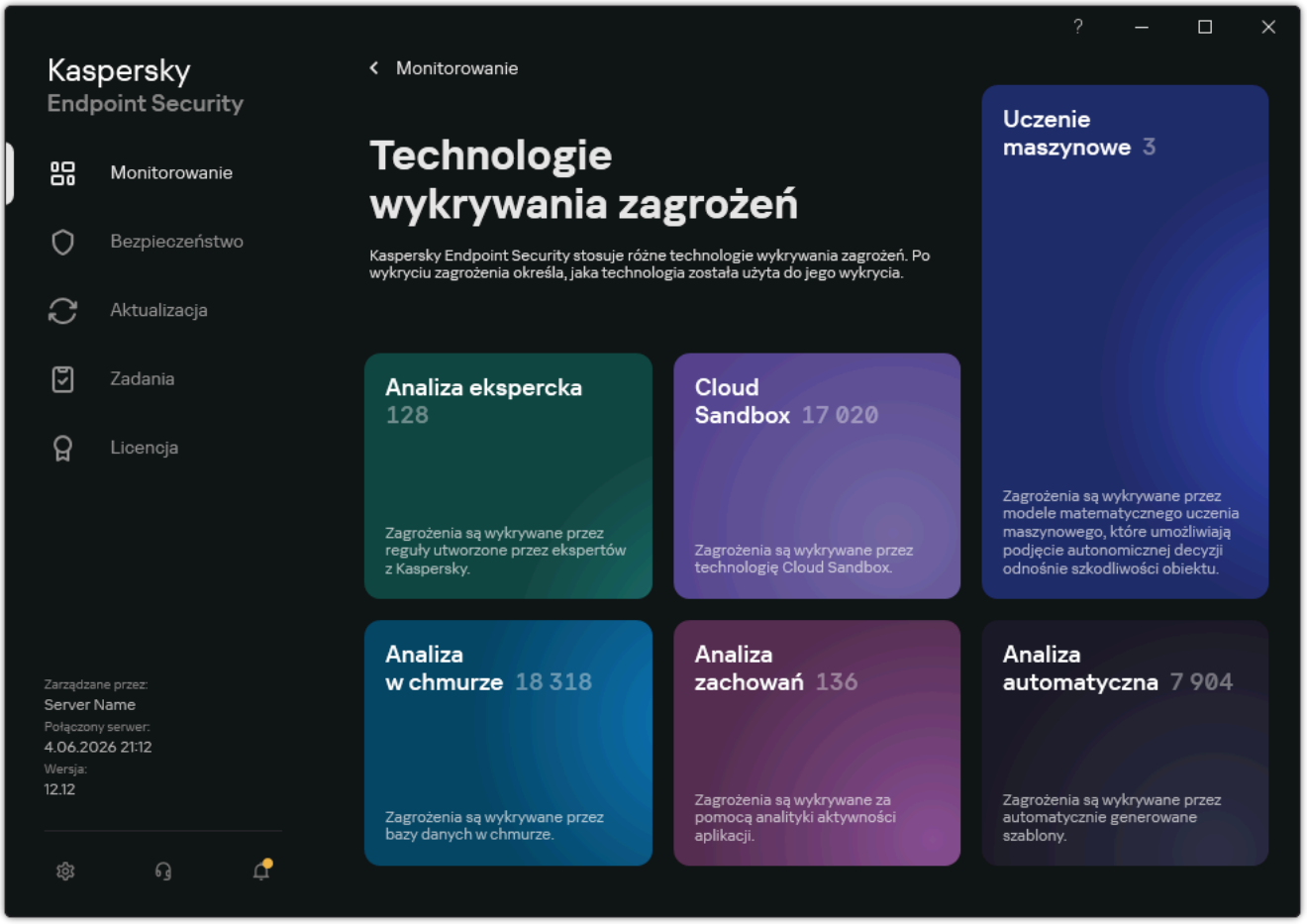
Cloud Sandbox

Cloud Sandbox to technologia pozwalająca na wykrywanie zaawansowanych zagrożeń na komputerze. Kaspersky Endpoint Security automatycznie przesyła usunięte pliki do Cloud Sandbox w celu ich przeanalizowania. Cloud Sandbox uruchamia te pliki w odizolowanym środowisku, aby zidentyfikować złośliwą aktywność i zdecydować o ich reputacji. Dane z tych plików są następnie wysyłane do Kaspersky Security Network. Dlatego też, jeżeli Cloud Sandbox wykrył szkodliwy plik, Kaspersky Endpoint Security wykona odpowiednią akcję w celu wyeliminowania tego zagrożenia na wszystkich komputerach, na których ten plik został wykryty.

Aby Cloud Sandbox mógł działać, musisz włączyć korzystanie z Kaspersky Security Network.

Jeśli używasz Kaspersky Private Security Network, technologia Cloud Sandbox nie jest dostępna.

Technologia Cloud Sandbox jest stale włączona i jest dostępna dla wszystkich użytkowników Kaspersky Security Network, niezależnie od typu licencji, z której korzystają. Jeśli wdrożono już rozwiązanie Endpoint Detection and Response Optimum, możesz włączyć osobny licznik zagrożeń wykrytych przez Cloud Sandbox. Możesz użyć tego licznika do kompilowania statystyk podczas analizy wykrytych zagrożeń. Kaspersky Endpoint Security wskazuje technologię wykrywania zagrożeń Cloud Sandbox w *Raport o zagrożeniach* w konsoli Kaspersky Security Center.



Liczniki zagrożeń

Aby włączyć licznik Cloud Sandbox:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Endpoint Detection and Response**.
5. Wybierz zakładkę **Cloud Sandbox**.
6. Włącz przełącznik **Cloud Sandbox WŁĄCZONY**.
7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Za każdym razem, gdy pojawi się zagrożenie, Kaspersky Endpoint Security aktywuje licznik zagrożeń wykrytych przy użyciu Cloud Sandbox w głównym oknie aplikacji pod **Technologie wykrywania zagrożeń**. Kaspersky Endpoint Security będzie również wskazywał technologię wykrywania zagrożeń Cloud Sandbox w *Raport o zagrożeniach* w konsoli Kaspersky Security Center.

Przewodnik migracji z KEA do KES dla EDR Optimum

Kaspersky Endpoint Security for Windows zawiera wbudowanego agenta dla rozwiązania Kaspersky Endpoint Detection and Response Optimum. Nie potrzebujesz już oddzielnej aplikacji Kaspersky Endpoint Agent do pracy z EDR Optimum. Wszystkie funkcje Kaspersky Endpoint Agent będą wykonywane przez Kaspersky Endpoint Security.

Podczas wdrażania Kaspersky Endpoint Security na komputerach, na których jest zainstalowany Kaspersky Endpoint Agent, rozwiązanie Kaspersky Endpoint Detection and Response Optimum będzie nadal działać z Kaspersky Endpoint Security. Dodatkowo, Kaspersky Endpoint Agent zostanie usunięty z komputera. To samo zachowanie w systemie wystąpi podczas aktualizacji Kaspersky Endpoint Security do wersji 11.7.0 lub nowszej.

Kaspersky Endpoint Security nie jest kompatybilny z Kaspersky Endpoint Agent. Obu tych aplikacji nie można zainstalować na tym samym komputerze.

Aby aplikacja Kaspersky Endpoint Security działała w ramach Kaspersky Endpoint Detection and Response Optimum, muszą być spełnione następujące warunki:

- Kaspersky Endpoint Detection and Response Optimum w wersji 2.0 lub nowszej.
- Kaspersky Security Center w wersji 13.2 lub nowszej (w tym Agent sieciowy). We wcześniejszych wersjach Kaspersky Security Center nie ma możliwości aktywowania funkcji EDR Optimum.
- EDR Optimum może być zarządzany tylko przy użyciu konsoli Kaspersky Security Center Web Console.
- Przesyłanie danych do Serwera administracyjnego jest włączone. Dane są wymagane do uzyskania informacji o plikach poddanych kwarantannie na komputerze za pośrednictwem Web Console.
- Połączenia w tle między Kaspersky Security Center Web Console a Serwerem administracyjnym zostało nawiązane. Aby rozwiązanie EDR Optimum działało z Serwerem administracyjnym poprzez Kaspersky Security Center Web Console, należy nawiązać nowe bezpieczne połączenie – *połączenie w tle*.

Kroki migracji konfiguracji [KES+KEA] do [KES+wbudowanego agenta] dla EDR Optimum

1. **Aktualizowanie wtyczki webowej Kaspersky Endpoint Security**

   Komponentem EDR Optimum można zarządzać przy użyciu wtyczki sieciowej Kaspersky Endpoint Security w wersji 11.7.0 lub nowszej.

2. **Migrowanie zasad i zadań**

   Przenieś ustawienia Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows. W tym celu użyj kreatora migracji z Kaspersky Endpoint Agent w Web Console.

   Jak dokonać migracji ustawień zasady i zadania z Kaspersky Endpoint Agent do Kaspersky Endpoint Security w Web Console:

   W oknie głównym Web Console wybierz **Operacje → Migracja z Kaspersky Endpoint Agent**.

   To spowoduje uruchomienie Kreatora migracji zasad i zadań. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Migracja zasady

Kreator migracji tworzy nową zasadę, która scala ustawienia zasad Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Na liście zasad wybierz zasady Kaspersky Endpoint Agent, których ustawienia chcesz scalić z zasadą Kaspersky Endpoint Security. Kliknij zasadę Kaspersky Endpoint Agent, aby wybrać zasadę Kaspersky Endpoint Security, z którą chcesz scalić ustawienia. Upewnij się, że wybrałeś poprawne zasady i przejdź do następnego kroku.

Krok 2. Migracja zadania

Kreator migracji tworzy nowe zadania dla Kaspersky Endpoint Security. Na liście zadań wybierz zadania Kaspersky Endpoint Agent, które chcesz utworzyć dla zasady Kaspersky Endpoint Security. Przejdź do następnego kroku.

Krok 3. Kończenie działania kreatora

Zakończ działanie Kreatora. W rezultacie kreator wykona następujące czynności:

- Utworzy nową zasadę Kaspersky Endpoint Security.

  Zasada scala ustawienia z Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Zasada zostaje nazwana *<Nazwa zasady Kaspersky Endpoint Security> & <Nazwa zasady Kaspersky Endpoint Agent>*. Nowa zasada posiada stan *Nieaktywny*. Aby kontynuować, zmień stany zasad Kaspersky Endpoint Agent i Kaspersky Endpoint Security na *Nieaktywny* i aktywuj nową scaloną zasadę.

  Po migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows upewnij się, że nowa zasada posiada funkcjonalność przesyłania danych do Serwera administracyjnego (dane pliku poddanego kwarantannie oraz dane łańcucha rozwoju zagrożeń). Wartości parametrów przesyłania danych nie zostają przeniesione z zasady Kaspersky Endpoint Agent.

- Utworzy nowe zadania Kaspersky Endpoint Security.

  Nowe zadania są kopiami zadań Kaspersky Endpoint Agent. Jednocześnie kreator pozostawia zadania Kaspersky Endpoint Agent niezmienione.

3 Udzielanie licencji funkcjonalności EDR Optimum

Jeśli do aktywowania Kaspersky Endpoint Security for Windows i Kaspersky Endpoint Agent używasz wspólnej licencji dla Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security, funkcjonalność EDR Optimum zostanie aktywowana automatycznie po zaktualizowaniu aplikacji do wersji 11.7.0 lub nowszej. Nie musisz robić nic innego.

Jeśli do aktywowania funkcjonalności EDR Optimum używasz autonomicznej licencji Kaspersky Endpoint Detection and Response Optimum Add-on, musisz upewnić się, że klucz EDR Optimum zostanie dodany do repozytorium Kaspersky Security Center, a funkcjonalność automatycznej dystrybucji klucza licencyjnego zostanie włączona. Po zaktualizowaniu aplikacji do wersji 11.7.0 lub nowszej, funkcjonalność EDR Optimum zostanie aktywowana automatycznie.

Jeśli do aktywowania Kaspersky Endpoint Agent użyjesz licencji dla Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security, a do aktywowania Kaspersky Endpoint Security for Windows użyjesz innej licencji, musisz zastąpić klucz Kaspersky Endpoint Security for Windows standardowym kluczem Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security. Możesz zastąpić klucz przy użyciu zadania *Dodaj klucz*.

4. **Instalacja / aktualizacja aplikacji Kaspersky Endpoint Security**

   Aby przeprowadzić migrację funkcjonalności EDR Optimum podczas instalacji lub aktualizacji aplikacji, zaleca się użycie zadania zdalnej instalacji. Podczas tworzenia zadania zdalnej instalacji należy wybrać komponent EDR Optimum w ustawieniach pakietu instalacyjnego.

   Możesz także zaktualizować aplikację za pomocą następujących metod:

   - Przy użyciu usługi aktualizacji Kaspersky.
   - Lokalnie, za pomocą Kreatora instalacji.

   Kaspersky Endpoint Security obsługuje automatyczne wybieranie komponentów podczas aktualizacji aplikacji na komputerze z zainstalowaną aplikacją Kaspersky Endpoint Agent. Automatyczne wybieranie komponentów zależy od uprawnień konta użytkownika, które aktualizuje aplikację.

   Jeśli aktualizujesz Kaspersky Endpoint Security przy użyciu pliku EXE lub MSI z poziomu konta systemowego (SYSTEM), Kaspersky Endpoint Security uzyskuje dostęp do bieżących licencji rozwiązań firmy Kaspersky. Dlatego też, jeśli na komputerze jest, na przykład, zainstalowany Kaspersky Endpoint Agent i aktywowane rozwiązanie EDR Optimum, instalator Kaspersky Endpoint Security automatycznie konfiguruje zestaw komponentów i wybiera komponent EDR Optimum. To powoduje przełączenie Kaspersky Endpoint Security na używanie wbudowanego agenta i usunięcie Kaspersky Endpoint Agent. Uruchomienie instalatora MSI z poziomu konta systemowego (SYSTEM) jest zazwyczaj wykonywane podczas aktualizacji za pośrednictwem usługi aktualizacji Kaspersky lub podczas wdrażania pakietu instalacyjnego za pośrednictwem Kaspersky Security Center.

   Jeśli aktualizujesz Kaspersky Endpoint Security przy użyciu pliku MSI z poziomu konta użytkownika bez uprawnień, Kaspersky Endpoint Security nie ma dostępu do bieżących licencji dla rozwiązań Kaspersky. W tym przypadku Kaspersky Endpoint Security automatycznie wybiera komponenty w oparciu o konfigurację Kaspersky Endpoint Agent. Następnie Kaspersky Endpoint Security przełączy się na korzystanie z wbudowanego agenta i usunie Kaspersky Endpoint Agent.

   > Kaspersky Endpoint Security obsługuje aktualizację bez ponownego uruchamiania komputera. Możesz wybrać tryb aktualizacji aplikacji we właściwościach zasad.

5. **Sprawdzanie działania aplikacji**

   Jeśli po instalacji lub aktualizacji aplikacji komputer posiada stan *Krytyczny* w konsoli Kaspersky Security Center:

   - Upewnij się, że na komputerze jest zainstalowany Agent sieciowy w wersji 13.2 lub wyższej.
   - Sprawdź stan działania komponentów, przeglądając *Raport o stanie składników aplikacji*. Jeśli komponent ma stan *Nie zainstalowano*, zainstaluj komponent przy użyciu zadania *Zmiana składników aplikacji*. Jeśli komponent ma stan *Nieobjęte licencją*, upewnij się, że aktywowano wbudowaną funkcję agenta.
   - Upewnij się, że akceptujesz Oświadczenie Kaspersky Security Network w nowej zasadzie Kaspersky Endpoint Security for Windows.

Kaspersky Sandbox



Kaspersky Endpoint Security for Windows zawiera wbudowanego agenta do integracji z rozwiązaniem Kaspersky Sandbox. Komponent *Sandbox* wykrywa i automatycznie blokuje zaawansowane zagrożenia na komputerach. Sandbox analizuje zachowanie obiektów w celu wykrywania szkodliwej aktywności oraz aktywności charakterystycznej dla ataków docelowych ukierunkowanych na infrastrukturę IT organizacji. Sandbox analizuje i skanuje obiekty na specjalnych serwerach z wdrożonymi obrazami wirtualnymi systemów operacyjnych Microsoft Windows (serwery Sandbox). Szczegółowe informacje na temat rozwiązania można znaleźć w systemie pomocy dla Kaspersky Sandbox i dla Kaspersky Anti Targeted Attack Platform.

Integracja wbudowanego agenta z ze środowiskiem testowym "Kaspersky Sandbox"

Dodawanie komponentu Sandbox jest wymagane do integracji z komponentem Kaspersky Sandbox. Możesz wybrać składnik Sandbox podczas instalacji lub aktualizacji, a także przy użyciu zadania *Zmiana składników aplikacji*.

W celu użycia komponentu spełnione muszą być następujące warunki:

- Kaspersky Security Center 13.2. Wcześniejsze wersje Kaspersky Security Center nie pozwalają na utworzenie autonomicznych zadań Skanowanie IOC w celu reakcji na zagrożenia.
- Komponent może być zarządzany tylko przy użyciu konsoli Web Console. Nie możesz zarządzać tym komponentem przy użyciu Konsoli administracyjnej (MMC).
- Aplikacja jest aktywowana, a funkcjonalność jest objęta licencją.
- Przesyłanie danych do Serwera administracyjnego jest włączone.

  Aby użyć wszystkich funkcji Kaspersky Sandbox, upewnij się, że przesyłanie danych pliku poddanego kwarantannie jest włączone. Dane są wymagane do uzyskania informacji o plikach poddanych kwarantannie na komputerze za pośrednictwem Web Console. Na przykład, możesz pobrać plik z kwarantanny do analizy w Web Console.

  Jak włączyć przesyłanie danych do Serwera administracyjnego w Web Console?

  1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
  2. Kliknij nazwę zasady Kaspersky Endpoint Security.

     Zostanie otwarte okno właściwości profilu.
  3. Wybierz zakładkę **Ustawienia aplikacji**.
  4. Wybierz **Ustawienia ogólne** → **Integracja KSC**.
  5. W sekcji **Przesyłanie danych do Serwera administracyjnego** zaznacz pole **Informacje o plikach Kwarantanny**.
  6. Zapisz swoje zmiany.
- Połączenia w tle między Kaspersky Security Center Web Console a Serwerem administracyjnym zostało nawiązane

Aby rozwiązanie Kaspersky Sandbox działało z Serwerem administracyjnym poprzez Kaspersky Security Center Web Console, należy nawiązać nowe bezpieczne połączenie - *połączenie w tle*. Więcej informacji o integracji Kaspersky Security Center z innymi rozwiązaniami Kaspersky można znaleźć w pomocy dla Kaspersky Security Center.

Nawiązywanie połączenia w tle w Web Console

1. W oknie głównym Web Console wybierz **Ustawienia** → **Integracja**.
2. Przejdź do sekcji **Integracja**.
3. Włącz przełącznik **Połączenie w tle w celu integracji Włączone**.
4. Zapisz swoje zmiany.

Jeśli połączenie w tle między Kaspersky Security Center Web Console a Serwerem administracyjnym nie zostanie nawiązane, autonomiczne zadania skanowania IOC nie może zostać utworzone jako część Threat Response.

- Aby skonfigurować zaufane połączenie z serwera Sandbox, musisz przygotować certyfikat TLS. Następnie należy dodać certyfikat do komputera, stosując zasady. Należy również dodać certyfikat do serwera Sandbox.

  Uwierzytelnianie dwukierunkowe przy użyciu kontenera szyfrowania nie jest dostępne w przypadku Kaspersky Sandbox.

  Możesz także dodać certyfikat TLS w Web Console lub lokalnie przy użyciu wiersza polecenia.

- Komponent Kaspersky Sandbox jest włączony.
- Komponenty aplikacji zapewniające działanie platformy Sandbox są włączone i działają. Działanie platformy Sandbox zapewniają następujące komponenty:
  - Ochrona plików.
  - Ochrona przed włamaniami.
  - Zapora sieciowa.
  - Ochrona AMSI.
  - Skanowanie w tle.

W celu włączenia lub wyłączenia integracji z Kaspersky Sandbox:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Sandbox**.
5. Użyj przełącznika **Integracja z Sandbox WŁĄCZONA**, aby włączyć lub wyłączyć komponent.

6. W sekcji **Tryb integracji** wybierz tryb działania komponentu: **Kaspersky Sandbox**.

7. Kliknij odnośnik **Ustawienia połączenia**.

   To spowoduje otwarcie okna ustawień połączenia z serwerem Sandbox.

8. W sekcji **Certyfikat TLS serwera** kliknij **Wczytaj** i wybierz plik certyfikatu TLS.

   Kaspersky Endpoint Security może mieć tylko jeden certyfikat TLS dla serwera Sandbox. Jeśli wcześniej dodałeś certyfikat TLS, ten certyfikat zostanie odwołany. Używany jest tylko ostatnio dodany certyfikat.

9. Skonfiguruj zaawansowane ustawienia połączenia dla serwerów Sandbox:

   - **Limit czasu (ms)**. Limit czasu połączenia dla serwera Sandbox został przekroczony. Po skonfigurowaniu upłynięcia określonej ilości czasu, Kaspersky Endpoint Security wyśle żądanie do następnego serwera. Możesz zwiększyć limit czasu połączenia dla serwera, jeśli prędkość Twojego połączenia spada lub jeśli połączenie jest niestabilne. Zalecany limit czasu żądania wynosi 0,5 sekundy lub mniej.

   - **Kolejka żądań**. Rozmiar folderu kolejki żądań. Podczas wysyłania kilku obiektów do skanowania w Sandbox Kaspersky Endpoint Security tworzy kolejkę żądań. Domyślnie, rozmiar folderu kolejki żądań jest ograniczony do 100 MB. Po osiągnięciu maksymalnego rozmiaru, Sandbox przestanie dodawać nowe żądania do kolejki i wyśle odpowiednie zdarzenie do Kaspersky Security Center. Możesz skonfigurować rozmiar folderu kolejki żądań w zależności od konfiguracji Twojego serwera.

10. W sekcji **Połączenie z serwerami Sandbox** kliknij przycisk **Dodaj**.

11. To okno zostanie otwarte; w tym oknie wprowadź port i adres serwera Sandbox (IPv4, IPv6, DNS).

    Więcej informacji dotyczących wdrożenia obrazów wirtualnych i skonfigurowania serwerów Sandbox można znaleźć w pomocy dla Kaspersky Sandbox.

12. Zapisz swoje zmiany.

W wyniku tego program Kaspersky Endpoint Security będzie sprawdzał certyfikat TLS. Jeśli certyfikat zostanie pomyślnie zweryfikowany, Kaspersky Endpoint Security wczyta plik certyfikatu do komputera podczas kolejnej synchronizacji z Kaspersky Security Center. Jeśli dodałeś dwa certyfikaty TLS, Kaspersky Sandbox użyje najnowszego certyfikatu do nawiązania zaufanego połączenia. Sprawdź stan działania komponentu, przeglądając *Raport o stanie składników aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Sandbox** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

Możesz włączyć lub wyłączyć integrację z Kaspersky Sandbox w Web Console lub lokalnie przy użyciu wiersza poleceń.

Kaspersky Endpoint Security zapisuje informacje o działaniu komponentu Kaspersky Sandbox do raportu. Raport zawiera także informacje o błędach. Jeśli uzyskasz błąd z opisem odpowiadający `Error code: XXX` (na przykład: `0xa67b01f4`), skontaktuj się z Działem pomocy technicznej.

Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa (zadanie autonomiczne)

Wskaźnik naruszeń bezpieczeństwa (IOC) to zestaw danych dotyczących obiektu lub aktywności, która wskazuje nieautoryzowany dostęp do komputera (naruszenie bezpieczeństwa danych). Na przykład, wiele niepomyślnych prób zalogowania do systemu może stanowić wskaźnik naruszeń bezpieczeństwa. Zadanie *Skanowanie IOC* umożliwia odszukanie wskaźników naruszeń bezpieczeństwa na komputerze i podejmują środki reakcji na zagrożenia.

Kaspersky Endpoint Security wyszukuje wskaźniki zagrożenia za pomocą plików IOC. *Pliki IOC* to pliki zawierające zestawy wskaźników, które aplikacja próbuje dopasować do licznika wykrywania. Pliki IOC muszą pasować do standardu OpenIOC. Kaspersky Endpoint Security automatycznie generuje pliki IOC dla Kaspersky Sandbox.

Tryb uruchamiania zadania Skanowanie IOC

Aplikacja tworzy autonomiczne zadania skanowania IOC dla Kaspersky Sandbox. *Autonomiczne zadanie skanowania IOC* to zadanie grupowe, które jest tworzone automatycznie podczas reagowania na zagrożenie wykryte przez Kaspersky Sandbox. Kaspersky Endpoint Security automatycznie generuje plik IOC. Niestandardowe pliki IOC nie są obsługiwane. Zadania są automatycznie usuwane 30 dni po czasie utworzenia. Więcej informacji o autonomicznych zadaniach skanowania IOC możesz znaleźć w pomocy dla Kaspersky Sandbox.

Ustawienia zadania Skanowanie IOC

Kaspersky Sandbox może tworzyć i uruchamiać zadania *Skanowanie IOC* automatycznie po reakcji na zagrożenia.

Możesz skonfigurować ustawienia tylko w Web Console.

Potrzebujesz Kaspersky Security Center 13.2 do działania autonomicznych zadań skanowania IOC dla Kaspersky Sandbox.

W celu zmiany ustawień zadania Skanowanie IOC:

1. W oknie głównym Web Console wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij zadanie **Skanowanie IOC** Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości zadania.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Przejdź do sekcji **Ustawienia skanowania IOC**.

5. Skonfiguruj akcje po wykryciu IOC:

- **Przenieś kopię do Kwarantanny, usuń obiekt**. Jeśli ta opcja została zaznaczona, Kaspersky Endpoint Security usunie szkodliwy obiekt wykryty na komputerze. Przed usunięciem obiektu Kaspersky Endpoint Security utworzy kopię zapasową w przypadku, gdy obiekt musi zostać przywrócony w późniejszym czasie. Kaspersky Endpoint Security przeniesie kopię zapasową do Kwarantanny.

- **Uruchom skanowanie obszarów krytycznych**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security uruchamia zadanie *Skanowanie obszarów krytycznych*. Domyślnie, Kaspersky Endpoint Security skanuje pamięć jądra, uruchomione procesy i sektory startowe dysku.

- **Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności**. Odroczono uruchomienie zadania, gdy zasoby komputera są zajęte. Kaspersky Endpoint Security uruchamia zadanie skanowania, jeśli komputer jest zablokowany lub wygaszacz ekranu jest włączony. Jeśli przerwałeś wykonywanie zadania, na przykład, poprzez odblokowanie komputera, Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane. Ta opcja terminarza umożliwia zaoszczędzenie zasobów komputera w trakcie korzystania z komputera.

6. Zapisz swoje zmiany.

Możesz przejrzeć wyniki zadania we właściwościach zadania, w sekcji **Wyniki**. Informacje o wykrytych wskaźnikach naruszeń bezpieczeństwa możesz przejrzeć we właściwościach zadania: **Ustawienia aplikacji** → **Wyniki skanowania IOC**.

Wyniki skanowania IOC są przechowywane 30 dni. Po tym czasie Kaspersky Endpoint Security automatycznie usuwa najstarsze wpisy.

Przewodnik migracji z KEA do KES dla Kaspersky Sandbox

Kaspersky Endpoint Security for Windows zawiera wbudowanego agenta do rozwiązania Kaspersky Sandbox. Nie potrzebujesz już oddzielnej aplikacji Kaspersky Endpoint Agent do pracy z Kaspersky Sandbox. Wszystkie funkcje Kaspersky Endpoint Agent będą wykonywane przez Kaspersky Endpoint Security.

Podczas wdrażania Kaspersky Endpoint Security na komputerach, na których jest zainstalowany Kaspersky Endpoint Agent, rozwiązania Kaspersky Sandbox będą nadal działać z Kaspersky Endpoint Security. Dodatkowo, Kaspersky Endpoint Agent zostanie usunięty z komputera. To samo zachowanie w systemie wystąpi podczas aktualizacji Kaspersky Endpoint Security do wersji 11.7.0 lub nowszej.

Kaspersky Endpoint Security nie jest kompatybilny z Kaspersky Endpoint Agent. Obu tych aplikacji nie można zainstalować na tym samym komputerze.

Aby aplikacja Kaspersky Endpoint Security działała w ramach Kaspersky Sandbox, muszą być spełnione następujące warunki:

- Kaspersky Sandbox w wersji 2.0 lub nowszej.

- Kaspersky Security Center w wersji 13.2 lub nowszej (w tym Agent sieciowy). We wcześniejszych wersjach Kaspersky Security Center nie ma możliwości aktywowania funkcji Kaspersky Sandbox.

- Kaspersky Sandbox może być zarządzany tylko przy użyciu konsoli Kaspersky Security Center Web Console.

- Przesyłanie danych do Serwera administracyjnego jest włączone. Dane są wymagane do uzyskania informacji o plikach poddanych kwarantannie na komputerze za pośrednictwem Web Console.
- Połączenia w tle między Kaspersky Security Center Web Console a Serwerem administracyjnym zostało nawiązane. Aby rozwiązanie Kaspersky Sandbox działało z Serwerem administracyjnym poprzez Kaspersky Security Center Web Console, należy nawiązać nowe bezpieczne połączenie - *połączenie w tle*.

Kroki migracji konfiguracji [KES+KEA] do [KES+wbudowanego agenta] dla Kaspersky Sandbox

1. **Aktualizowanie wtyczki webowej Kaspersky Endpoint Security**

   Komponentem Kaspersky Sandbox można zarządzać przy użyciu wtyczki sieciowej Kaspersky Endpoint Security w wersji 11.7.0 lub nowszej.

2. **Migrowanie zasad i zadań**

   Przenieś ustawienia Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows. W tym celu użyj kreatora migracji z Kaspersky Endpoint Agent w Web Console.

   Jak dokonać migracji ustawień zasady i zadania z Kaspersky Endpoint Agent do Kaspersky Endpoint Security w Web Console:

   W oknie głównym Web Console wybierz **Operacje** → **Migracja z Kaspersky Endpoint Agent**.

   To spowoduje uruchomienie Kreatora migracji zasad i zadań. Postępuj zgodnie z instrukcjami Kreatora.

   Krok 1. Migracja zasady

   Kreator migracji tworzy nową zasadę, która scala ustawienia zasad Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Na liście zasad wybierz zasady Kaspersky Endpoint Agent, których ustawienia chcesz scalić z zasadą Kaspersky Endpoint Security. Kliknij zasadę Kaspersky Endpoint Agent, aby wybrać zasadę Kaspersky Endpoint Security, z którą chcesz scalić ustawienia. Upewnij się, że wybrałeś poprawne zasady i przejdź do następnego kroku.

   Krok 2. Migracja zadania

   Kreator migracji tworzy nowe zadania dla Kaspersky Endpoint Security. Na liście zadań wybierz zadania Kaspersky Endpoint Agent, które chcesz utworzyć dla zasady Kaspersky Endpoint Security. Przejdź do następnego kroku.

   Krok 3. Kończenie działania kreatora

   Zakończ działanie Kreatora. W rezultacie kreator wykona następujące czynności:

   - Utworzy nową zasadę Kaspersky Endpoint Security.

Zasada scala ustawienia z Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Zasada zostaje nazwana *<Nazwa zasady Kaspersky Endpoint Security> & <Nazwa zasady Kaspersky Endpoint Agent>*. Nowa zasada posiada stan *Nieaktywny*. Aby kontynuować, zmień stany zasad Kaspersky Endpoint Agent i Kaspersky Endpoint Security na *Nieaktywny* i aktywuj nową scaloną zasadę.

Po migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows upewnij się, że nowa zasada posiada funkcjonalność przesyłania danych do Serwera administracyjnego (dane pliku poddanego kwarantannie oraz dane łańcucha rozwoju zagrożeń). Wartości parametrów przesyłania danych nie zostają przeniesione z zasady Kaspersky Endpoint Agent.

- Utworzy nowe zadania Kaspersky Endpoint Security.

  Nowe zadania są kopiami zadań Kaspersky Endpoint Agent. Jednocześnie kreator pozostawia zadania Kaspersky Endpoint Agent niezmienione.

3 Licencjonowanie funkcjonalności Kaspersky Sandbox

Aby aktywować Kaspersky Endpoint Security jako część rozwiązania Kaspersky Sandbox, potrzebujesz osobnej licencji na dodatek Kaspersky Sandbox. Możesz dodać klucz przy użyciu zadania *Dodaj klucz*. W rezultacie do aplikacji zostaną dodane dwa klucze: *Kaspersky Endpoint Security* i *Kaspersky Sandbox*.

4 Instalacja / aktualizacja aplikacji Kaspersky Endpoint Security

Aby przeprowadzić migrację funkcjonalności Kaspersky Sandbox podczas instalacji lub aktualizacji aplikacji, zaleca się użycie zadania zdalnej instalacji. Podczas tworzenia zadania zdalnej instalacji należy wybrać komponent Kaspersky Sandbox w ustawieniach pakietu instalacyjnego.

Możesz także zaktualizować aplikację za pomocą następujących metod:

- Przy użyciu usługi aktualizacji Kaspersky.
- Lokalnie, za pomocą Kreatora instalacji.

Kaspersky Endpoint Security obsługuje automatyczne wybieranie komponentów podczas aktualizacji aplikacji na komputerze z zainstalowaną aplikacją Kaspersky Endpoint Agent. Automatyczne wybieranie komponentów zależy od uprawnień konta użytkownika, które aktualizuje aplikację.

Jeśli aktualizujesz Kaspersky Endpoint Security przy użyciu pliku EXE lub MSI z poziomu konta systemowego (SYSTEM), Kaspersky Endpoint Security uzyskuje dostęp do bieżących licencji rozwiązań firmy Kaspersky. Dlatego też, jeśli na komputerze jest, na przykład, zainstalowany Kaspersky Endpoint Agent i aktywowane rozwiązanie Kaspersky Sandbox, instalator Kaspersky Endpoint Security automatycznie konfiguruje zestaw komponentów i wybiera komponent Kaspersky Sandbox. To powoduje przełączenie Kaspersky Endpoint Security na używanie wbudowanego agenta i usunięcie Kaspersky Endpoint Agent. Uruchomienie instalatora MSI z poziomu konta systemowego (SYSTEM) jest zazwyczaj wykonywane podczas aktualizacji za pośrednictwem usługi aktualizacji Kaspersky lub podczas wdrażania pakietu instalacyjnego za pośrednictwem Kaspersky Security Center.

Jeśli aktualizujesz Kaspersky Endpoint Security przy użyciu pliku MSI z poziomu konta użytkownika bez uprawnień, Kaspersky Endpoint Security nie ma dostępu do bieżących licencji dla rozwiązań Kaspersky. W tym przypadku Kaspersky Endpoint Security automatycznie wybiera komponenty w oparciu o konfigurację Kaspersky Endpoint Agent. Następnie Kaspersky Endpoint Security przełączy się na korzystanie z wbudowanego agenta i usunie Kaspersky Endpoint Agent.

Kaspersky Endpoint Security obsługuje aktualizację bez ponownego uruchamiania komputera. Możesz wybrać tryb aktualizacji aplikacji we właściwościach zasad.

5 Sprawdzanie działania aplikacji

Jeśli po instalacji lub aktualizacji aplikacji komputer posiada stan *Krytyczny* w konsoli Kaspersky Security Center:

- Upewnij się, że na komputerze jest zainstalowany Agent sieciowy w wersji 13.2 lub wyższej.
- Sprawdź stan działania komponentów, przeglądając *Raport o stanie składników aplikacji*. Jeśli komponent ma stan *Nie zainstalowano*, zainstaluj komponent przy użyciu zadania *Zmiana składników aplikacji*. Jeśli komponent ma stan *Nieobjęte licencją*, upewnij się, że aktywowano wbudowaną funkcję agenta.
- Upewnij się, że akceptujesz Oświadczenie Kaspersky Security Network w nowej zasadzie Kaspersky Endpoint Security for Windows.

Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Security for Windows obsługuje współpracę z rozwiązaniem Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* to rozwiązanie zaprojektowane w celu szybkiego wykrywania złożonych zagrożeń, takich jak ataki ukierunkowane, zaawansowane trwałe zagrożenia (APT), ataki zero-day i inne. Kaspersky Anti Targeted Attack Platform składa się z trzech jednostek funkcjonalnych:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Można zakupić wszystkie jednostki funkcjonalne lub poszczególne jednostki funkcjonalne osobno. Szczegółowe informacje na temat rozwiązania można znaleźć w systemie pomocy dla Kaspersky Anti Targeted Attack Platform. Aplikacja zawiera wbudowanych agentów dla komponentów EDR, NDR. Aplikacja obsługuje również pracę z komponentem Sandbox, który jest częścią KATA.

Narzędzia analizy zagrożeń

Kaspersky Endpoint Detection and Response używa następujących narzędzi Threat Intelligence:

- Integracja z portalem Kaspersky Threat Intelligence Portal, który zawiera i wyświetla informacje o reputacji plików i adresów sieciowych.
- Baza danych Kaspersky Threats.
- Infrastruktura usługi chmury Kaspersky Security Network (zwana dalej również „KSN"), która zapewnia dostęp do informacji o reputacji pliku, strony internetowej i oprogramowania w czasie rzeczywistym z bazy wiedzy Kaspersky. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji firmy Kaspersky na zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie prawdopodobieństwa wystąpienia fałszywych alarmów.

Zasada działania rozwiązania

Aplikacja Kaspersky Endpoint Security jest instalowana na pojedynczych komputerach w korporacyjnej infrastrukturze IT i cały czas monitoruje procesy, otwiera połączenia sieciowe i modyfikowane pliki. Informacje o zdarzeniach na komputerze (dane telemetryczne) są wysyłane na serwer Kaspersky Anti Targeted Attack Platform. W takim przypadku Kaspersky Endpoint Security wysyła również informacje do serwera Kaspersky Anti Targeted Attack Platform o zagrożeniach wykrytych przez aplikację oraz informacje o wynikach przetwarzania tych zagrożeń.

Integracja EDR (KATA) i NDR (KATA) jest konfigurowana na konsoli Kaspersky Security Center. Wbudowany agent jest następnie zarządzany przy użyciu konsoli Kaspersky Anti Targeted Attack Platform, w tym uruchamianie zadań, zarządzanie obiektami poddanymi kwarantannie, przeglądanie raportów i inne działania.

Konfiguracje Kaspersky Endpoint Security do pracy z EDR / NDR (KATA)

Do pracy z EDR / NDR (KATA) można zastosować następujące konfiguracje:

- **[KES+wbudowany agent]**. W tej konfiguracji Kaspersky Endpoint Security działa zarówno jako aplikacja zapewniająca bezpieczeństwo komputera, jak i aplikacja do pracy z EDR / NDR (KATA). Wbudowany agent EDR (KATA) jest dostępny w programie Kaspersky Endpoint Security 12.1 for Windows lub nowszym. Wbudowany agent NDR (KATA) jest dostępny w programie Kaspersky Endpoint Security 12.7 for Windows lub nowszym.

- **[zewnętrzny agent EPP+EDR]**. W tej konfiguracji bezpieczeństwo infrastruktury IT zapewnia zewnętrzna platforma Endpoint Protection Platform (EPP). Interakcja z EDR / NDR (KATA) jest zapewniana przez Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent (EDR Agent). W tej konfiguracji EDR Agent jest kompatybilny z aplikacjami EPP innych firm. EDR Agent dla EDR (KATA) jest dostępny w Kaspersky Endpoint Security 12.3 for Windows lub nowszym. EDR Agent dla NDR (KATA) jest dostępny w Kaspersky Endpoint Security 12.7 for Windows lub nowszym.

Obsługa poprzednich wersji Kaspersky Endpoint Security

Jeśli używasz Kaspersky Endpoint Security 11.2.0–11.8.0 do współdziałania z Kaspersky Anti Targeted Attack Platform (EDR), aplikacja zawiera Kaspersky Endpoint Agent. Możesz zainstalować Kaspersky Endpoint Agent wraz z Kaspersky Endpoint Security.

Jeśli używasz Kaspersky Endpoint Security 11.9.0–12.0, musisz zainstalować Kaspersky Endpoint Agent oddzielnie, ponieważ począwszy od Kaspersky Endpoint Security 11.9.0 pakiet dystrybucyjny Kaspersky Endpoint Agent nie jest już częścią zestawu dystrybucyjnego Kaspersky Endpoint Security.

Integracja wbudowanego agenta z EDR / NDR (KATA)

Aby uzyskać integrację z EDR/NDR (KATA), należy dodać odpowiedni komponent: Endpoint Detection and Response (KATA) lub Network Detection and Response (KATA). Możesz wybrać komponent do integracji z EDR / NDR (KATA) podczas instalacji lub aktualizacji, a także przy użyciu zadania *Zmiana składników aplikacji*.

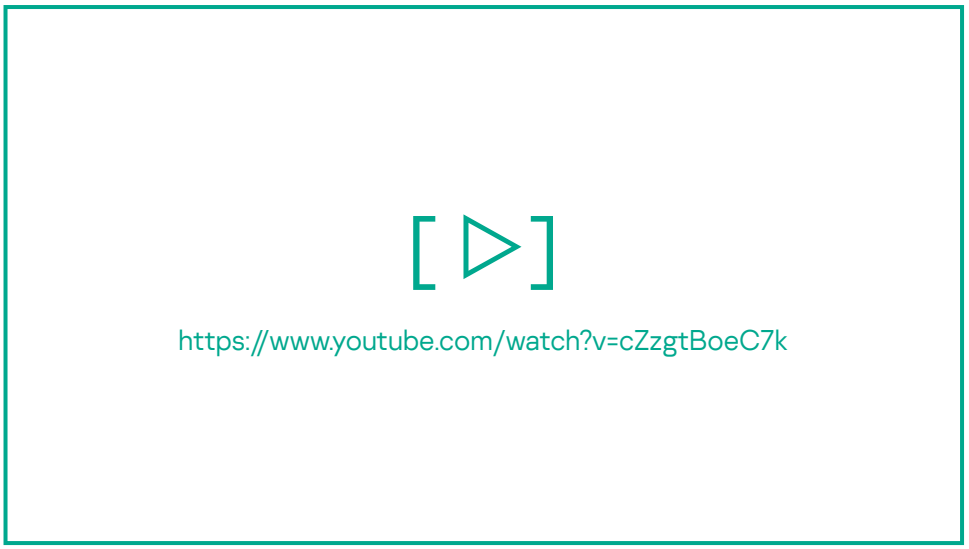
Od wersji 12.11 Kaspersky Endpoint Security for Windows nazwa komponentu EDR (KATA) została zmieniona na **Endpoint Detection and Response Expert (wersja 8.0 lub nowsze)**. W tej wersji aplikacji komponent jest kompatybilny z Kaspersky Anti Targeted Attack Platform 7.1 i starszymi wersjami, a także z Kaspersky Endpoint Detection and Response Expert (on-premises).

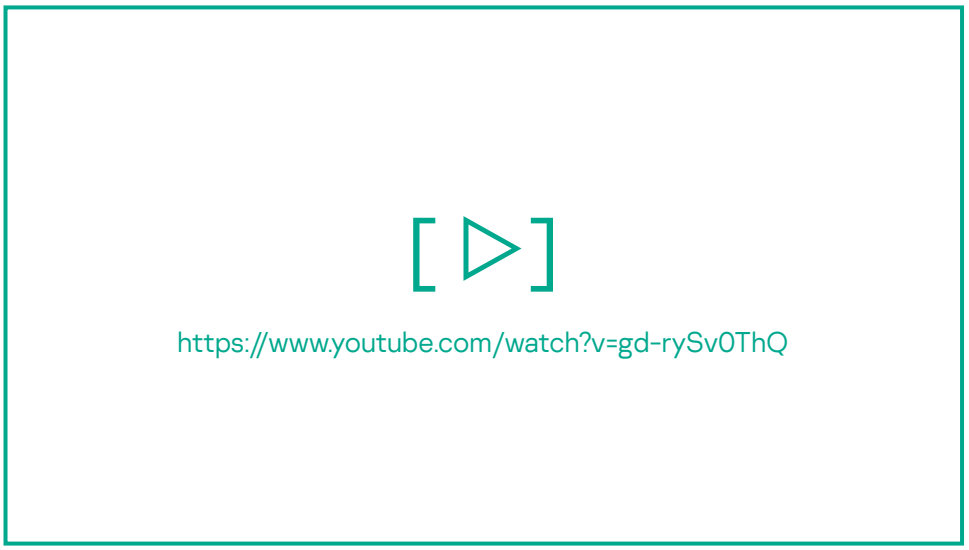
Komponenty Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) i Endpoint Detection and Response Expert (on-premises) nie są ze sobą kompatybilne.

W celu użycia platformy EDR / NDR (KATA) spełnione muszą być następujące warunki:

- EDR (KATA): Kaspersky Anti Targeted Attack Platform w wersjach 5.0–7.1.
- NDR (KATA): Kaspersky Anti Targeted Attack Platform w wersji 7.0 lub nowszej.
- EDR (KATA): Kaspersky Endpoint Security for Windows w wersji 12.1 lub nowszej. Aby uzyskać więcej informacji na temat zgodności KATA z różnymi wersjami Kaspersky Endpoint Security, zapoznaj się z pomocą dla Kaspersky Anti Targeted Attack Platform.
- NDR (KATA): Kaspersky Endpoint Security for Windows w wersji 12.7 lub nowszej.
- Kaspersky Security Center w wersji 14.2 lub nowszej. We wcześniejszych wersjach Kaspersky Security Center nie ma możliwości aktywowania funkcjonalności integracji platformy EDR / NDR (KATA).
- Aplikacja jest aktywowana, a funkcjonalność jest objęta licencją.
- Komponenty Endpoint Detection and Response (KATA) oraz Network Detection and Response (KATA) są włączone.
- Komponenty aplikacji zapewniające działanie EDR/NDR (KATA) są włączone i działają. Działanie EDR / NDR (KATA) zapewniają następujące komponenty:
  - Ochrona plików.
  - Ochrona WWW.
  - Ochrona poczty.
  - Ochrona przed exploitami.
  - Wykrywanie zachowań.
  - Ochrona przed włamaniami.
  - Ochrona AMSI.

- Skanowanie w tle.
- Kaspersky Security Network.





Integracja z Endpoint Detection and Response (KATA) obejmuje następujące etapy:

1. **Instalowanie komponentów Endpoint Detection and Response (KATA) oraz Network Detection and Response (KATA)**

   Możesz wybrać komponent EDR (KATA) i NDR (KATA) podczas instalacji lub aktualizacji, a także przy użyciu zadania *Zmiana składników aplikacji*.

   > Musisz ponownie uruchomić komputer, aby dokończyć aktualizację aplikacji o nowe komponenty.

2. **Aktywacja Endpoint Detection and Response (KATA) i Network Detection and Response (KATA)**

   W celu korzystania z EDR (KATA) i NDR (KATA) musisz zakupić osobną licencję (na przykład dodatek Kaspersky Endpoint Detection and Response (KATA)).

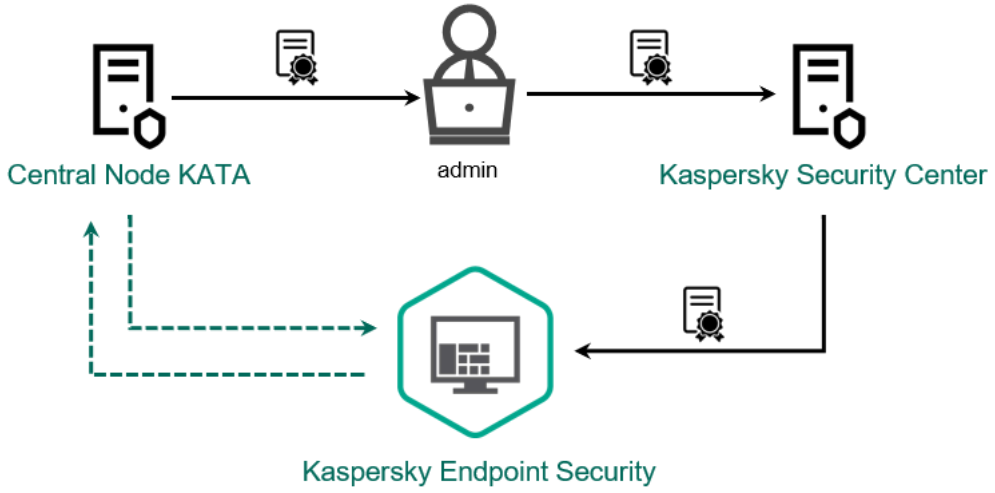
   Funkcjonalność ta będzie dostępna po dodaniu oddzielnego klucza obejmującego funkcjonalność EDR (KATA) i NDR (KATA). W rezultacie na komputerze dodanych zostanie kilka kluczy: klucz dla Kaspersky Endpoint Security i klucze dla Kaspersky Endpoint Detection and Response (KATA) i Network Detection and Response (KATA).

   Zasady udzielania licencji dla autonomicznej funkcjonalności EDR (KATA) i NDR (KATA) są takie same jak w przypadku udzielania licencji dla Kaspersky Endpoint Security.

   Upewnij się, że funkcjonalność EDR (KATA) i NDR (KATA) znajduje się w licencji i jest uruchomiona w lokalnym interfejsie aplikacji.

3 Łączenie z węzłem centralnym

Kaspersky Anti Targeted Attack Platform wymaga ustanowienia zaufanego połączenia między Kaspersky Endpoint Security a komponentem Central Node. Aby skonfigurować zaufane połączenie, musisz użyć certyfikatu TLS. Możesz uzyskać certyfikat TLS w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w Pomoc Kaspersky Anti Targeted Attack Platform). Następnie musisz dodać certyfikat TLS do Kaspersky Endpoint Security (zobacz instrukcje poniżej).



Dodanie certyfikatu TLS do Kaspersky Endpoint Security

Domyślnie Kaspersky Endpoint Security sprawdza tylko certyfikat TLS węzła centralnego. Aby połączenie było bezpieczniejsze, możesz dodatkowo włączyć weryfikację komputera na Węźle Centralnym (uwierzytelnianie dwukierunkowe). Aby włączyć tę weryfikację, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach węzła centralnego i Kaspersky Endpoint Security. Aby korzystać z uwierzytelniania dwukierunkowego, potrzebujesz również kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform).

Jak połączyć komputer Kaspersky Endpoint Security z Węzłem centralnym przy użyciu Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasad wybierz **Detection and Response** i wybierz komponent, który chcesz skonfigurować: **Endpoint Detection and Response Expert (on-premises)** lub **Network Detection and Response (KATA)**.
5. Zaznacz odpowiednie pole wyboru: **Endpoint Detection and Response Expert (wersja 7.1 lub starsze)** lub **Network Detection and Response (KATA)**.
6. Kliknij **Ustawienia połączenia z serwerem**.
7. Skonfiguruj połączenie z serwerem:
   - **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera węzła centralnego. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem węzła centralnego.
   - **Certyfikat TLS serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem Central Node. Możesz uzyskać certyfikat TLS w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w Pomoc Kaspersky Anti Targeted Attack Platform).

- **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem Central Node. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera Central Node, a następnie uzyskać kontener szyfrowania i ustawić hasło chroniące kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform). Po skonfigurowaniu ustawień węzła centralnego należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny.

  Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.

8. Kliknij **OK**.
9. Dodaj serwery węzła centralnego. W tym celu należy określić adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.

   Można dodać wiele adresów serwera węzła centralnego. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.
10. W razie potrzeby skonfiguruj telemetrię.
11. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak połączyć komputer Kaspersky Endpoint Security z węzłem centralnym przy użyciu Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do sekcji **Konfiguracja wbudowanych agentów** i wybierz komponent, który chcesz skonfigurować: **Endpoint Detection and Response Expert (on-premise)** lub **Network Detection and Response (KATA)**.
5. Włącz odpowiedni przełącznik: **Endpoint Detection and Response Expert (on-premise) WŁĄCZONO** lub **Network Detection and Response (KATA) WŁĄCZONE**.
6. Aby skonfigurować EDR (KATA), wybierz **Endpoint Detection and Response Expert (wersja 7.1 lub starsze)** z listy rozwiązań.
7. Kliknij **Ustawienia połączenia**.
8. Skonfiguruj połączenie z serwerem:

   - **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera węzła centralnego. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem węzła centralnego.
   - **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem Central Node. Możesz uzyskać certyfikat TLS w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w Pomoc Kaspersky Anti Targeted Attack Platform).

- **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem Central Node. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera Central Node, a następnie uzyskać kontener szyfrowania i ustawić hasło chroniące kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform). Po skonfigurowaniu ustawień węzła centralnego należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny.

  Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.

9. Kliknij **OK**.
10. Dodaj serwery węzła centralnego. W tym celu należy określić adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.

    Można dodać wiele adresów serwera węzła centralnego. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.
11. W razie potrzeby skonfiguruj telemetrię.
12. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Możesz także dodać certyfikat TLS lokalnie przy użyciu wiersza polecenia.

W rezultacie komputer zostanie dodany do konsoli Kaspersky Anti Targeted Attack Platform. Sprawdź stan działania komponentów, przeglądając *Raport o stanie składników aplikacji*. Stan działania komponentów można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponenty **Endpoint Detection and Response Expert (wersja 8.0 lub nowsze)** i **Network Detection and Response (KATA)** zostaną dodane do listy komponentów Kaspersky Endpoint Security.

Stan komponentów można sprawdzić w konsoli Kaspersky Security Center we właściwościach komputera w sekcji **Komponenty**. Sprawdzając status komponentu w konsoli, należy wziąć pod uwagę poniższe kwestie. Jeżeli komponent nie jest zainstalowany i jego funkcjonalność nie jest objęta licencją, w konsoli zostanie wyświetlony komunikat **Nieobsługiwane przez licencję** zamiast **Nie zainstalowano**.

Począwszy od Kaspersky Endpoint Security 12.6 for Windows, możesz monitorować stan komponentu EDR (KATA) w konsoli administracyjnej Kaspersky Security Center Administration Console (MMC). Bieżący status komponentu jest wyświetlany we właściwościach komputera w kolumnie **Stan czujnika Endpoint Sensor** (*Uruchomiona*, *Uruchamianie*, *Zatrzymano*, *Wstrzymana*, *Niepowodzenie*, *Nieznany*). Konsola Web Console nie wyświetla statusu Endpoint Sensor.

Konfiguracja telemetrii EDR (KATA)

Telemetria to lista zdarzeń, które wystąpiły na chronionym komputerze. Kaspersky Endpoint Security analizuje dane telemetryczne i wysyła je do Kaspersky Anti Targeted Attack Platform podczas synchronizacji. Zdarzenia telemetryczne docierają do serwera prawie nieprzerwanie. Kaspersky Endpoint Security inicjuje synchronizację z serwerem, gdy spełniony jest jeden z następujących warunków:

- Upłynął interwał synchronizacji.
- Liczba zdarzeń w buforze przekracza górną granicę.

Dlatego domyślnie aplikacja synchronizuje się co 30 sekund lub zawsze, gdy w buforze znajdują się 1024 zdarzenia. Możesz skonfigurować sposób synchronizacji w zasadzie Kaspersky Endpoint Security i wybrać optymalne wartości odpowiadające obciążeniu sieci (zobacz instrukcje poniżej).

Jeśli nie ma połączenia między Kaspersky Endpoint Security a serwerem, aplikacja umieszcza nowe zdarzenia w kolejce. Po przywróceniu połączenia Kaspersky Endpoint Security wysyła zdarzenia z kolejki do serwera w odpowiedniej kolejności. Aby uniknąć przeciążenia serwera, Kaspersky Endpoint Security może pominąć niektóre zdarzenia. Aby to włączyć, możesz zoptymalizować ustawienia transmisji zdarzeń, na przykład ustawić maksymalną liczbę zdarzeń na godzinę (patrz instrukcje poniżej).

Jeśli używasz Kaspersky Anti Targeted Attack Platform wraz z innym rozwiązaniem, które również wykorzystuje telemetrię, możesz wyłączyć telemetrię dla KATA (EDR) — patrz instrukcje poniżej. Pozwala to zoptymalizować obciążenie serwera dla tych rozwiązań. Na przykład, jeśli masz wdrożone rozwiązanie Managed Detection and Response i KATA (EDR), możesz użyć telemetrii MDR i utworzyć zadania Threat Response w KATA (EDR).

Jak skonfigurować telemetrię w Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasad wybierz **Detection and Response** i wybierz komponent, który chcesz skonfigurować: **Endpoint Detection and Response Expert (on-premises)** lub **Network Detection and Response (KATA)**.
5. Skonfiguruj ustawienie **Wysyłaj żądanie synchronizacji do serwera KATA co (min)**. Częstotliwość żądań synchronizacji wysyłanych do serwera. Podczas synchronizacji Kaspersky Endpoint Security wysyła informacje o zmodyfikowanych ustawieniach i zadaniach aplikacji.
6. Należy upewnić się, że pole **Wyślij dane telemetryczne do KATA** jest zaznaczone.
7. W razie potrzeby skonfiguruj synchronizację z ustawieniami serwera w sekcji **Ustawienia przesyłania danych**:
   - **Maksymalne opóźnienie transmisji zdarzeń (s)**. Aplikacja synchronizuje się z serwerem w celu wysyłania zdarzeń po wygaśnięciu przedziału synchronizacji. Domyślnie ustawienie to 30 sekund.
   - **Maksymalna liczba zdarzeń na pakiet**. Aplikacja synchronizuje się z serwerem, gdy bufor zostanie zapełniony zdarzeniami. Domyślnie ustawienie to 1024 zdarzenia.

8. W razie potrzeby zaznacz pole wyboru **Włącz ograniczanie żądań** w bloku **Ograniczanie żądań**.

   Ta funkcja pomaga zoptymalizować obciążenie serwera. Jeśli ta funkcja jest włączona, aplikacja ogranicza przesyłanie zdarzeń. Jeśli liczba zdarzeń przekroczy skonfigurowane limity, Kaspersky Endpoint Security przestanie wysyłać zdarzenia.

9. Skonfiguruj ustawienia optymalizacji wysyłania zdarzeń na serwer:

   - **Maksymalna liczba zdarzeń na godzinę**. Aplikacja analizuje strumień danych telemetrycznych i ogranicza wysyłanie zdarzeń, jeśli strumień zdarzeń przekroczy skonfigurowany limit zdarzeń na godzinę. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń po godzinie. Ustawienie domyślne to 3000 zdarzeń na godzinę. Jeżeli aplikacja jest zainstalowana na serwerze, strumień danych telemetrycznych jest większy. W przypadku serwerów zaleca się zwiększenie wartości do 60 000 zdarzeń na godzinę.

   - **Procent przekroczenia limitu zdarzeń**. Aplikacja sortuje zdarzenia według typu (np. zdarzenia „zmiany w rejestrze") i ogranicza transmisję zdarzeń, jeśli stosunek zdarzeń tego samego typu do całkowitej liczby zdarzeń przekroczy skonfigurowany limit w procentach. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń, gdy stosunek innych zdarzeń do łącznej liczby zdarzeń ponownie stanie się wystarczająco duży. Ustawienie domyślne to 15%.

10. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak skonfigurować telemetrię w Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Konfiguracja wbudowanych agentów** → **Endpoint Detection and Response Expert (on-premise)**.

5. Aby skonfigurować EDR (KATA), wybierz **Endpoint Detection and Response Expert (wersja 7.1 lub starsze)** z listy rozwiązań.

6. Upewnij się, że pole wyboru **Wyślij dane telemetryczne do serwerów KATA** jest zaznaczone w sekcji **Ustawienia przesyłania danych**.

7. Skonfiguruj ustawienie **Wysyłaj żądanie synchronizacji do serwera co (min)**. Częstotliwość żądań synchronizacji wysyłanych do serwera. Podczas synchronizacji Kaspersky Endpoint Security wysyła informacje o zmodyfikowanych ustawieniach i zadaniach aplikacji.

8. Należy upewnić się, że pole **Wyślij dane telemetryczne do serwerów KATA** jest zaznaczone.

9. W razie potrzeby skonfiguruj synchronizację z ustawieniami serwera w sekcji **Ustawienia przesyłania danych**:

   - **Maksymalne opóźnienie transmisji zdarzeń (s)**. Aplikacja synchronizuje się z serwerem w celu wysyłania zdarzeń po wygaśnięciu przedziału synchronizacji. Domyślnie ustawienie to 30 sekund.

   - **Maksymalna liczba pakietów zdarzeń**. Aplikacja synchronizuje się z serwerem, gdy bufor zostanie zapełniony zdarzeniami. Domyślnie ustawienie to 1024 zdarzenia.

10. W razie potrzeby zaznacz pole wyboru **Włącz ograniczanie żądań** w bloku **Ograniczanie żądań**.

    Ta funkcja pomaga zoptymalizować obciążenie serwera. Jeśli ta funkcja jest włączona, aplikacja ogranicza przesyłanie zdarzeń. Jeśli liczba zdarzeń przekroczy skonfigurowane limity, Kaspersky Endpoint Security przestanie wysyłać zdarzenia.

11. Skonfiguruj ustawienia optymalizacji wysyłania zdarzeń na serwer:

    - **Maksymalna liczba zdarzeń na godzinę**. Aplikacja analizuje strumień danych telemetrycznych i ogranicza wysyłanie zdarzeń, jeśli strumień zdarzeń przekroczy skonfigurowany limit zdarzeń na godzinę. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń po godzinie. Ustawienie domyślne to 3000 zdarzeń na godzinę. Jeżeli aplikacja jest zainstalowana na serwerze, strumień danych telemetrycznych jest większy. W przypadku serwerów zaleca się zwiększenie wartości do 60 000 zdarzeń na godzinę.

    - **Procent przekroczenia limitu zdarzeń**. Aplikacja sortuje zdarzenia według typu (np. zdarzenia „zmiany w rejestrze") i ogranicza transmisję zdarzeń, jeśli stosunek zdarzeń tego samego typu do całkowitej liczby zdarzeń przekroczy skonfigurowany limit w procentach. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń, gdy stosunek innych zdarzeń do łącznej liczby zdarzeń ponownie stanie się wystarczająco duży. Ustawienie domyślne to 15%.

12. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Idź do **sekcji Integracja KATA** → **Wykluczenia telemetrii**.

5. Pod **Ustawienia przesyłania danych** wybierz pole wyboru **Użyj wykluczeń**.

6. Kliknij **Dodaj** i skonfiguruj wykluczenia:

   Kryteria są łączone z logiką *I*.

   - **Ścieżka**. Pełna ścieżka do pliku, w tym jego nazwa i rozszerzenie. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. Aby wykluczenie zadziałało, należy określić ścieżkę do pliku.

   - **Wiersz poleceń**. Komenda używana do uruchomienia obiektu.

   - **Opis**. Wartość parametru FileDescription z zasobu RT_VERSION (VersionInfo).

     Aby uzyskać więcej informacji na temat zasobu VersionInfo, odwiedź witrynę firmy Microsoft.

   - **Nazwa oryginalnego pliku**. Wartość parametru OriginalFilename z zasobu RT_VERSION (VersionInfo).

   - **Wersja**. Wartość parametru FileVersion z zasobu RT_VERSION (VersionInfo).

   - **MD5**. suma kontrolna MD5 pliku

- **SHA256**. suma kontrolna SHA256 pliku
- **Typy zdarzeń**. Aby wykluczenie zadziałało, musisz wybrać co najmniej jeden typ zdarzenia.

7. Zapisz swoje zmiany.

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zadania**.

   Zostanie otwarta lista zadań.

2. Kliknij **Nowe zadanie**.

Zostanie uruchomiony Kreator tworzenia zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie typu zadania

1. Wybierz **Kaspersky Endpoint Security for Windows (14.1)** → **Wycofywanie aktualizacji**.

Krok 2. Wybieranie urządzeń, do których zadanie zostanie przypisane

Wybierz komputery, na których zadanie zostanie wykonane. Dostępne są następujące opcje:

- Przypisz zadanie do grupy administracyjnej. W tym przypadku zadanie jest przypisywane do komputerów znajdujących się we wcześniej utworzonej grupie administracyjnej.
- Wybierz komputery wykryte w sieci przez Serwer administracyjny: *urządzenia nieprzypisane*. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy. Możesz określić nazwy NetBIOS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Krok 3. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz zadania, na przykład ręcznie.

Krok 4. Definiowanie nazwy zadania

Wprowadź nazwę zadania.

Krok 7. Kończenie tworzenia zadania

Zakończ działanie Kreatora. Jeśli to konieczne, zaznacz pole wyboru **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Wykluczenia telemetryczne EDR (KATA)

Aby poprawić wydajność i zoptymalizować transmisję danych do serwera telemetrii, możesz skonfigurować wykluczenia telemetryczne. Można na przykład zrezygnować z wysyłania danych komunikacyjnych sieci dla poszczególnych aplikacji.

Jak utworzyć wykluczenie telemetryczne w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne → Wykluczenia i typy obiektów**.
4. W sekcji **Ustawienia telemetrii → Telemetria EDR (KATA) / NDR (KATA)** kliknij przycisk **Ustawienia**.
5. W oknie, które zostanie otwarte, skonfiguruj wykluczenia telemetryczne (patrz tabela poniżej).

   Aplikacja łączy warunki wykluczenia za pomocą logicznego AND. Aby utworzyć regułę, określ wartość w polu **Pełna ścieżka** i wybierz co najmniej jeden typ zdarzenia z listy **Użyj dla następujących typów zdarzeń**.
6. Zapisz swoje zmiany.

Jak utworzyć wykluczenie telemetryczne w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne → Ustawienia telemetrii**.
5. Wybierz zakładkę **Telemetria EDR (KATA) / NDR (KATA)**.
6. W oknie, które zostanie otwarte, skonfiguruj wykluczenia telemetryczne (patrz tabela poniżej).

   Aplikacja łączy warunki wykluczenia za pomocą logicznego AND. Aby utworzyć regułę, określ wartość w polu **Pełna ścieżka** i wybierz co najmniej jeden typ zdarzenia.
7. Zapisz swoje zmiany.

Parametry wykluczenia telemetrycznego

Parametr	Opis
Wykluczone procesy	**Optymalizuj rozmiar wysyłania telemetrii**. Kaspersky Endpoint Security umożliwia optymalizację ilości przesyłanych danych i wykluczanie zdarzeń z określonymi kodami z telemetrii: kod 102 (podstawowa komunikacja) i 8 (aktywność sieciowa procesu) dla protokołu Microsoft SMB, usługi WinRM i procesu klnagent.exe Agenta sieciowego, a także rozszerzone informacje o rodzajach pakietów sieciowych dla wszystkich typów protokołów sieciowych. Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND. **Proces** i **Proces nadrzędny**: • **Pełna ścieżka**. Pełna ścieżka do pliku, w tym jego nazwa i rozszerzenie. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. • **Tekst wiersza polecenia**. Komenda używana do uruchomienia pliku. • **Opis**. Wartość parametru FileDescription z zasobu RT_VERSION (VersionInfo). • **Nazwa oryginalnego pliku**. Wartość parametru OriginalFilename z zasobu RT_VERSION (VersionInfo). • **Wersja**. Wartość parametru FileVersion z zasobu RT_VERSION (VersionInfo). • **Sumy kontrolne pliku**. MD5 i SHA256. Możesz także wybrać plik ręcznie, a aplikacja automatycznie wypełni pola z wybranego pliku. W 64-bitowych systemach operacyjnych należy ręcznie wprowadzić parametry 64-bitowej wersji pliku wykonywalnego procesu z folderu `C:\windows\system32`, ponieważ aplikacja wypełnia pola parametrów pliku wykonywalnego danymi z właściwości wersji 32-bitowej tego samego pliku wykonywalnego w folderze `C:\windows\syswow64`. Na przykład, jeśli wybierzesz `C:\windows\system32\cmd.exe`, wtyczka wyświetli parametry `C:\windows\syswow64\cmd.exe`. Takie zachowanie jest podyktowane specyfiką systemu operacyjnego. **Użyj dla następujących typów zdarzeń**: • **Modyfikacja pliku**. • **Zdarzenia sieciowe**. • **Proces: Interaktywne wejście konsoli**. • **Moduł wczytany**. • **Zmodyfikowano rejestr**. • **Dzienniki DNS**. • **Dostęp do procesu**. • **Wstrzyknięcie kodu**. • **Zapytanie WMI**. • **Obiekt przetwarzający**. • **LDAP**. • **AMSI**.
Wykluczona komunikacja sieciowa	**Nazwa reguły**. **Kierunek**. **Protokół**. **Gniazdo typu raw**. **Numer protokołu**. **Certyfikat TLS**. **Port lokalny lub zakres**. **Port zdalny lub zakres**. **Adres lokalny**. Adres sieciowy komputera, dla którego Kaspersky Endpoint Security wyklucza dane telemetryczne z ruchu sieciowego. **Adres zdalny**. Adres sieciowy komputera, dla którego Kaspersky Endpoint Security wyklucza dane telemetryczne z ruchu sieciowego. W przypadku adresów IP obsługiwany jest wyłącznie format IPv4. **Aplikacje**. Lista plików wykonywalnych aplikacji, dla których Kaspersky Endpoint Security wyklucza telemetrię EDR z ruchu sieciowego.

Parametr	Opis
Wykluczone operacje na plikach	**Nazwa reguły**. **Nazwa pliku lub maska**. Nazwa lub maska pliku lub folderu; Kaspersky Endpoint Security stosuje regułę wykluczenia podczas uzyskiwania dostępu do tego pliku lub folderu. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski. **Typ operacji**. **Poprzednia ścieżka**. Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND. **Proces** i **Proces nadrzędny**: • **Pełna ścieżka**. Pełna ścieżka do pliku, w tym jego nazwa i rozszerzenie. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. • **Tekst wiersza polecenia**. Komenda używana do uruchomienia pliku. • **Opis**. Wartość parametru FileDescription z zasobu RT_VERSION (VersionInfo). • **Nazwa oryginalnego pliku**. Wartość parametru OriginalFilename z zasobu RT_VERSION (VersionInfo). • **Wersja**. Wartość parametru FileVersion z zasobu RT_VERSION (VersionInfo). • **Sumy kontrolne pliku**. MD5 i SHA256. Możesz także wybrać plik ręcznie, a aplikacja automatycznie wypełni pola z wybranego pliku. W 64-bitowych systemach operacyjnych należy ręcznie wprowadzić parametry 64-bitowej wersji pliku wykonywalnego procesu z folderu `C:\windows\system32`, ponieważ aplikacja wypełnia pola parametrów pliku wykonywalnego danymi z właściwości wersji 32-bitowej tego samego pliku wykonywalnego w folderze `C:\windows\syswow64`. Na przykład, jeśli wybierzesz `C:\windows\system32\cmd.exe`, wtyczka wyświetli parametry `C:\windows\syswow64\cmd.exe`. Takie zachowanie jest podyktowane specyfiką systemu operacyjnego.
Wykluczone operacje DNS	**Nazwa reguły**. Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND. **Proces** i **Proces nadrzędny**: • **Pełna ścieżka**. Pełna ścieżka do pliku, w tym jego nazwa i rozszerzenie. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. • **Tekst wiersza polecenia**. Komenda używana do uruchomienia pliku. • **Opis**. Wartość parametru FileDescription z zasobu RT_VERSION (VersionInfo). • **Nazwa oryginalnego pliku**. Wartość parametru OriginalFilename z zasobu RT_VERSION (VersionInfo). • **Wersja**. Wartość parametru FileVersion z zasobu RT_VERSION (VersionInfo). • **Sumy kontrolne pliku**. MD5 i SHA256. Możesz także wybrać plik ręcznie, a aplikacja automatycznie wypełni pola z wybranego pliku. W 64-bitowych systemach operacyjnych należy ręcznie wprowadzić parametry 64-bitowej wersji pliku wykonywalnego procesu z folderu `C:\windows\system32`, ponieważ aplikacja wypełnia pola parametrów pliku wykonywalnego danymi z właściwości wersji 32-bitowej tego samego pliku wykonywalnego w folderze `C:\windows\syswow64`. Na przykład, jeśli wybierzesz `C:\windows\system32\cmd.exe`, wtyczka wyświetli parametry `C:\windows\syswow64\cmd.exe`. Takie zachowanie jest podyktowane specyfiką systemu operacyjnego. **DNS**: • **Adres IP serwera DNS**. • **Opcje zapytania**. • **Stan**. • **Nazwa domeny**. • **ID typu ustawień**. • **Dane odpowiedzi**.

Parametr	Opis
Wykluczone operacje LDAP	**Nazwa reguły**. **Zakres wyszukiwania LDAP**. **Filtr**. **Nazwa odróżniająca dla wyszukiwania obiektów LDAP**. **Atrybuty obiektu**. Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND. **Proces** i **Proces nadrzędny**: • **Pełna ścieżka**. Pełna ścieżka do pliku, w tym jego nazwa i rozszerzenie. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. • **Tekst wiersza polecenia**. Komenda używana do uruchomienia pliku. • **Opis**. Wartość parametru FileDescription z zasobu RT_VERSION (VersionInfo). • **Nazwa oryginalnego pliku**. Wartość parametru OriginalFilename z zasobu RT_VERSION (VersionInfo). • **Wersja**. Wartość parametru FileVersion z zasobu RT_VERSION (VersionInfo). • **Sumy kontrolne pliku**. MD5 i SHA256. Możesz także wybrać plik ręcznie, a aplikacja automatycznie wypełni pola z wybranego pliku. W 64-bitowych systemach operacyjnych należy ręcznie wprowadzić parametry 64-bitowej wersji pliku wykonywalnego procesu z folderu `C:\windows\system32`, ponieważ aplikacja wypełnia pola parametrów pliku wykonywalnego danymi z właściwości wersji 32-bitowej tego samego pliku wykonywalnego w folderze `C:\windows\syswow64`. Na przykład, jeśli wybierzesz `C:\windows\system32\cmd.exe`, wtyczka wyświetli parametry `C:\windows\syswow64\cmd.exe`. Takie zachowanie jest podyktowane specyfiką systemu operacyjnego.
Wykluczone zapytania o dostęp do procesów	**Nazwa reguły**. **Typ operacji**. **Żądanie dostępu do procesu**. **Śledzenie stosu wywołań**. Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND. **Proces**, **Proces nadrzędny**, **Plik procesu docelowego**, **Uchwyt procesu źródłowego** i **Uchwyt procesu docelowego**. • **Pełna ścieżka**. Pełna ścieżka do pliku, w tym jego nazwa i rozszerzenie. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. • **Tekst wiersza polecenia**. Komenda używana do uruchomienia pliku. • **Określ kryteria wyzwalania reguły i typy zdarzeń, dla których ta reguła ma być stosowana**. Wartość parametru FileDescription z zasobu RT_VERSION (VersionInfo). • **Nazwa oryginalnego pliku**. Wartość parametru OriginalFilename z zasobu RT_VERSION (VersionInfo). • **Wersja**. Wartość parametru FileVersion z zasobu RT_VERSION (VersionInfo). • **Sumy kontrolne pliku**. MD5 i SHA256. Możesz także wybrać plik ręcznie, a aplikacja automatycznie wypełni pola z wybranego pliku. W 64-bitowych systemach operacyjnych należy ręcznie wprowadzić parametry 64-bitowej wersji pliku wykonywalnego procesu z folderu `C:\windows\system32`, ponieważ aplikacja wypełnia pola parametrów pliku wykonywalnego danymi z właściwości wersji 32-bitowej tego samego pliku wykonywalnego w folderze `C:\windows\syswow64`. Na przykład, jeśli wybierzesz `C:\windows\system32\cmd.exe`, wtyczka wyświetli parametry `C:\windows\syswow64\cmd.exe`. Takie zachowanie jest podyktowane specyfiką systemu operacyjnego.

Parametr	Opis
Wykluczone wprowadzenia kodu	**Nazwa reguły**. **Metoda dostępu**. **Stos wywołań**. **Zmodyfikowany wiersz poleceń**. **Adres wprowadzenia**. **Wprowadzona nazwa DLL**. Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND. **Proces** i **Proces nadrzędny**: • **Pełna ścieżka**. Pełna ścieżka do pliku, w tym jego nazwa i rozszerzenie. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. • **Tekst wiersza polecenia**. Komenda używana do uruchomienia pliku. • **Opis**. Wartość parametru FileDescription z zasobu RT_VERSION (VersionInfo). • **Nazwa oryginalnego pliku**. Wartość parametru OriginalFilename z zasobu RT_VERSION (VersionInfo). • **Wersja**. Wartość parametru FileVersion z zasobu RT_VERSION (VersionInfo). • **Sumy kontrolne pliku**. MD5 i SHA256. Możesz także wybrać plik ręcznie, a aplikacja automatycznie wypełni pola z wybranego pliku. W 64-bitowych systemach operacyjnych należy ręcznie wprowadzić parametry 64-bitowej wersji pliku wykonywalnego procesu z folderu `C:\windows\system32`, ponieważ aplikacja wypełnia pola parametrów pliku wykonywalnego danymi z właściwości wersji 32-bitowej tego samego pliku wykonywalnego w folderze `C:\windows\syswow64`. Na przykład, jeśli wybierzesz `C:\windows\system32\cmd.exe`, wtyczka wyświetli parametry `C:\windows\syswow64\cmd.exe`. Takie zachowanie jest podyktowane specyfiką systemu operacyjnego.
Wykluczone zapytania WMI	**Nazwa reguły**. **Typ operacji WMI**. **Zdalne zapytanie**. **Nazwa komputera, który wykonał polecenie WMI**. **Konto użytkownika WMI**. **Wykonane polecenie WMI**. **Nazwa przestrzeni WMI**. **Filtr konsumentów zdarzeń WMI**. **Nazwa utworzonego konsumenta zdarzeń WMI**. **Kod źródłowy konsumenta zdarzenia WMI**. Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND. **Proces** i **Proces nadrzędny**: • **Pełna ścieżka**. Pełna ścieżka do pliku, w tym jego nazwa i rozszerzenie. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. • **Tekst wiersza polecenia**. Komenda używana do uruchomienia pliku. • **Opis**. Wartość parametru FileDescription z zasobu RT_VERSION (VersionInfo). • **Nazwa oryginalnego pliku**. Wartość parametru OriginalFilename z zasobu RT_VERSION (VersionInfo). • **Wersja**. Wartość parametru FileVersion z zasobu RT_VERSION (VersionInfo). • **Sumy kontrolne pliku**. MD5 i SHA256. Możesz także wybrać plik ręcznie, a aplikacja automatycznie wypełni pola z wybranego pliku. W 64-bitowych systemach operacyjnych należy ręcznie wprowadzić parametry 64-bitowej wersji pliku wykonywalnego procesu z folderu `C:\windows\system32`, ponieważ aplikacja wypełnia pola parametrów pliku wykonywalnego danymi z właściwości wersji 32-bitowej tego samego pliku wykonywalnego w folderze `C:\windows\syswow64`. Na przykład, jeśli wybierzesz `C:\windows\system32\cmd.exe`, wtyczka wyświetli parametry `C:\windows\syswow64\cmd.exe`. Takie zachowanie jest podyktowane specyfiką systemu operacyjnego.

Parametr	Opis
Wykluczone operacje przetwarzania danych	**Nazwa reguły**. **Nazwa obiektu przetwarzającego**. **Typ operacji**. Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND. **Proces** i **Proces nadrzędny**: • **Pełna ścieżka**. Pełna ścieżka do pliku, w tym jego nazwa i rozszerzenie. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. • **Tekst wiersza polecenia**. Komenda używana do uruchomienia pliku. • **Opis**. Wartość parametru FileDescription z zasobu RT_VERSION (VersionInfo). • **Nazwa oryginalnego pliku**. Wartość parametru OriginalFilename z zasobu RT_VERSION (VersionInfo). • **Wersja**. Wartość parametru FileVersion z zasobu RT_VERSION (VersionInfo). • **Sumy kontrolne pliku**. MD5 i SHA256. Możesz także wybrać plik ręcznie, a aplikacja automatycznie wypełni pola z wybranego pliku. W 64-bitowych systemach operacyjnych należy ręcznie wprowadzić parametry 64-bitowej wersji pliku wykonywalnego procesu z folderu `C:\windows\system32`, ponieważ aplikacja wypełnia pola parametrów pliku wykonywalnego danymi z właściwości wersji 32-bitowej tego samego pliku wykonywalnego w folderze `C:\windows\syswow64`. Na przykład, jeśli wybierzesz `C:\windows\system32\cmd.exe`, wtyczka wyświetli parametry `C:\windows\syswow64\cmd.exe`. Takie zachowanie jest podyktowane specyfiką systemu operacyjnego.
Wykluczono zmiany w rejestrze	**Nazwa reguły**. **Typ operacji**. **Ścieżka**. **Nazwa wartości**. **Wartość**. **Pełna nazwa pliku rejestru**. Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND. **Proces** i **Proces nadrzędny**: • **Pełna ścieżka**. Pełna ścieżka do pliku, w tym jego nazwa i rozszerzenie. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. • **Tekst wiersza polecenia**. Komenda używana do uruchomienia pliku. • **Opis**. Wartość parametru FileDescription z zasobu RT_VERSION (VersionInfo). • **Nazwa oryginalnego pliku**. Wartość parametru OriginalFilename z zasobu RT_VERSION (VersionInfo). • **Wersja**. Wartość parametru FileVersion z zasobu RT_VERSION (VersionInfo). • **Sumy kontrolne pliku**. MD5 i SHA256. Możesz także wybrać plik ręcznie, a aplikacja automatycznie wypełni pola z wybranego pliku. W 64-bitowych systemach operacyjnych należy ręcznie wprowadzić parametry 64-bitowej wersji pliku wykonywalnego procesu z folderu `C:\windows\system32`, ponieważ aplikacja wypełnia pola parametrów pliku wykonywalnego danymi z właściwości wersji 32-bitowej tego samego pliku wykonywalnego w folderze `C:\windows\syswow64`. Na przykład, jeśli wybierzesz `C:\windows\system32\cmd.exe`, wtyczka wyświetli parametry `C:\windows\syswow64\cmd.exe`. Takie zachowanie jest podyktowane specyfiką systemu operacyjnego.
Wykluczone operacje z urządzeniami	**Nazwa reguły**. **Typ urządzenia**. **ID urządzenia**. **Nazwa urządzenia**.

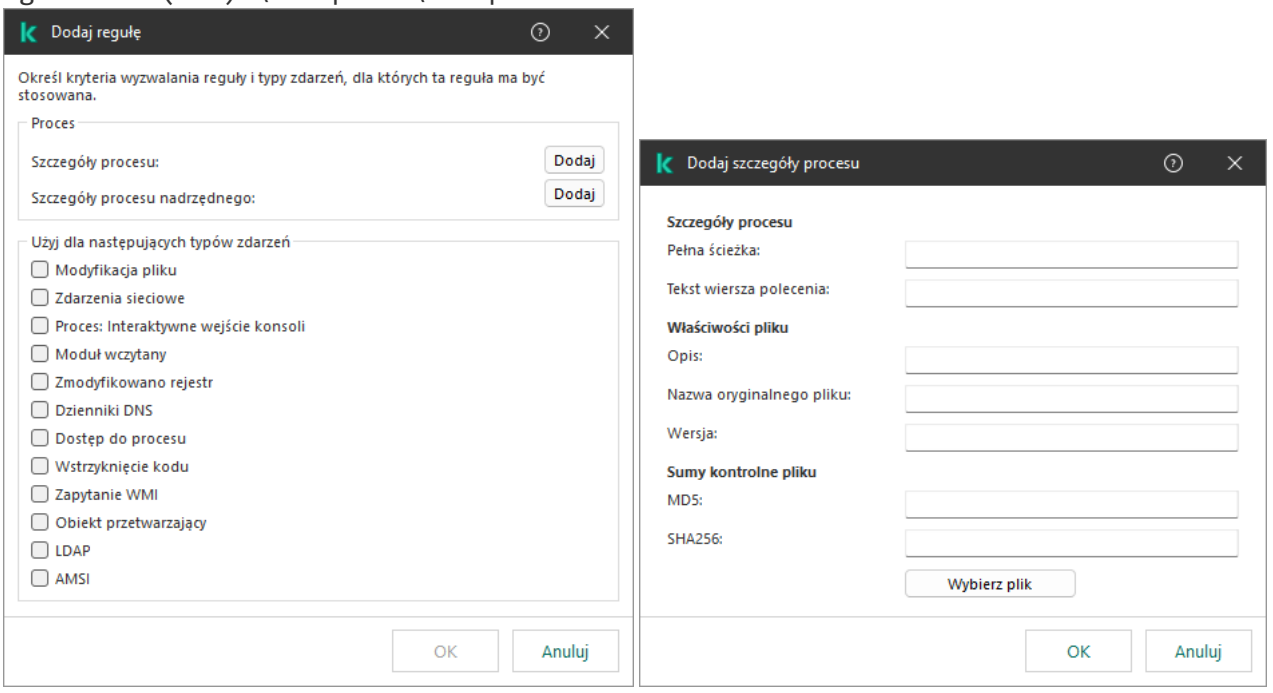
Przykład 1. Wykluczone procesy

Aby wykluczyć zdarzenia aplikacji (procesów) innych firm z telemetrii, otwórz okno wykluczeń telemetrii EDR na karcie **Wykluczone procesy** i dodaj plik wykonywalny aplikacji.

Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND.

Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. Na przykład:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



Wykluczanie procesu

Przykład 1. Modyfikacja pliku

Jeśli często edytujesz skrypty w aplikacji Notepad++ i chcesz wykluczyć zdarzenia modyfikacji dla odpowiednich skryptów, dodaj plik wykonywalny Notepad++ do wykluczeń telemetrii.

Określ ustawienia w następujący sposób:

- **Pełna ścieżka**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Użyj dla następujących typów zdarzeń**: Modyfikacja pliku.

Przykład 2. Zdarzenia sieciowe

Jeśli używasz aplikacji WinSCP do zarządzania plikami na serwerze zdalnym i chcesz wykluczyć zdarzenia sieciowe, dodaj plik wykonywalny WinSCP do wykluczeń telemetrii.

Określ ustawienia w następujący sposób:

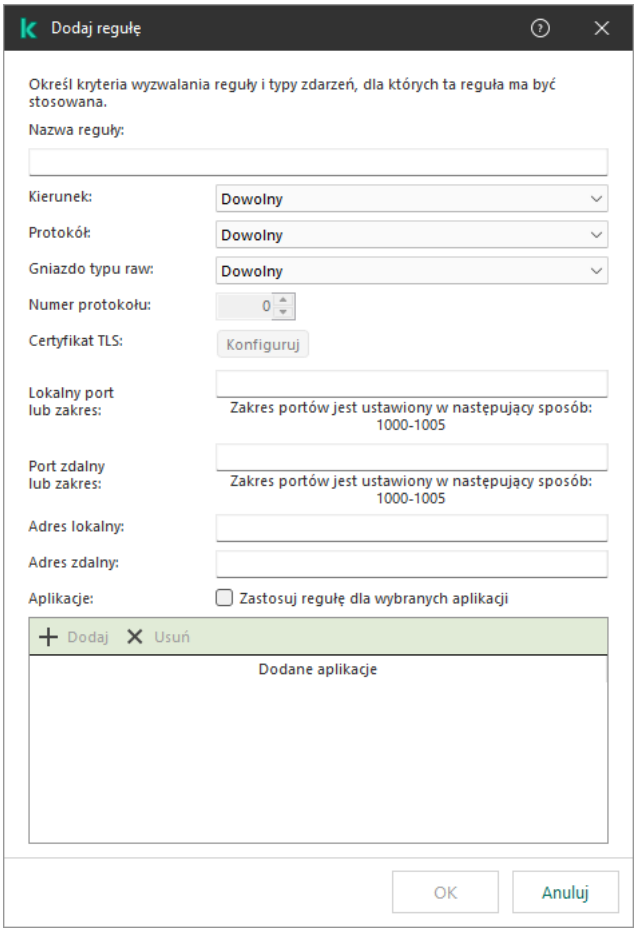
- **Pełna ścieżka**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (opcjonalnie).
- **Użyj dla następujących typów zdarzeń**: Zdarzenia sieciowe.

Przykład 2. Wykluczona komunikacja sieciowa

Aby wykluczyć zdarzenia połączenia usługi zdalnej z telemetrii, otwórz okno wykluczeń telemetrii EDR na karcie **Wykluczona komunikacja sieciowa** i dodaj ustawienia połączenia: protokół, port, kierunek, adres IP, certyfikat TLS i inne.

Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND.

Nie można określić adresu podsieci (na przykład 10.28.0.0/24). Aplikacja pozwala na określenie tylko jednego adresu IP (na przykład 10.28.0.105).



Wykluczenie komunikacji sieciowej

Jeśli korzystasz z korporacyjnego serwera WWW i chcesz wykluczyć zdarzenia przeglądarki podczas łączenia się z tym serwerem, dodaj adres IP serwera i plik wykonywalny przeglądarki do wykluczeń telemetrii.

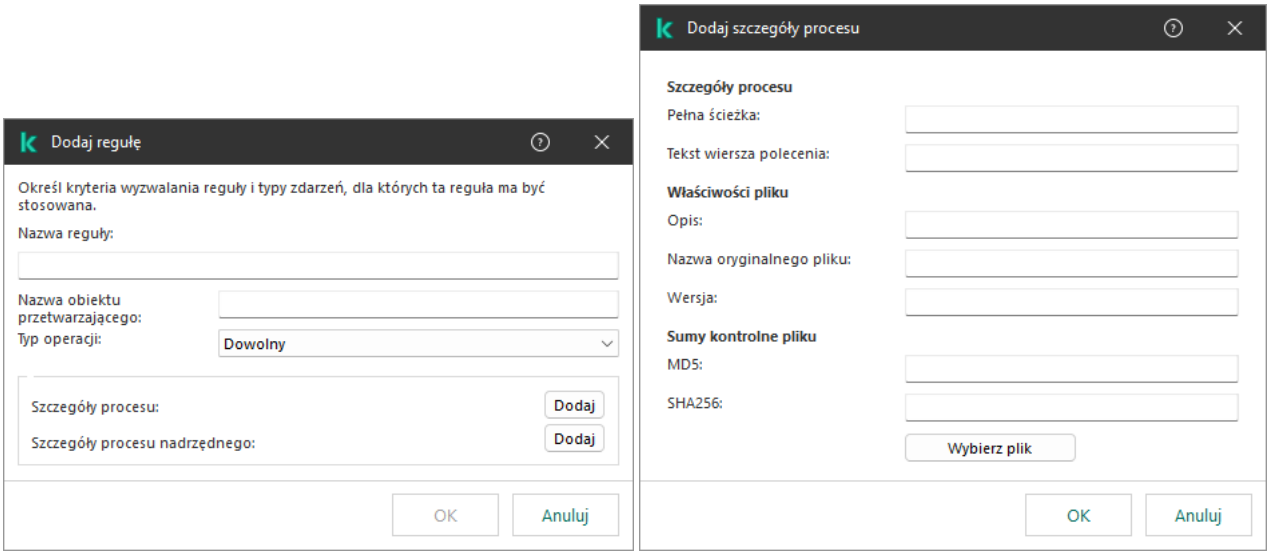
Określ ustawienia w następujący sposób:

- **Protokół**: TCP.
- **Port zdalny lub zakres**: 443.
- **Adres zdalny**: 10.28.0.105.
- **Aplikacje**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Przykład 3. Wykluczone operacje na plikach

Aby wykluczyć z telemetrii zdarzenia obejmujące operacje na zaufanych plikach, otwórz okno wykluczeń telemetrii EDR na karcie **Wykluczone operacje na plikach** i dodaj zaufany plik.

Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND.



Wykluczanie operacji na plikach

Jeśli aplikacja zapisuje dane do dziennika i chcesz wykluczyć zdarzenia modyfikacji pliku dziennika, dodaj plik dziennika i plik wykonywalny aplikacji do wykluczeń telemetrii.

Określ ustawienia w następujący sposób:

- **Nazwa pliku lub maska**: `C:\Apache24\logs\error.log`.
- **Typ operacji**: Modyfikacja pliku.
- **Pełna ścieżka**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Przykład 4. Wykluczone modyfikacje rejestru

Aby wykluczyć zdarzenia modyfikacji rejestru z telemetrii, otwórz okno wykluczeń telemetrii EDR na karcie **Wykluczono zmiany w rejestrze** i dodaj klucz rejestru.

Kaspersky Endpoint Security łączy kryteria wyzwalania reguły z logicznym AND.

Jeśli aplikacja często modyfikuje wartości rejestru i chcesz wykluczyć te zdarzenia modyfikacji rejestru z telemetrii, dodaj klucz rejestru i plik wykonywalny aplikacji do wykluczeń telemetrii.

Określ ustawienia w następujący sposób:

- **Typ operacji**: Modyfikacja.
- **Ścieżka**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Pełna ścieżka**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

Kaspersky Anti Targeted Attack Platform zawiera komponent Sandbox (KATA Sandbox). *Sandbox* to technologia pozwalająca na wykrywanie zaawansowanych zagrożeń na komputerze. Sandbox analizuje zachowanie obiektów w celu wykrywania szkodliwej aktywności oraz aktywności charakterystycznej dla ataków docelowych ukierunkowanych na infrastrukturę IT organizacji. Sandbox analizuje i skanuje obiekty na specjalnych serwerach z wdrożonymi obrazami wirtualnymi systemów operacyjnych Microsoft Windows (serwery Sandbox). Szczegółowe informacje na temat rozwiązania można znaleźć w systemie pomocy dla Kaspersky Anti Targeted Attack Platform.

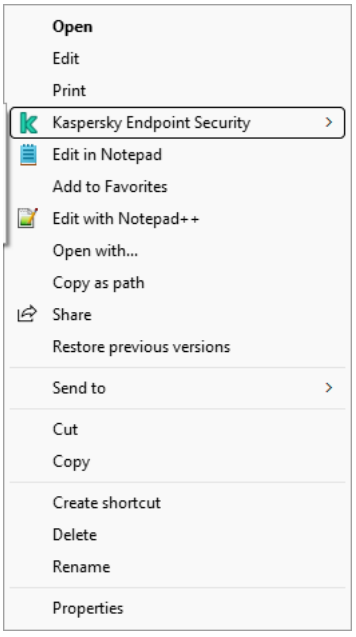
Aby aktywować KATA Sandbox, potrzebny jest klucz licencyjny obejmujący funkcjonalność KATA lub KEDR. Szczegółowe informacje na temat rozwiązania można znaleźć w pomocy Kaspersky Anti Targeted Attack Platform.

KATA Sandbox umożliwia skanowanie plików w następujących trybach:

- *Ręcznie*. Użytkownik ręcznie przesyła plik do skanowania z menu kontekstowego (**Wyślij do Sandbox**). Podczas wysłania pliku do Sandbox aplikacja również skanuje plik przy użyciu antywirusowych baz danych.
- *Automatycznie*. Aplikacja automatycznie wykrywa obiekty i przesyła je do Sandboxa w celu zeskanowania.

Po przesłaniu pliku do Sandbox, użytkownik nadal będzie miał do niego dostęp. Kaspersky Endpoint Security rejestruje odpowiednie zdarzenie i wysyła je do Kaspersky Security Center oraz konsoli Kaspersky Anti Targeted Attack Platform. Jeśli Sandbox wykryje szkodliwą aktywność, Kaspersky Endpoint Security wykona automatycznie akcję Threat Response (na przykład usunie obiekt i zainicjuje skanowanie obszarów krytycznych).

Aby KATA Sandbox działał w trybie ręcznym, konieczne jest wdrożenie Kaspersky Anti Targeted Attack Platform w wersji 7.0 lub nowszej. Aby KATA Sandbox działał w trybie automatycznym, konieczne jest wdrożenie Kaspersky Anti Targeted Attack Platform w wersji 8.0 lub nowszej.



Skanowanie w KATA Sandbox z menu kontekstowego

Integracja wbudowanego agenta z ze środowiskiem testowym "KATA Sandbox"

Dodawanie komponentu Sandbox jest wymagane do integracji z komponentem KATA Sandbox. Możesz wybrać składnik Sandbox podczas instalacji lub aktualizacji, a także przy użyciu zadania *Zmiana składników aplikacji*.

Aby wysłać pliki do skanowania, należy włączyć integrację z KATA Sandbox i dodać serwer Central Node wdrożony w ramach rozwiązania. Komponent może być zarządzany tylko przy użyciu konsoli Kaspersky Security Center Web Console. Nie możesz zarządzać tym komponentem przy użyciu Konsoli administracyjnej (MMC).

W celu włączenia lub wyłączenia integracji z KATA Sandbox:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Sandbox**.
5. Użyj przełącznika **Integracja z Sandbox WŁĄCZONA**, aby włączyć lub wyłączyć komponent.

6. Wybierz tryb działania KATA Sandbox:

   - **Ręcznie**. Użytkownik ręcznie przesyła plik do skanowania z menu kontekstowego (**Wyślij do Sandbox**).
   - **Automatycznie**. Aplikacja automatycznie wykrywa obiekty i przesyła je do Sandboxa w celu zeskanowania.
   - **Powiązany**.

7. Kliknij odnośnik **Ustawienia połączenia**.

8. Skonfiguruj ustawienia połączenia z serwerem Central Node:

   - **Limit czasu (ms)**. Limit czasu połączenia dla serwera Central Node został przekroczony. Po skonfigurowaniu upłynięcia określonej ilości czasu, Kaspersky Endpoint Security wyśle żądanie do następnego serwera. Możesz zwiększyć limit czasu połączenia dla serwera, jeśli prędkość Twojego połączenia spada lub jeśli połączenie jest niestabilne. Zalecany limit czasu żądania wynosi 0,5 sekundy lub mniej.
   - **Kolejka żądań**. Rozmiar folderu kolejki żądań. Podczas wysyłania kilku obiektów do skanowania w Sandbox Kaspersky Endpoint Security tworzy kolejkę żądań. Domyślnie, rozmiar folderu kolejki żądań jest ograniczony do 100 MB. Po osiągnięciu maksymalnego rozmiaru, Sandbox przestanie dodawać nowe żądania do kolejki i wyśle odpowiednie zdarzenie do Kaspersky Security Center. Możesz skonfigurować rozmiar folderu kolejki żądań w zależności od konfiguracji Twojego serwera.
   - **Certyfikat TLS serwera**. Aby skonfigurować zaufane połączenie z serwera Central Node, musisz przygotować certyfikat TLS. Następnie należy dodać certyfikat do komputera, stosując zasady. Należy również dodać certyfikat do serwera Central Node.
   - **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem Central Node. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera Central Node, a następnie uzyskać kontener szyfrowania i ustawić hasło chroniące kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform). Po skonfigurowaniu ustawień węzła centralnego należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny.

9. W sekcji **Połączenie z serwerami Sandbox** kliknij przycisk **Dodaj**.

10. Otworzy się okno; wprowadź w nim adres serwera Central Node (IPv4, IPv6, DNS) i port.

    Więcej informacji dotyczących wdrożenia obrazów wirtualnych i skonfigurowania serwerów Central Node można znaleźć w systemie pomocy dla Kaspersky Anti Targeted Attack Platform.

11. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

W rezultacie komponent Sandbox jest włączony. Sprawdź stan działania komponentu, przeglądając *Raport o stanie składników aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Sandbox** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

Konfigurowanie akcji Threat Response

Jeśli Sandbox wykryje szkodliwą aktywność, Kaspersky Endpoint Security wykona automatycznie akcję Threat Response (na przykład usunie obiekt i zainicjuje skanowanie obszarów krytycznych).

Aby skonfigurować akcje Threat Response:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Sandbox**.
5. W sekcji **Działanie po wykryciu zagrożenia** wybierz żądaną akcję:

   - **Przenieś kopię do Kwarantanny, usuń obiekt**. Jeśli ta opcja została zaznaczona, Kaspersky Endpoint Security usunie szkodliwy obiekt wykryty na komputerze. Przed usunięciem obiektu Kaspersky Endpoint Security utworzy kopię zapasową w przypadku, gdy obiekt musi zostać przywrócony w późniejszym czasie. Kaspersky Endpoint Security przeniesie kopię zapasową do Kwarantanny.
   - **Uruchom skanowanie obszarów krytycznych**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security uruchamia zadanie *Skanowanie obszarów krytycznych*. Domyślnie, Kaspersky Endpoint Security skanuje pamięć jądra, uruchomione procesy i sektory startowe dysku.
   - **Utwórz zadanie skanowania IOC**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security automatycznie tworzy zadanie *Skanowanie IOC (autonomiczne zadanie skanowania IOC)*. Dla tego zadania możesz skonfigurować tryb uruchamiania, obszar skanowania oraz akcję po wykryciu IOC (*Przenieś kopię do Kwarantanny, usuń obiekt* lub *Uruchom skanowanie obszarów krytycznych*). Aby zmodyfikować inne ustawienia zadania *Skanowanie IOC*, przejdź do ustawień zadania.
6. W razie potrzeby skonfiguruj ustawienia zadania *Skanowanie IOC* w bloku **Zakres skanowania IOC**.

   - **Krytyczne obszary plików**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security wykonuje skanowanie IOC tylko w krytycznych obszarach plików komputera: pamięci jądra i sektorów startowych.
   - **Obszary plików na dysku systemowym komputera**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security nie skanuje IOC na dysku systemowym komputera.
7. W razie potrzeby skonfiguruj ustawienia zadania *Skanowanie IOC* w bloku **Uruchom zadanie skanowania IOC**.

   - **Ręcznie**. Tryb uruchamiania, w którym możesz ręcznie uruchomić zadanie *Skanowanie IOC* w wygodnym dla siebie momencie.
   - **Automatycznie**. Tryb uruchamiania, w którym Kaspersky Endpoint Security automatycznie uruchamia zadanie *Skanowanie IOC* po wykryciu zagrożenia.
   - **Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności**. Tryb uruchamiania, w którym Kaspersky Endpoint Security uruchomi zadanie *Skanowanie IOC*, jeśli wygaszacz ekranu jest aktywny lub ekran jest zablokowany. Jeśli użytkownik odblokuje komputer, Kaspersky Endpoint Security wstrzyma zadanie. To oznacza, że wykonanie zadania może zająć kilka dni.
8. Skonfiguruj zaawansowane ustawienia zadań dla *Skanowanie IOC*.
9. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Przewodnik migracji z KEA do KES dla EDR (KATA)

Począwszy od wersji 12.1 Kaspersky Endpoint Security for Windows zawiera wbudowanego agenta do zarządzania komponentem Kaspersky Endpoint Detection and Response w ramach rozwiązania Kaspersky Anti Targeted Attack Platform. Nie potrzebujesz już oddzielnej aplikacji Kaspersky Endpoint Agent do pracy z EDR (KATA). Wszystkie funkcje Kaspersky Endpoint Agent będą wykonywane przez Kaspersky Endpoint Security. Obciążenie serwerów Kaspersky Anti Targeted Attack Platform pozostanie takie samo.

Podczas wdrażania Kaspersky Endpoint Security na komputerach, na których jest zainstalowany Kaspersky Endpoint Agent, rozwiązanie Kaspersky Anti Targeted Attack Platform (EDR) będzie nadal działać z Kaspersky Endpoint Security. Dodatkowo, Kaspersky Endpoint Agent zostanie usunięty z komputera. To samo zachowanie w systemie wystąpi podczas aktualizacji Kaspersky Endpoint Security do wersji 12.1 lub nowszej.

Kaspersky Endpoint Security nie jest kompatybilny z Kaspersky Endpoint Agent. Obu tych aplikacji nie można zainstalować na tym samym komputerze.

Aby aplikacja Kaspersky Endpoint Security działała w ramach Endpoint Detection and Response (KATA), muszą być spełnione następujące warunki:

- Kaspersky Anti Targeted Attack Platform w wersji 5.0 lub nowszej.
- Kaspersky Security Center w wersji 14.2 lub nowszej (w tym Agent sieciowy). We wcześniejszych wersjach Kaspersky Security Center nie ma możliwości aktywowania funkcji Endpoint Detection and Response (KATA).

Kroki migracji konfiguracji [KES+KEA] do [KES+wbudowanego agenta] dla EDR (KATA)

1. **Aktualizowanie wtyczki zarządzającej Kaspersky Endpoint Security**

   Komponentem EDR (KATA) można zarządzać przy użyciu wtyczki zarządzającej Kaspersky Endpoint Security w wersji 12.1 lub nowszej. W zależności od typu konsoli Kaspersky Security Center, której używasz, zaktualizuj wtyczkę zarządzającą w Konsoli administracyjnej (MMC) lub wtyczkę webową w Web Console.

2. **Migrowanie zasad i zadań**

   Przenieś ustawienia Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows. Dostępne są następujące opcje:

   - Kreator migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security. Kreator migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security działa tylko w usłudze Web Console.

     Jak dokonać migracji ustawień zasady i zadania z Kaspersky Endpoint Agent do Kaspersky Endpoint Security w Web Console:

     W oknie głównym Web Console wybierz **Operacje** → **Migracja z Kaspersky Endpoint Agent**.

     To spowoduje uruchomienie Kreatora migracji zasad i zadań. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Migracja zasady

Kreator migracji tworzy nową zasadę, która scala ustawienia zasad Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Na liście zasad wybierz zasady Kaspersky Endpoint Agent, których ustawienia chcesz scalić z zasadą Kaspersky Endpoint Security. Kliknij zasadę Kaspersky Endpoint Agent, aby wybrać zasadę Kaspersky Endpoint Security, z którą chcesz scalić ustawienia. Upewnij się, że wybrałeś poprawne zasady i przejdź do następnego kroku.

Krok 2. Migracja zadania

Kreator migracji nie obsługuje zadań EDR (KATA). Pomiń ten krok.

Krok 3. Kończenie działania kreatora

Zakończ działanie Kreatora. W wyniku działania kreatora zostanie utworzona nowa zasada Kaspersky Endpoint Security. Zasada scala ustawienia z Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Zasada zostaje nazwana *<Nazwa zasady Kaspersky Endpoint Security> & <Nazwa zasady Kaspersky Endpoint Agent>*. Nowa zasada posiada stan *Nieaktywny*. Aby kontynuować, zmień stany zasad Kaspersky Endpoint Agent i Kaspersky Endpoint Security na *Nieaktywny* i aktywuj nową scaloną zasadę.

Kreator migracji w usłudze Web Console pomija następujące ustawienia reguł i nie migruje ich:

- Zakaz modyfikacji ustawień **Ustawienia połączenia** („blokada").

  Domyślnie ustawienia można modyfikować („blokada" jest otwarta). Dlatego ustawienia nie są stosowane na komputerze. Należy zakazać modyfikacji ustawień i zamknąć „blokadę".

- Kontener szyfrowania.

  Jeśli do łączenia się z serwerami Central Node używasz uwierzytelniania dwuskładnikowego, należy dodać kontener szyfrowania.

Ponieważ Kreator migracji nie przeprowadza migracji tych ustawień, podczas łączenia komputera z serwerami Central Node mogą wystąpić błędy. Aby naprawić błędy, musisz przejść do właściwości profilu i skonfigurować ustawienia połączenia.

- Standardowy kreator konwersji zasad i zadań. Kreator konwersji zasad i zadań jest dostępny tylko w Konsoli administracyjnej (MMC). Więcej informacji o kreatorze konwersji zasad i zadań można znaleźć w pomocy Kaspersky Security Center.

Aby upewnić się, że Kaspersky Endpoint Security działa poprawnie na serwerach, zaleca się dodanie plików ważnych dla funkcjonowania serwera do strefy zaufanej. W przypadku serwerów SQL należy dodać pliki baz danych MDF i LDF. W przypadku serwerów Microsoft Exchange należy dodać pliki CHK, EDB, JRS, LOG i JSL. Możesz użyć masek, np. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Począwszy od Kaspersky Endpoint Security 12.6 for Windows, wykluczenia skanowania I zaufane aplikacje są dodawane do strefy zaufanej. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach.

Wykluczenia telemetrii EDR nie są migrowane z zasady Kaspersky Endpoint Agent do zasady Kaspersky Endpoint Security. Kaspersky Endpoint Security ma własne narzędzia wykluczające – zaufane aplikacje. Działanie Kaspersky Endpoint Security jest zoptymalizowane w taki sposób, że brak indywidualnych wykluczeń telemetrii EDR nie spowoduje dodatkowego obciążenia komputera w porównaniu z Kaspersky Endpoint Agent. Kaspersky Endpoint Security wykorzystuje telemetrię nie tylko do EDR (KATA), ale także do działania komponentów zabezpieczeń aplikacji. Nie ma zatem potrzeby przenoszenia poszczególnych wykluczeń telemetrii EDR. Jeśli wydajność komputera spada, sprawdź działanie aplikacji (patrz krok 7. Sprawdzanie działania).

3 Udzielanie licencji funkcjonalności EDR (KATA)

Aby aktywować Kaspersky Endpoint Security jako część rozwiązania Kaspersky Anti Targeted Attack Platform, potrzebujesz osobnej licencji na dodatek Kaspersky Endpoint Detection and Response (KATA). Możesz dodać klucz przy użyciu zadania *Dodaj klucz*. W rezultacie do aplikacji zostaną dodane dwa klucze: *Kaspersky Endpoint Security* i *Kaspersky Endpoint Detection and Response (KATA)*.

Uzyskanie licencji dodatku Kaspersky Endpoint Detection and Response (KATA) na komputerach z wcześniej aktywowanymi funkcjami EDR Optimum lub EDR Expert wiąże się z następującymi szczególnymi kwestiami:

- Jeśli korzystasz z *pliku klucza* w celu uzyskania licencji Kaspersky Endpoint Security z funkcjami EDR Optimum lub EDR Expert, nie można dodawać oddzielnego klucza dla dodatku Kaspersky Endpoint Detection and Response (KATA). Możesz przełączyć się na używanie kodu aktywacyjnego w celu uzyskania licencji lub skontaktować się z usługodawcą w celu uzyskania nowego pliku klucza do aktywacji funkcji Kaspersky Endpoint Security i EDR. Usługodawca dostarczy jeden lub więcej plików klucza do licencjonowania.

- Jeśli korzystasz z *pliku klucza* w celu uzyskania licencji Kaspersky Endpoint Security bez funkcji EDR Optimum lub EDR Expert, można dodać oddzielny klucz dla dodatku Kaspersky Endpoint Detection and Response (KATA) bez ponownego wystawiania plików klucza.

- Jeśli korzystasz z *kodu aktywacyjnego* w celu uzyskania licencji, serwer aktywacji Kaspersky automatycznie ponownie wystawi klucze, a funkcje EDR (KATA) staną się dostępne automatycznie. W takim przypadku EDR Optimum i EDR Expert zostaną wyłączone.

- Kaspersky Endpoint Security umożliwia dodanie maksymalnie dwóch aktywnych kluczy: klucza Kaspersky Endpoint Security i klucza typu dodatku. Możesz także dodać maksymalnie dwa klucze zapasowe. Jeden klucz zapasowy Kaspersky Endpoint Security i jeden klucz zapasowy typu dodatku.

4 Instalacja / aktualizacja aplikacji Kaspersky Endpoint Security

Aby przeprowadzić migrację funkcjonalności EDR (KATA) podczas instalacji lub aktualizacji aplikacji, zaleca się użycie zadania zdalnej instalacji. Podczas tworzenia zadania zdalnej instalacji należy wybrać komponent EDR (KATA) w ustawieniach pakietu instalacyjnego.

Możesz także zaktualizować aplikację za pomocą następujących metod:

- Przy użyciu usługi aktualizacji Kaspersky.

- Lokalnie, za pomocą Kreatora instalacji.

Kaspersky Endpoint Security obsługuje automatyczne wybieranie komponentów podczas aktualizacji aplikacji na komputerze z zainstalowaną aplikacją Kaspersky Endpoint Agent. Automatyczne wybieranie komponentów zależy od uprawnień konta użytkownika, które aktualizuje aplikację.

Jeśli aktualizujesz Kaspersky Endpoint Security przy użyciu pliku EXE lub MSI z poziomu konta systemowego (SYSTEM), Kaspersky Endpoint Security uzyskuje dostęp do bieżących licencji rozwiązań firmy Kaspersky. Dlatego też, jeśli na komputerze jest zainstalowany Kaspersky Endpoint Agent i aktywowane rozwiązanie EDR (KATA), instalator Kaspersky Endpoint Security automatycznie konfiguruje zestaw komponentów i wybiera komponent EDR (KATA). To powoduje przełączenie Kaspersky Endpoint Security na używanie wbudowanego agenta i usunięcie Kaspersky Endpoint Agent. Uruchomienie instalatora MSI z poziomu konta systemowego (SYSTEM) jest zazwyczaj wykonywane podczas aktualizacji za pośrednictwem usługi aktualizacji Kaspersky lub podczas wdrażania pakietu instalacyjnego za pośrednictwem Kaspersky Security Center.

Jeśli aktualizujesz Kaspersky Endpoint Security przy użyciu pliku MSI z poziomu konta użytkownika bez uprawnień, Kaspersky Endpoint Security nie ma dostępu do bieżących licencji dla rozwiązań Kaspersky. W takim przypadku Kaspersky Endpoint Security automatycznie wybiera komponenty na podstawie zestawu komponentów Kaspersky Endpoint Agent. Następnie Kaspersky Endpoint Security przełączy się na korzystanie z wbudowanego agenta i usunie Kaspersky Endpoint Agent.

Kaspersky Endpoint Security obsługuje aktualizację bez ponownego uruchamiania komputera. Możesz wybrać tryb aktualizacji aplikacji we właściwościach zasad.

5 Sprawdzanie działania aplikacji

Jeśli po instalacji lub aktualizacji aplikacji komputer posiada stan *Krytyczny* w konsoli Kaspersky Security Center:

- Upewnij się, że na komputerze jest zainstalowany Agent sieciowy w wersji 13.2 lub wyższej.
- Sprawdź stan działania komponentów, przeglądając *Raport o stanie składników aplikacji*. Jeśli komponent ma stan *Nie zainstalowano*, zainstaluj komponent przy użyciu zadania *Zmiana składników aplikacji*. Jeśli komponent ma stan *Nieobjęte licencją*, upewnij się, że aktywowano wbudowaną funkcję agenta.
- Upewnij się, że akceptujesz Oświadczenie Kaspersky Security Network w nowej zasadzie Kaspersky Endpoint Security for Windows.

6 Sprawdzanie połączenia z serwerem Kaspersky Anti Targeted Attack Platform

Sprawdź połączenie z serwerem Kaspersky Anti Targeted Attack Platform. W tym celu:

1. Sprawdź, czy masz ważny certyfikat.
2. Sprawdź ustawienia połączenia z serwerem.
3. Sprawdź dziennik zdarzeń.

   W przypadku nawiązania połączenia z serwerem aplikacja wysyła zdarzenie *Pomyślne połączenie z serwerem EDR Expert*. Jeśli nie ma zdarzenia udanego połączenia i nie ma zdarzeń z błędami połączenia, sprawdź ustawienia dziennika zdarzeń i włącz wysyłanie zdarzeń dla Endpoint Detection and Response (KATA).

Stan połączenia z serwerem nie wpływa na stan komputera w konsoli Kaspersky Security Center. Dlatego, jeśli nie ma połączenia z serwerem, komputer nadal może mieć status *OK*. Sprawdź dziennik zdarzeń, aby zweryfikować połączenie z serwerem.

7 Sprawdzanie działania

Jeśli wydajność komputera spadła po zainstalowaniu lub zaktualizowaniu aplikacji, możesz zoptymalizować transfer danych. W tym celu:

1. Wyłącz komponent EDR (KATA) i sprawdź, czy spadek wydajności jest spowodowany przez EDR (KATA).
2. W przypadku zaufanych aplikacji wyłącz zbieranie danych telemetrycznych dla czynności wprowadzania danych konsoli (domyślnie włączone).

3. Dodaj aplikacje, które zmniejszają wydajność komputera do listy zaufanych aplikacji.

4. Skontaktuj się z pomocą techniczną Kaspersky. Eksperci pomocy technicznej pomogą Ci skonfigurować filtrowanie danych telemetrycznych w Kaspersky Anti Targeted Attack Platform. Zmniejszy to natężenie ruchu. Jeśli określona aplikacja ma wpływ na wydajność komputera, dołącz do wniosku pakiet dystrybucyjny tej aplikacji.

Endpoint Detection and Response Expert (on-premises)



Kaspersky Endpoint Security for Windows obsługuje integrację z rozwiązaniem Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* to korporacyjne rozwiązanie z zakresu bezpieczeństwa cybernetycznego obejmujące aplikacje Kaspersky, które umożliwiają organizacji obronę przed większością typów zagrożeń cybernetycznych i obejmują najważniejsze scenariusze rozprzestrzeniania się zagrożeń. Komponenty EDR Expert (on-premises) są wdrażane na platformie OSMP (Open Single Management Platform). Platforma ta obsługuje scenariusze wieloplatformowe w ramach jednego interfejsu i umożliwia integrację aplikacji Kaspersky z aplikacjami innych firm w ramach jednego kompleksowego systemu bezpieczeństwa.

Jednym z centralnych elementów rozwiązania jest *SIEM*. SIEM śledzi zdarzenia pochodzące ze wszystkich komponentów i koreluje je ze sobą, wykorzystując reguły zdefiniowane przez dostawcę i użytkownika. Rozwiązanie EDR Expert (on-premises) analizuje logi i dane telemetryczne otrzymane z infrastruktury korporacyjnej w celu automatycznego wykrywania ataków i umożliwia badanie incydentów przy użyciu ujednoliconego wykresu dochodzeniowego, który łączy wszystkie zdarzenia zebrane w rozwiązaniu EDR Expert (on-premises), w tym zdarzenia z aplikacji firmy Kaspersky i produktów zabezpieczających informacje innych firm.

W przypadku zaawansowanych incydentów rozwiązanie EDR Expert (on-premises) wykorzystuje scenariusze wstępnie ustawione i zdefiniowane przez użytkownika. Można również wykorzystać akcje reagowania z aplikacji innych firm i scenariusze reagowania obejmujące wiele aplikacji.

Narzędzia analizy zagrożeń

Kaspersky Endpoint Detection and Response używa następujących narzędzi Threat Intelligence:

- Integracja z portalem Kaspersky Threat Intelligence Portal, który zawiera i wyświetla informacje o reputacji plików i adresów sieciowych.
- Baza danych Kaspersky Threats.
- Infrastruktura usługi chmury Kaspersky Security Network (zwana dalej również „KSN"), która zapewnia dostęp do informacji o reputacji pliku, strony internetowej i oprogramowania w czasie rzeczywistym z bazy wiedzy Kaspersky. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji firmy Kaspersky na zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie prawdopodobieństwa wystąpienia fałszywych alarmów.

Zasada działania rozwiązania

Aplikacja Kaspersky Endpoint Security jest instalowana na pojedynczych komputerach w korporacyjnej infrastrukturze IT i cały czas monitoruje procesy, otwiera połączenia sieciowe i modyfikowane pliki.

Po zainstalowaniu w trybie standardowym w infrastrukturze VDI program Kaspersky Endpoint Security obsługuje integrację z rozwiązaniem EDR Expert (on-premises). Nie gwarantujemy jednak działania pozostałych funkcjonalności aplikacji. Aby chronić maszyny wirtualne w infrastrukturze VDI, zalecamy korzystanie z Kaspersky Endpoint Security w trybie Light Agent.

Informacje o zdarzeniach na komputerze (telemetria) są przesyłane do serwera EDR Expert (on-premises). W takim przypadku Kaspersky Endpoint Security wysyła również do serwerów gromadzących dane telemetryczne informacje o zagrożeniach wykrytych przez aplikację oraz informacje o wynikach przetwarzania tych zagrożeń.

Integracja EDR Expert (on-premises) jest konfigurowana na konsoli Kaspersky Security Center. Wbudowany agent jest następnie zarządzany przy użyciu Open Single Management Platform (OSMP), co obejmuje uruchamianie zadań, zarządzanie obiektami poddanymi kwarantannie, przeglądanie raportów i inne działania.

Konfiguracje Kaspersky Endpoint Security do pracy z EDR Expert (on-premises)

Do pracy z EDR Expert (on-premises) można zastosować następujące konfiguracje:

- **[KES+wbudowany agent]**. W tej konfiguracji Kaspersky Endpoint Security działa zarówno jako aplikacja zapewniająca bezpieczeństwo komputera, jak i aplikacja do pracy z EDR Expert (on-premises). Wbudowany agent EDR Expert (on-premises) jest dostępny w programie Kaspersky Endpoint Security 12.11 for Windows lub nowszym.
- **[zewnętrzny agent EPP+EDR]**. W tej konfiguracji bezpieczeństwo infrastruktury IT zapewnia zewnętrzna platforma Endpoint Protection Platform (EPP). Interakcja z EDR Expert (on-premises) jest zapewniana przez Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent (EDR Agent). W tej konfiguracji EDR Agent jest kompatybilny z aplikacjami EPP innych firm. EDR Agent dla EDR Expert (on-premises) jest dostępny w Kaspersky Endpoint Security 12.11 for Windows lub nowszym.

Integracja wbudowanego agenta z EDR Expert (on-premises)

Aby przeprowadzić integrację z rozwiązaniem Kaspersky Endpoint Detection and Response Expert (on-premises), należy dodać komponent Endpoint Detection and Response Expert (on-premises) i skonfigurować Kaspersky Endpoint Security.

Komponenty Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) i Endpoint Detection and Response Expert (on-premises) nie są ze sobą kompatybilne.

W celu zapewnienia działania Endpoint Detection and Response Expert (on-premises) muszą być spełnione następujące warunki:

- Zainstalowana jest platforma OSMP (Open Single Management Platform).
- Aplikacja jest aktywowana, a funkcjonalność jest objęta licencją.
- Komponent Endpoint Detection and Response Expert (on-premises) jest włączony.
- Komponenty aplikacji zapewniające działanie EDR Expert (on-premises) są włączone i działają. Działanie EDR Expert (on-premises) zapewniają następujące komponenty:
  - Ochrona plików.
  - Ochrona WWW.
  - Ochrona poczty.
  - Ochrona przed exploitami.
  - Wykrywanie zachowań.
  - Ochrona przed włamaniami.
  - Silnik korygujący.
  - Adaptacyjna kontrola anomalii.

Konfiguracja integracji EDR Expert (on-premises) obejmuje następujące kroki:

1. **Instalowanie komponentu EDR Expert (on-premises)**

   Możesz wybrać składnik EDR Expert (on-premises) podczas instalacji lub aktualizacji, a także przy użyciu zadania *Zmiana składników aplikacji*.

   > Musisz ponownie uruchomić komputer, aby dokończyć aktualizację aplikacji o nowe komponenty.

2. **Aktywowanie Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Należy zakupić osobną licencję w celu korzystania z EDR Expert (on-premises) (dodatek Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Funkcja będzie dostępna po dodaniu oddzielnego klucza dla Kaspersky Endpoint Detection and Response Expert (on-premises). W rezultacie na komputerze dodane zostają dwa klucze: klucz dla Kaspersky Endpoint Security i klucz dla Kaspersky Endpoint Detection and Response Expert (on-premises).

   Licencjonowanie dla autonomicznej funkcjonalności Endpoint Detection and Response Expert (on-premises) jest takie samo jak w przypadku licencjonowania Kaspersky Endpoint Security.

   Upewnij się, że funkcja EDR Expert (on-premises) znajduje się w licencji i jest uruchomiona w lokalnym interfejsie aplikacji.

3. **Nawiązywanie połączenia z serwerem gromadzącym dane telemetryczne i serwerem odpowiedzi**

Kaspersky Endpoint Detection and Response Expert (on-premises) wymaga zaufanego połączenia między rozwiązaniem Kaspersky Endpoint Security a dwoma serwerami:

- *Serwer gromadzenia danych telemetrycznych* jest serwerem stanowiącym część rozwiązania SIEM, które zbiera, normalizuje, koreluje, analizuje i przechowuje informacje o zdarzeniach mających miejsce na komputerze.

- *Serwer odpowiedzi* jest serwerem służącym do odbierania i skanowania danych, badania zachowań obiektów i publikowania wyników tych badań.

Aby skonfigurować zaufane połączenie, musisz użyć certyfikatu TLS. Certyfikat TLS można uzyskać na platformie Open Single Management Platform (instrukcje można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)). Następnie musisz dodać certyfikat TLS do Kaspersky Endpoint Security (zobacz instrukcje poniżej).

Domyślnie Kaspersky Endpoint Security sprawdza tylko certyfikat TLS serwerów. Aby połączenie było bezpieczniejsze, możesz dodatkowo włączyć weryfikację komputera na serwerze (uwierzytelnianie dwukierunkowe). Aby włączyć tę weryfikację, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera i Kaspersky Endpoint Security. Aby korzystać z uwierzytelniania dwukierunkowego, potrzebujesz również kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać na platformie Open Single Management Platform (instrukcje znajdują się w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)).

Jak połączyć komputer Kaspersky Endpoint Security z platformą EDR Expert (on-premises) przy użyciu Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Konfiguracja wbudowanych agentów → Endpoint Detection and Response Expert (on-premise)**.

5. Włącz przełącznik **Endpoint Detection and Response Expert (on-premise) WŁĄCZONO**.

6. Aby skonfigurować EDR Expert (on-premises), wybierz **Endpoint Detection and Response Expert (wersja 8.0 lub nowsze)** z listy rozwiązań.

7. Skonfiguruj połączenie z *serwerami gromadzącymi dane telemetryczne*:

   a. W sekcji **Połączenie z serwerami gromadzenia danych telemetrycznych** kliknij odnośnik **Ustawienia połączenia**.

   b. Skonfiguruj połączenie z serwerami gromadzącymi dane telemetryczne:

   - **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem.

   - **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem. Certyfikat TLS można uzyskać na platformie Open Single Management Platform (instrukcje można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera, a następnie uzyskać kontener kryptograficzny i ustawić hasło chroniące kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać na platformie Open Single Management Platform (instrukcje znajdują się w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)). Po skonfigurowaniu ustawień serwera należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener szyfrowania.

  Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.

c. Kliknij **OK**.

d. Dodaj serwery gromadzące dane telemetryczne. W tym celu należy określić adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.

Można dodać wiele adresów serwerów gromadzących dane telemetryczne. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.

e. W razie potrzeby skonfiguruj telemetrię.

8. Skonfiguruj połączenie z *serwerami odpowiedzi*:

a. W sekcji **Połączenie z serwerami odpowiedzi** skonfiguruj połączenie **Wysyłaj żądanie synchronizacji do serwera co (min)**. Częstotliwość żądań synchronizacji wysyłanych do serwera. Podczas synchronizacji program Kaspersky Endpoint Security odbiera zadania reagowania na zagrożenia i wysyła wyniki zadań.

b. Kliknij odnośnik **Ustawienia połączenia**.

c. Skonfiguruj połączenie z serwerami odpowiedzi:

- **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem.

- **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem. Certyfikat TLS można uzyskać na platformie Open Single Management Platform (instrukcje można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera, a następnie uzyskać kontener kryptograficzny i ustawić hasło chroniące kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać na platformie Open Single Management Platform (instrukcje znajdują się w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)). Po skonfigurowaniu ustawień serwera należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener szyfrowania.

  Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.

d. Kliknij **OK**.

e. Dodaj serwery odpowiedzi. W tym celu należy określić adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.

   Można dodać wiele adresów serwerów odpowiedzi. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.

9. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

W rezultacie komputer zostaje dodany do listy zarządzanych urządzeń na platformie Open Single Management Platform (OSMP). Sprawdź stan działania komponentu, przeglądając *Raport o stanie składników aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Endpoint Detection and Response Expert (on-premises)** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

Konfigurowanie ustawień telemetrii EDR Expert (on-premises)

Telemetria to lista zdarzeń, które wystąpiły na chronionym komputerze. Kaspersky Endpoint Security analizuje dane telemetryczne i wysyła je do serwerów gromadzących dane telemetryczne podczas synchronizacji. Zdarzenia telemetryczne docierają do serwera prawie nieprzerwanie. Kaspersky Endpoint Security inicjuje synchronizację z serwerem, gdy spełniony jest jeden z następujących warunków:

- Upłynął interwał synchronizacji.
- Liczba zdarzeń w buforze przekracza górną granicę.

Dlatego domyślnie aplikacja synchronizuje się co 30 sekund lub zawsze, gdy w buforze znajdują się 1024 zdarzenia. Możesz skonfigurować sposób synchronizacji w zasadzie Kaspersky Endpoint Security i wybrać optymalne wartości odpowiadające obciążeniu sieci (zobacz instrukcje poniżej).

Jeśli nie ma połączenia między Kaspersky Endpoint Security a serwerem, aplikacja umieszcza nowe zdarzenia w kolejce. Po przywróceniu połączenia Kaspersky Endpoint Security wysyła zdarzenia z kolejki do serwera w odpowiedniej kolejności. Aby uniknąć przeciążenia serwera, Kaspersky Endpoint Security może pominąć niektóre zdarzenia. Aby to włączyć, możesz zoptymalizować ustawienia transmisji zdarzeń, na przykład ustawić maksymalną liczbę zdarzeń na godzinę (patrz instrukcje poniżej).

Aby skonfigurować ustawienia telemetrii, wykonaj następujące kroki:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Endpoint Detection and Response Expert (on-premise)**.
5. Aby skonfigurować EDR Expert (on-premises), wybierz **Endpoint Detection and Response Expert (wersja 8.0 lub nowsze)** z listy rozwiązań.
6. Upewnij się, że pole wyboru **Wyślij dane telemetryczne do serwerów gromadzenia danych telemetrycznych** jest zaznaczone w sekcji **Ustawienia przesyłania danych**.
7. Jeśli to konieczne, zaznacz pole wyboru **Wysyłaj telemetrię tylko za pomocą wskaźnika IOA**. *Wskaźnik ataku (IOA)* jest regułą zawierającą opis podejrzanego zachowania w systemie, które może wskazywać na ukierunkowany atak. Aplikacja porównuje bieżące zachowanie systemu z tymi regułami i rejestruje zdarzenia wskazujące na ukierunkowany atak. Aplikacja wykorzystuje technologię *skanowania strumieniowego* umożliwiającą śledzenie takich zdarzeń w czasie rzeczywistym.
8. W razie potrzeby skonfiguruj synchronizację z ustawieniami serwera w sekcji **Ustawienia przesyłania danych**:

   - **Maksymalne opóźnienie transmisji zdarzeń (s)**. Aplikacja synchronizuje się z serwerem w celu wysyłania zdarzeń po wygaśnięciu przedziału synchronizacji. Domyślnie ustawienie to 30 sekund.
   - **Maksymalna liczba pakietów zdarzeń**. Aplikacja synchronizuje się z serwerem, gdy bufor zostanie zapełniony zdarzeniami. Domyślnie ustawienie to 1024 zdarzenia.
9. W razie potrzeby wyczyść pole wyboru **Włącz ograniczanie żądań** w bloku **Ograniczanie żądań**.

   Ta funkcja pomaga zoptymalizować obciążenie serwera. Jeśli ta funkcja jest włączona, aplikacja ogranicza przesyłanie zdarzeń. Jeśli liczba zdarzeń przekroczy skonfigurowane limity, Kaspersky Endpoint Security przestanie wysyłać zdarzenia. Ta opcja jest domyślnie włączona.
10. Skonfiguruj ustawienia optymalizacji wysyłania zdarzeń na serwer:

    - **Maksymalna liczba zdarzeń na godzinę**. Aplikacja analizuje strumień danych telemetrycznych i ogranicza wysyłanie zdarzeń, jeśli strumień zdarzeń przekroczy skonfigurowany limit zdarzeń na godzinę. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń po godzinie. Ustawienie domyślne to 3000 zdarzeń na godzinę. Jeżeli aplikacja jest zainstalowana na serwerze, strumień danych telemetrycznych jest większy. W przypadku serwerów zaleca się zwiększenie wartości do 60 000 zdarzeń na godzinę.
    - **Procent przekroczenia limitu zdarzeń**. Aplikacja sortuje zdarzenia według typu (np. zdarzenia „zmiany w rejestrze") i ogranicza transmisję zdarzeń, jeśli stosunek zdarzeń tego samego typu do całkowitej liczby zdarzeń przekroczy skonfigurowany limit w procentach. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń, gdy stosunek innych zdarzeń do łącznej liczby zdarzeń ponownie stanie się wystarczająco duży. Ustawienie domyślne to 15%.
11. W sekcji **Połączenie z serwerami odpowiedzi** wprowadź wartość dla parametru **Wysyłaj żądanie synchronizacji do serwera co (min)**.

12. Częstotliwość żądań synchronizacji wysyłanych do serwera. Podczas synchronizacji Kaspersky Endpoint Security wysyła informacje o zmodyfikowanych ustawieniach i zadaniach aplikacji.

13. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Wykluczenia telemetrii EDR Expert (on-premises)

Aby poprawić wydajność i zoptymalizować transmisję danych do serwera gromadzenia danych telemetrycznych, możesz dodać wykluczenia telemetryczne. Można na przykład zrezygnować z wysyłania danych komunikacyjnych sieci dla poszczególnych aplikacji.

Użycie zbyt wielu reguł może zwiększyć obciążenie serwera gromadzenia danych telemetrii i obniżyć wydajność komputera. Zalecamy dodawanie tylko niezbędnych reguł.

Tworzenie wykluczenia telemetrycznego w Web Console i Cloud Console:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne** → **Ustawienia telemetrii**.

5. Wybierz zakładkę **Telemetria EDR Expert (on-premise)**.

6. W sekcji **Wykluczenia ogólne** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Dodaj regułę wykluczania**.

7. W razie potrzeby zmień status reguły. Domyślnie ta reguła jest włączona.

8. Wprowadź nazwę reguły.

9. Wybierz akcję, która ma zostać wykonana po wyzwoleniu tej reguły:

   - **Nie gromadź**. Odfiltrowane zdarzenie zostanie wykluczone z wysyłanych danych telemetrycznych.

   - **Wyklucz IOA**. Zdarzenie wyzwalające regułę IOA zostanie wykluczone z wysyłanych danych telemetrycznych.

10. Jeśli wybrano opcję **Wyklucz IOA**, określ reguły IOA, które mają zostać dodane do wykluczeń:

    - **Wyklucz wszystko**. Jeśli spełniony zostanie określony warunek, aplikacja wykluczy z danych telemetrycznych zdarzenia wygenerowane na podstawie wszystkich reguł IOA.

    - **Wyklucz wg GUID**. Podaj identyfikator GUID reguły IOA. Można określić wiele identyfikatorów GUID za pomocą `,`. Aby uzyskać więcej szczegółów na temat zasad IOA, zapoznaj się z pomocą do EDR Expert (on-premises).

11. Określ warunek filtrowania:

    a. Wybierz nazwę pola, które będzie używane do filtrowania.

    b. Wybierz operator (zobacz tabelę poniżej) i określ wartość, z którą będzie porównywana wartość pola ze zdarzenia.

Lista operatorów warunkowych

Operator	Opis
<	Jeśli wartość pola jest mniejsza od wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
≤	Jeśli wartość pola jest mniejsza lub równa wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
=	Jeżeli wartość pola jest równa wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
≥	Jeżeli wartość pola jest większa lub równa wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
>	Jeśli wartość pola jest większa od wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
≠	Jeżeli wartość pola nie jest równa wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
jest jak	Jeśli wartość pola jest zgodne z maską określoną w warunku, zdarzenie zostanie odfiltrowane. Ta aplikacja obsługuje znaki `*` i `?` podczas wprowadzania maski:
nie jest jak	Jeśli wartość pola jest niezgodna z maską określoną w warunku, zdarzenie zostanie odfiltrowane. Ta aplikacja obsługuje znaki `*` i `?` podczas wprowadzania maski:
jedno z	Jeżeli wartość pola jest zgodna z jedną z wartości na liście określonej w warunku, zdarzenie jest uznawane za odfiltrowane.
żadne z	Jeżeli wartość pola jest niezgodna z żadną z wartości na liście określonej w warunku, zdarzenie jest uznawane za odfiltrowane.
jest jak jeden z	Jeśli wartość pola jest zgodna z jedną z masek określonych w warunku, zdarzenie zostanie odfiltrowane. Aplikacja ta obsługuje znaki * i ? podczas wprowadzania maski.
nie jest jak jeden z	Jeśli wartość pola jest niezgodna z żadną z masek określonych w warunku, zdarzenie zostanie odfiltrowane. Aplikacja ta obsługuje znaki * i ? podczas wprowadzania maski.
istnieje	Jeśli pole określone w warunku występuje w zdarzeniu, to zdarzenie zostanie odfiltrowane.
nie istnieje	Jeżeli pole określone w warunku nie występuje w zdarzeniu, to zdarzenie zostanie odfiltrowane.
zawiera	Jeżeli wartość określona w warunku znajduje się w wartości pola, to zdarzenie zostanie odfiltrowane.
jest równy	Jeżeli wartość pola jest równa wartości określonej w warunku, zdarzenie zostanie odfiltrowane. Podczas skanowania nie jest uwzględniana wielkość liter.
bitowy AND	Jeżeli wynik operacji bitowej AND (&) pomiędzy wartością pola i wartością określoną w warunku wynosi 1, to zdarzenie zostanie odfiltrowane.

12. W razie potrzeby możesz utworzyć złożone kryteria filtrowania, dodając wiele warunków filtrowania i grup warunków. Do grupy warunków można również dodać zagnieżdżone warunki i grupy warunków. Możesz użyć następujących operatorów:

    - **AND** oznacza, że filtr wybiera zdarzenia spełniające wszystkie określone warunki.
    - **OR** oznacza, że filtr wybiera zdarzenia spełniające jeden z określonych warunków.
    - **NOT** (aby użyć tego operatora, wybierz opcję **Dodaj NOT przed**) oznacza, że filtr wybiera zdarzenia, które nie spełniają żadnego ze wskazanych warunków.

    Warunki i grupy warunków pierwszego poziomu są łączone za pomocą operatora **AND**.

13. Jeśli na Twoim komputerze działa platforma OSMP (Open Single Management Platform), możesz przeskanować utworzoną regułę filtrowania. Aby uruchomić skanowanie, kliknij przycisk **Sprawdź regułę**.

    W oknie, które zostanie otwarte, wyświetli się tabela zdarzeń przefiltrowanych przez utworzoną regułę. Aby uzyskać więcej szczegółów, zapoznaj się z pomocą do EDR Expert (on-premises).

14. W razie potrzeby w obszarze **Wszystkie typy zdarzeń** dodaj wykluczenia telemetrii według typu zdarzenia.

    a. Kliknij nazwę typu zdarzenia.

    b. W otwartym oknie kliknij przycisk **Skonfiguruj ręcznie**.

    c. W razie potrzeby skonfiguruj transmisję telemetryczną dla wybranego typu zdarzenia za pomocą przełącznika **Wyślij zdarzenie**. Domyślnie transmisja telemetryczna jest włączona dla wszystkich typów zdarzeń.

    d. W sekcji **Reguły wykluczania** kliknij przycisk **Dodaj**.

    Zostanie otwarte okno **Dodaj regułę wykluczania**.

    e. Dla każdej dodawanej reguły wykonaj czynności opisane w krokach 7–13.

15. W przypadku niektórych typów zdarzeń możesz również dodać reguły uwzględniania, aby rozszerzyć zakres zbieranych danych telemetrycznych:

    a. W sekcji **Reguły włączania** kliknij przycisk **Dodaj**.

    Zostanie otwarte okno **Dodaj regułę włączania**.

    b. Wprowadź nazwę reguły.

    c. W obszarze **Warunek** wprowadź wartości dla wyświetlanych pól. Typ dostępnych pól zależy od wybranego zdarzenia.

> Reguły wykluczania mają pierwszeństwo przed regułami włączania.

16. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Eksportowanie i importowanie filtrów zdarzeń EDR Expert (on-premises)

Możesz wyeksportować listę wykluczeń do pliku JSON. Następnie możesz zmodyfikować plik, na przykład, aby dodać dużą liczbę identyfikatorów zdarzeń. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej filtrów zdarzeń lub przeniesienia listy na inny serwer.

> Użycie zbyt wielu reguł może zwiększyć obciążenie serwera gromadzenia danych telemetrii i obniżyć wydajność komputera. Zalecamy dodawanie tylko niezbędnych reguł.

Jak eksportować i importować filtry zdarzeń w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Ustawienia ogólne → Wykluczenia i typy obiektów**.

5. W sekcji **Ustawienia telemetrii → Telemetria EDR Expert (on-premises)** kliknij przycisk **Ustawienia**.

6. Aby wyeksportować filtry zdarzeń:

   a. Kliknij **Eksportuj**.

   W otwartym oknie określ nazwę pliku JSON, do którego chcesz wyeksportować filtry zdarzeń, i wybierz folder, w którym chcesz zapisać ten plik.

   b. Zapisz plik.

   Kaspersky Endpoint Security eksportuje filtry zdarzeń do pliku JSON.

7. Aby zaimportować filtry zdarzeń:

   a. Kliknij **Importuj**.

   b. W oknie, które się otworzy, wybierz plik JSON, z którego chcesz zaimportować filtry zdarzeń.

   c. Otwórz plik.

   Jeśli na komputerze istnieją już reguły filtrowania zdarzeń, Kaspersky Endpoint Security zastąpi je podczas importowania.

8. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak eksportować i importować filtry zdarzeń w Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne → Ustawienia telemetrii**.

5. Wybierz zakładkę **Telemetria EDR Expert (on-premise)**.

6. Aby wyeksportować filtry zdarzeń:

   a. Kliknij **Eksportuj**.

   b. W otwartym oknie określ nazwę pliku JSON, do którego chcesz wyeksportować filtry zdarzeń, i wybierz folder, w którym chcesz zapisać ten plik.

   c. Zapisz plik.

   Kaspersky Endpoint Security eksportuje filtry zdarzeń do pliku JSON.

7. Aby zaimportować filtry zdarzeń:

   a. Kliknij **Importuj**.

   b. W oknie, które się otworzy, wybierz plik JSON, z którego chcesz zaimportować filtry zdarzeń.

c. Wybierz, w jaki sposób chcesz importować reguły filtrowania zdarzeń: dodając je do istniejących reguł lub odrzucając istniejące reguły i zastępując je nowymi.

d. Otwórz plik.

8. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Możesz również eksportować lub importować filtry zdarzeń w wierszu poleceń.

Szczególne uwagi dotyczące używania profili zasad do konfigurowania integracji z EDR Expert (on-premises) i EDR (KATA)

Aby skonfigurować integrację z EDR (KATA) dla niektórych grup administracyjnych i z EDR Expert (on-premises) dla innych w ramach jednej zasady, należy użyć profili zasad. Ustawienia integracji z EDR (KATA) należy skonfigurować we właściwościach zasady, a integrację z EDR Expert (on-premises) dla wybranych grup administracyjnych należy skonfigurować we właściwościach profilu zasad.

Korzystanie z profili zasad do konfigurowania integracji z EDR Expert (on-premises) ma następujące ograniczenia:

- Jeśli integracja z EDR Expert (on-premises) zostanie skonfigurowana we właściwościach zasady, ustawienia te będą stosowane do wszystkich grup administracyjnych; ustawienia integracji z profili zasad nie zostaną zastosowane.

- Podczas korzystania z profili zasad do konfigurowania integracji z EDR Expert (on-premises) nie można używać Konsoli administracyjnej (MMC) do zarządzania zasadami. Po otwarciu właściwości zasady w Konsoli administracyjnej ustawienia integracji z EDR Expert (on-premises) w profilach zasad zostaną zastąpione ustawieniami z zasady, co spowoduje nieprawidłowe działanie komponentu. Konieczne będzie zresetowanie ustawień komponentu Endpoint Detection and Response Expert (on-premises) zgodnie z poniższą instrukcją.

- Podczas korzystania z profili zasad do konfigurowania integracji z EDR Expert (on-premises) nie można używać zasad podrzędnych.

Jeśli zasada została już skonfigurowana w poprzedniej wersji wtyczki webowej, należy zresetować ustawienia komponentu Endpoint Detection and Response Expert (on-premises), aby zastosować ustawienia integracji z EDR Expert (on-premises) do zarządzanych urządzeń z profili zasad.

Aby zresetować ustawienia komponentu:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Konfiguracja wbudowanych agentów** → **Endpoint Detection and Response Expert (on-premise)**.

5. Zmień tryb działania z **Endpoint Detection and Response Expert (wersja 7.1 lub starsze)** na **Tryb Endpoint Detection and Response Expert (wersja 8.0 lub nowsze)**.

6. Przełącz z powrotem na **Endpoint Detection and Response Expert (wersja 7.1 lub starsze)**.

7. Zapisz swoje zmiany.

Endpoint Detection and Response Expert (cloud)

Integracja Kaspersky Endpoint Security for Windows z Kaspersky Endpoint Detection and Response Expert (cloud) jest tymczasowo niedostępna. Wsparcie tej funkcjonalności planowane jest na koniec 2026 roku. Śledź nasze informacje o wydaniach, aby być na bieżąco z aktualizacjami aplikacji i nowymi funkcjami.



Kaspersky Endpoint Security for Windows obsługuje integrację z rozwiązaniem Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* to oparte na chmurze korporacyjne rozwiązanie z zakresu bezpieczeństwa cybernetycznego obejmujące aplikacje Kaspersky, które umożliwiają organizacji obronę przed większością typów zagrożeń cybernetycznych i obejmują najważniejsze scenariusze rozprzestrzeniania się zagrożeń. Komponenty EDR Expert (cloud) są wdrażane na platformie OSMP (Open Single Management Platform). Platforma ta obsługuje scenariusze wieloplatformowe w ramach jednego interfejsu i umożliwia integrację aplikacji Kaspersky z aplikacjami innych firm w ramach jednego kompleksowego systemu bezpieczeństwa.

Integracja z Kaspersky Endpoint Detection and Response Expert (cloud) nie jest obsługiwana na komputerach opartych na architekturze Arm.

Jednym z centralnych elementów rozwiązania jest *SIEM*. SIEM śledzi zdarzenia pochodzące ze wszystkich komponentów i koreluje je ze sobą, wykorzystując reguły zdefiniowane przez dostawcę i użytkownika. Rozwiązanie EDR Expert (cloud) analizuje logi i dane telemetryczne otrzymane z infrastruktury korporacyjnej w celu automatycznego wykrywania ataków i umożliwia badanie incydentów przy użyciu ujednoliconego wykresu dochodzeniowego, który łączy wszystkie zdarzenia zebrane w rozwiązaniu EDR Expert (cloud), w tym zdarzenia z aplikacji firmy Kaspersky i produktów zabezpieczających informacje innych firm.

W przypadku zaawansowanych incydentów rozwiązanie EDR Expert (cloud) wykorzystuje scenariusze wstępnie ustawione i zdefiniowane przez użytkownika. Można również wykorzystać akcje reagowania z aplikacji innych firm i scenariusze reagowania obejmujące wiele aplikacji.

Narzędzia analizy zagrożeń

Kaspersky Endpoint Detection and Response używa następujących narzędzi Threat Intelligence:

- Integracja z portalem Kaspersky Threat Intelligence Portal, który zawiera i wyświetla informacje o reputacji plików i adresów sieciowych.
- Baza danych Kaspersky Threats.
- Infrastruktura usługi chmury Kaspersky Security Network (zwana dalej również „KSN"), która zapewnia dostęp do informacji o reputacji pliku, strony internetowej i oprogramowania w czasie rzeczywistym z bazy wiedzy Kaspersky. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji firmy Kaspersky na zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie prawdopodobieństwa wystąpienia fałszywych alarmów.

Zasada działania rozwiązania

Aplikacja Kaspersky Endpoint Security jest instalowana na pojedynczych komputerach w korporacyjnej infrastrukturze IT i cały czas monitoruje procesy, otwiera połączenia sieciowe i modyfikowane pliki.

Informacje o zdarzeniach na komputerze (telemetria) są przesyłane do serwera EDR Expert (cloud). W takim przypadku Kaspersky Endpoint Security wysyła również do serwerów gromadzących dane telemetryczne informacje o zagrożeniach wykrytych przez aplikację oraz informacje o wynikach przetwarzania tych zagrożeń.

Integracja EDR Expert (cloud) jest konfigurowana na konsoli Kaspersky Security Center. Wbudowany agent jest następnie zarządzany przy użyciu Open Single Management Platform (OSMP), co obejmuje uruchamianie zadań, zarządzanie obiektami poddanymi kwarantannie, przeglądanie raportów i inne działania.

Integracja wbudowanego agenta z EDR Expert (cloud)

Aby skonfigurować integrację z rozwiązaniem Kaspersky Endpoint Detection and Response (cloud), należy zainstalować komponent Endpoint Detection and Response Expert (cloud) i skonfigurować Kaspersky Endpoint Security.

Komponenty Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) i Endpoint Detection and Response Expert (on-premises) nie są ze sobą kompatybilne.

Warunki działania EDR Expert (cloud)

Aby rozwiązanie EDR Expert (cloud) działało, muszą być spełnione następujące warunki:

- Infrastruktura Kaspersky Endpoint Detection and Response Expert (cloud) jest dostępna w Twoim regionie. Aby uzyskać informacje na temat dostępności infrastruktury EDR Expert (cloud) w Twoim regionie, skontaktuj się z działem pomocy technicznej.
- Zainstalowana jest platforma OSMP (Open Single Management Platform).
- Kaspersky Endpoint Security zainstalowany w trybie standardowym.
- Aplikacja Kaspersky Endpoint Security jest aktywowana, a funkcjonalność jest objęta licencją.
- Zaakceptowano warunki Umowy o przetwarzaniu danych dla Kaspersky Endpoint Detection and Response Expert (cloud).
- Endpoint Detection and Response Expert (cloud) – komponent jest włączony.
- Komponenty aplikacji zapewniające działanie EDR Expert (cloud) są włączone i działają:
  - Ochrona plików.
  - Ochrona WWW.

- Ochrona poczty.
- Ochrona przed exploitami.
- Wykrywanie zachowań.
- Ochrona przed włamaniami.
- Silnik korygujący.
- Adaptacyjna kontrola anomalii.

Kroki integracji z EDR Expert (cloud)

Konfiguracja integracji EDR Expert (cloud) obejmuje następujące kroki:

1. **Instalacja komponentu Endpoint Detection and Response Expert (cloud)**

   Możesz wybrać komponent Endpoint Detection and Response Expert (cloud) podczas instalacji lub aktualizacji, a także w przypadku korzystania z zadania *Zmiana składników aplikacji*.

   > Musisz ponownie uruchomić komputer, aby dokończyć aktualizację aplikacji o nowe komponenty.

2. **Aktywowanie Kaspersky Endpoint Detection and Response Expert (cloud)**

   Musisz zakupić osobną licencję na Kaspersky Endpoint Detection and Response Expert (cloud).

   Funkcja będzie dostępna po dodaniu oddzielnego klucza dla Kaspersky Endpoint Detection and Response Expert (cloud). W rezultacie na komputerze dodane zostają dwa klucze: klucz dla Kaspersky Endpoint Security i klucz dla Kaspersky Endpoint Detection and Response Expert (cloud).

   Licencjonowanie dla autonomicznej funkcjonalności Endpoint Detection and Response Expert (cloud) jest takie samo jak w przypadku licencjonowania Kaspersky Endpoint Security.

   Upewnij się, że funkcja EDR Expert (cloud) znajduje się w licencji i jest uruchomiona w lokalnym interfejsie aplikacji.

3. **Nawiązywanie połączenia z serwerem gromadzącym dane telemetryczne i serwerem odpowiedzi**

   Kaspersky Endpoint Detection and Response Expert (cloud) wymaga zaufanego połączenia między rozwiązaniem Kaspersky Endpoint Security a dwoma serwerami:

   - *Serwer gromadzenia danych telemetrycznych* jest serwerem stanowiącym część rozwiązania SIEM, które zbiera, normalizuje, koreluje, analizuje i przechowuje informacje o zdarzeniach mających miejsce na komputerze.
   - *Serwer odpowiedzi* jest serwerem służącym do odbierania i skanowania danych, badania zachowań obiektów i publikowania wyników tych badań.

   Jak połączyć komputer Kaspersky Endpoint Security z platformą EDR Expert (cloud) przy użyciu Web Console

   1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
   2. Kliknij nazwę zasady Kaspersky Endpoint Security.

      Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Konfiguracja wbudowanych agentów → Endpoint Detection and Response Expert (cloud)**.

5. Włącz komponent za pomocą przełącznika **Endpoint Detection and Response Expert (cloud) WYŁĄCZONO**.

6. Jeżeli bieżąca zasada jest zasadą potomną, a zasada nadrzędna zabrania wprowadzania zmian w ustawieniach integracji EDR Expert (cloud) (zamknięta „kłódka"), możesz skonfigurować dziedziczenie ustawień w sekcji **Dziedziczenie**:

   - **Dziedzicz ustawienia połączenia z zasad** (wartość domyślna). Ustawienia połączenia zostaną odziedziczone z zasady nadrzędnej. Edycja tych ustawień będzie niemożliwa.

   - **Użyj niestandardowych ustawień połączenia**. Możesz ręcznie skonfigurować ustawienia połączenia.

7. Ta karta **Serwer odpowiedzi** wyświetla w pełni kwalifikowaną nazwę domeny i port serwera odpowiedzi, które są pobierane automatycznie. Jeżeli zasada bezpieczeństwa w Twojej infrastrukturze nie pozwala na bezpośrednie połączenie z serwerami EDR Expert (cloud), możesz skonfigurować połączenie za pomocą tunelu TCP:

   a. Zaznacz pole **Użyj tunelu TCP do wysyłania odpowiedzi**.

   b. Wprowadź adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.

8. W razie potrzeby ustaw częstotliwość wysyłania żądań synchronizacji do serwera w polu **Wysyłaj żądanie synchronizacji do serwera co (min)**. Podczas synchronizacji program Kaspersky Endpoint Security odbiera zadania reagowania na zagrożenia i wysyła wyniki zadań.

9. Przejdź do zakładki **Serwer gromadzący dane telemetryczne**.

10. Skonfiguruj ustawienia połączenia z serwerem gromadzącym dane telemetryczne:

    a. Kliknij odnośnik **Edytuj**.

    b. W oknie, które zostanie otwarte, wybierz z listy serwer gromadzący dane telemetryczne. Kolektor KUMA pełni funkcję serwera gromadzącego dane telemetryczne w rozwiązaniu EDR Expert (cloud). Szczegółowe informacje można znaleźć w pomocy platformy Kaspersky Unified Monitoring and Analysis Platform.

       Jeżeli podczas łączenia się z serwerem gromadzącym dane telemetryczne wystąpi błąd, wybierz inny serwer. Jeżeli nie możesz nawiązać połączenia z serwerem gromadzącym dane telemetryczne, skontaktuj się z pomocą techniczną.

    c. W razie potrzeby możesz skonfigurować połączenie z serwerem zbierania telemetrii za pośrednictwem tunelu TCP, tak jak w przypadku serwera odpowiedzi.

11. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

W rezultacie komputer zostaje dodany do listy zarządzanych urządzeń na platformie Open Single Management Platform (OSMP). Sprawdź stan działania komponentu, przeglądając *Raport o stanie składników aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Endpoint Detection and Response Expert (cloud)** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

Konfigurowanie ustawień telemetrii EDR Expert (cloud)

Telemetria to lista zdarzeń, które wystąpiły na chronionym komputerze. Kaspersky Endpoint Security analizuje dane telemetryczne i wysyła je do serwerów gromadzących dane telemetryczne podczas synchronizacji. Zdarzenia telemetryczne docierają do serwera prawie nieprzerwanie. Kaspersky Endpoint Security inicjuje synchronizację z serwerem, gdy spełniony jest jeden z następujących warunków:

- Upłynął interwał synchronizacji.
- Liczba zdarzeń w buforze przekracza górną granicę.

Dlatego domyślnie aplikacja synchronizuje się co 30 sekund lub zawsze, gdy w buforze znajdują się 1024 zdarzenia. Możesz skonfigurować sposób synchronizacji w zasadzie Kaspersky Endpoint Security i wybrać optymalne wartości odpowiadające obciążeniu sieci (zobacz instrukcje poniżej).

Jeśli nie ma połączenia między Kaspersky Endpoint Security a serwerem, aplikacja umieszcza nowe zdarzenia w kolejce. Po przywróceniu połączenia Kaspersky Endpoint Security wysyła zdarzenia z kolejki do serwera w odpowiedniej kolejności. Aby uniknąć przeciążenia serwera, Kaspersky Endpoint Security może pominąć niektóre zdarzenia. Aby to włączyć, możesz zoptymalizować ustawienia transmisji zdarzeń, na przykład ustawić maksymalną liczbę zdarzeń na godzinę (patrz instrukcje poniżej).

Aby skonfigurować ustawienia telemetrii, wykonaj następujące kroki:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Endpoint Detection and Response Expert (cloud)**.
5. W otwartym oknie wybierz zakładkę **Ustawienia przesyłania danych**.
6. Należy upewnić się, że pole **Wysyłanie danych telemetrycznych WŁĄCZONE** jest zaznaczone.
7. Jeśli to konieczne, zaznacz pole wyboru **Wysyłaj telemetrię tylko za pomocą wskaźnika IOA**. *Wskaźnik ataku (IOA)* jest regułą zawierającą opis podejrzanego zachowania w systemie, które może wskazywać na ukierunkowany atak. Aplikacja porównuje bieżące zachowanie systemu z tymi regułami i rejestruje zdarzenia wskazujące na ukierunkowany atak. Aplikacja wykorzystuje technologię *skanowania strumieniowego* umożliwiającą śledzenie takich zdarzeń w czasie rzeczywistym.
8. W razie potrzeby skonfiguruj ustawienia synchronizacji serwera:

   - **Maksymalne opóźnienie transmisji zdarzeń (s)**. Aplikacja synchronizuje się z serwerem w celu wysyłania zdarzeń po wygaśnięciu przedziału synchronizacji. Domyślnie ustawienie to 30 sekund.
   - **Maksymalna liczba pakietów zdarzeń**. Aplikacja synchronizuje się z serwerem, gdy bufor zostanie zapełniony zdarzeniami. Domyślnie ustawienie to 1024 zdarzenia.
9. Przejdź do zakładki **Ograniczanie żądań**.

10. W razie potrzeby wyłącz ograniczanie żądań za pomocą przełącznika **Ograniczanie żądań WŁĄCZONO**.

    Ta funkcja pomaga zoptymalizować obciążenie serwera. Jeśli ta funkcja jest włączona, aplikacja ogranicza przesyłanie zdarzeń. Jeśli liczba zdarzeń przekroczy skonfigurowane limity, Kaspersky Endpoint Security przestanie wysyłać zdarzenia. Ta opcja jest domyślnie włączona.

11. Skonfiguruj ustawienia optymalizacji wysyłania zdarzeń na serwer:

    - **Maksymalna liczba zdarzeń na godzinę**. Aplikacja analizuje strumień danych telemetrycznych i ogranicza wysyłanie zdarzeń, jeśli strumień zdarzeń przekroczy skonfigurowany limit zdarzeń na godzinę. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń po godzinie. Ustawienie domyślne to 3000 zdarzeń na godzinę. Jeżeli aplikacja jest zainstalowana na serwerze, strumień danych telemetrycznych jest większy. W przypadku serwerów zaleca się zwiększenie wartości do 60 000 zdarzeń na godzinę.

    - **Procent przekroczenia limitu zdarzeń (%)**. Aplikacja sortuje zdarzenia według typu (np. zdarzenia „zmiany w rejestrze") i ogranicza transmisję zdarzeń, jeśli stosunek zdarzeń tego samego typu do całkowitej liczby zdarzeń przekroczy skonfigurowany limit w procentach. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń, gdy stosunek innych zdarzeń do łącznej liczby zdarzeń ponownie stanie się wystarczająco duży. Ustawienie domyślne to 15%.

12. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Wykluczenia telemetrii EDR Expert (cloud)

Aby poprawić wydajność i zoptymalizować transmisję danych do serwera gromadzenia danych telemetrycznych, możesz dodać wykluczenia telemetryczne. Można na przykład zrezygnować z wysyłania danych komunikacyjnych sieci dla poszczególnych aplikacji.

Użycie zbyt wielu reguł może zwiększyć obciążenie serwera gromadzenia danych telemetrii i obniżyć wydajność komputera. Zalecamy dodawanie tylko niezbędnych reguł.

Tworzenie wykluczenia telemetrycznego w Web Console i Cloud Console:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Ustawienia telemetrii**.
5. Wybierz zakładkę **Dane telemetryczne EDR Expert (cloud)**.
6. W sekcji **Wykluczenia ogólne** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Dodaj regułę wykluczania**.
7. W razie potrzeby zmień status reguły. Domyślnie ta reguła jest włączona.
8. Wprowadź nazwę reguły.

9. Wybierz akcję, która ma zostać wykonana po wyzwoleniu tej reguły:

   - **Nie gromadź**. Odfiltrowane zdarzenie zostanie wykluczone z wysyłanych danych telemetrycznych.
   - **Wyklucz IOA**. Zdarzenie wyzwalające regułę IOA zostanie wykluczone z wysyłanych danych telemetrycznych.

10. Jeśli wybrano opcję **Wyklucz IOA**, określ reguły IOA, które mają zostać dodane do wykluczeń:

    - **Wyklucz wszystko**. Jeśli spełniony zostanie określony warunek, aplikacja wykluczy z danych telemetrycznych zdarzenia wygenerowane na podstawie wszystkich reguł IOA.
    - **Wyklucz wg GUID**. Podaj identyfikator GUID reguły IOA. Można określić wiele identyfikatorów GUID za pomocą `,`. Aby uzyskać więcej szczegółów na temat reguł IOA, zapoznaj się z pomocą do rozwiązania EDR Expert (cloud).

11. Określ warunek filtrowania:

    a. Wybierz nazwę pola, które będzie używane do filtrowania.

    b. Wybierz operator (zobacz tabelę poniżej) i określ wartość, z którą będzie porównywana wartość pola ze zdarzenia.

Lista operatorów warunkowych

Operator	Opis
<	Jeśli wartość pola jest mniejsza od wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
≤	Jeśli wartość pola jest mniejsza lub równa wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
=	Jeżeli wartość pola jest równa wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
≥	Jeżeli wartość pola jest większa lub równa wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
>	Jeśli wartość pola jest większa od wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
≠	Jeżeli wartość pola nie jest równa wartości określonej w warunku, zdarzenie zostanie odfiltrowane.
jest jak	Jeśli wartość pola jest zgodne z maską określoną w warunku, zdarzenie zostanie odfiltrowane. Ta aplikacja obsługuje znaki `*` i `?` podczas wprowadzania maski:
nie jest jak	Jeśli wartość pola jest niezgodna z maską określoną w warunku, zdarzenie zostanie odfiltrowane. Ta aplikacja obsługuje znaki `*` i `?` podczas wprowadzania maski:
jedno z	Jeżeli wartość pola jest zgodna z jedną z wartości na liście określonej w warunku, zdarzenie jest uznawane za odfiltrowane.
żadne z	Jeżeli wartość pola jest niezgodna z żadną z wartości na liście określonej w warunku, zdarzenie jest uznawane za odfiltrowane.
jest jak jeden z	Jeśli wartość pola jest zgodna z jedną z masek określonych w warunku, zdarzenie zostanie odfiltrowane. Aplikacja ta obsługuje znaki * i ? podczas wprowadzania maski.
nie jest jak jeden z	Jeśli wartość pola jest niezgodna z żadną z masek określonych w warunku, zdarzenie zostanie odfiltrowane. Aplikacja ta obsługuje znaki * i ? podczas wprowadzania maski.
istnieje	Jeśli pole określone w warunku występuje w zdarzeniu, to zdarzenie zostanie odfiltrowane.
nie istnieje	Jeżeli pole określone w warunku nie występuje w zdarzeniu, to zdarzenie zostanie odfiltrowane.
zawiera	Jeżeli wartość określona w warunku znajduje się w wartości pola, to zdarzenie zostanie odfiltrowane.
jest równy	Jeżeli wartość pola jest równa wartości określonej w warunku, zdarzenie zostanie odfiltrowane. Podczas skanowania nie jest uwzględniana wielkość liter.
bitowy AND	Jeżeli wynik operacji bitowej AND (&) pomiędzy wartością pola i wartością określoną w warunku wynosi 1, to zdarzenie zostanie odfiltrowane.

12. W razie potrzeby możesz utworzyć złożone kryteria filtrowania, dodając wiele warunków filtrowania i grup warunków. Do grupy warunków można również dodać zagnieżdżone warunki i grupy warunków. Możesz użyć następujących operatorów:

    - **AND** oznacza, że filtr wybiera zdarzenia spełniające wszystkie określone warunki.
    - **OR** oznacza, że filtr wybiera zdarzenia spełniające jeden z określonych warunków.
    - **NOT** (aby użyć tego operatora, wybierz opcję **Dodaj NOT przed**) oznacza, że filtr wybiera zdarzenia, które nie spełniają żadnego ze wskazanych warunków.

    Warunki i grupy warunków pierwszego poziomu są łączone za pomocą operatora **AND**.

13. Aby przeskanować utworzoną regułę filtrowania, kliknij przycisk **Sprawdź regułę**.

    W oknie, które zostanie otwarte, wyświetli się tabela zdarzeń przefiltrowanych przez utworzoną regułę. Więcej szczegółów znajdziesz w pomocy do rozwiązania EDR Expert (cloud).

14. W razie potrzeby w obszarze **Wszystkie typy zdarzeń** dodaj wykluczenia telemetrii według typu zdarzenia.

    a. Kliknij nazwę typu zdarzenia.

    b. W otwartym oknie kliknij przycisk **Skonfiguruj ręcznie**.

    c. W razie potrzeby skonfiguruj transmisję telemetryczną dla wybranego typu zdarzenia za pomocą przełącznika **Wyślij zdarzenie**. Domyślnie transmisja telemetryczna jest włączona dla wszystkich typów zdarzeń.

    d. W sekcji **Reguły wykluczania** kliknij przycisk **Dodaj**.

    Zostanie otwarte okno **Dodaj regułę wykluczania**.

    e. Dla każdej dodawanej reguły wykonaj czynności opisane w krokach 7–13.

15. W przypadku niektórych typów zdarzeń możesz również dodać reguły uwzględniania, aby rozszerzyć zakres zbieranych danych telemetrycznych:

    a. W sekcji **Reguły włączania** kliknij przycisk **Dodaj**.

    Zostanie otwarte okno **Dodaj regułę włączania**.

    b. Wprowadź nazwę reguły.

    c. W obszarze **Warunek** wprowadź wartości dla wyświetlanych pól. Typ dostępnych pól zależy od wybranego zdarzenia.

    Reguły wykluczania mają pierwszeństwo przed regułami włączania.

16. Aby zastosować zasadę do komputerów, upewnij się, że kłódki są zamknięte (🔒), i zapisz zmiany.

Eksportowanie i importowanie filtrów zdarzeń EDR Expert (cloud)

Możesz wyeksportować listę wykluczeń do pliku JSON. Następnie możesz zmodyfikować plik, na przykład, aby dodać dużą liczbę identyfikatorów zdarzeń. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej filtrów zdarzeń lub przeniesienia listy na inny serwer.

Użycie zbyt wielu reguł może zwiększyć obciążenie serwera gromadzenia danych telemetrii i obniżyć wydajność komputera. Zalecamy dodawanie tylko niezbędnych reguł.

Eksport i import filtrów zdarzeń w Web Console:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Ustawienia telemetrii**.
5. Wybierz zakładkę **Dane telemetryczne EDR Expert (cloud)**.
6. Aby wyeksportować filtry zdarzeń:
   a. Kliknij **Eksportuj**.
   b. W otwartym oknie określ nazwę pliku JSON, do którego chcesz wyeksportować filtry zdarzeń, i wybierz folder, w którym chcesz zapisać ten plik.
   c. Zapisz plik.

      Kaspersky Endpoint Security eksportuje filtry zdarzeń do pliku JSON.
7. Aby zaimportować filtry zdarzeń:
   a. Kliknij **Importuj**.
   b. W oknie, które się otworzy, wybierz plik JSON, z którego chcesz zaimportować filtry zdarzeń.
   c. Wybierz, w jaki sposób chcesz importować reguły filtrowania zdarzeń: dodając je do istniejących reguł lub odrzucając istniejące reguły i zastępując je nowymi.
   d. Otwórz plik.
8. Aby zastosować zasadę do komputerów, upewnij się, że kłódki są zamknięte (🔒), i zapisz zmiany.
   1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
   2. Kliknij nazwę zasady Kaspersky Endpoint Security.

      Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne** → **Ustawienia telemetrii**.

5. Wybierz zakładkę **Dane telemetryczne EDR Expert (cloud)**.

6. Aby wyeksportować filtry zdarzeń:

   a. Kliknij **Eksportuj**.

   b. W otwartym oknie określ nazwę pliku JSON, do którego chcesz wyeksportować filtry zdarzeń, i wybierz folder, w którym chcesz zapisać ten plik.

   c. Zapisz plik.

   Kaspersky Endpoint Security eksportuje filtry zdarzeń do pliku JSON.

7. Aby zaimportować filtry zdarzeń:

   a. Kliknij **Importuj**.

   b. W oknie, które się otworzy, wybierz plik JSON, z którego chcesz zaimportować filtry zdarzeń.

   c. Wybierz, w jaki sposób chcesz importować reguły filtrowania zdarzeń: dodając je do istniejących reguł lub odrzucając istniejące reguły i zastępując je nowymi.

   d. Otwórz plik.

8. Aby zastosować zasadę do komputerów, upewnij się, że kłódki są zamknięte (), i zapisz zmiany.

Zarządzanie Kwarantanną

Kwarantanna to specjalny lokalny magazyn na komputerze. Użytkownik może poddać kwarantannie pliki, które użytkownik uznaje za niebezpieczne dla komputera. Pliki poddane kwarantannie są przechowywane w postaci zaszyfrowanej i nie zagrażają bezpieczeństwu urządzenia. Kaspersky Endpoint Security używa Kwarantanny tylko w przypadku integracji z rozwiązaniami Kaspersky Detection and Response. W innych przypadkach Kaspersky Endpoint Security umieszcza odpowiedni plik w Kopii zapasowej. Więcej informacji na temat zarządzania Kwarantanną jako częścią rozwiązań można znaleźć w pomocy dla Kaspersky Sandbox, pomocy dla Kaspersky Endpoint Detection and Response Optimum, pomocy dla Kaspersky Endpoint Detection and Response Expert, pomocy dla Kaspersky Anti Targeted Attack Platform i pomocy dla Kaspersky Endpoint Detection and Response Expert (on-premises).

Kaspersky Endpoint Security używa konta systemowego (SYSTEM) do poddania plików kwarantannie.

Ustawienia kwarantanny można skonfigurować tylko w konsoli Kaspersky Security Center Console. Można także użyć konsoli Kaspersky Security Center Console do zarządzania obiektami poddanymi kwarantannie (przywróć, usuń, dodaj itd.). Lokalnie, na komputerze, możesz tylko przywrócić obiekt przy użyciu wiersza polecenia.

Konfigurowanie maksymalnego rozmiaru Kwarantanny

Domyślnie, rozmiar Kwarantanny jest ograniczony do 1024 MB. Gdy Kwarantanna osiągnie maksymalny rozmiar, Kaspersky Endpoint Security przestaje wysyłać pliki i generuje zdarzenie *Brak wystarczającej ilości miejsca w magazynie Kwarantanny*. Aby zapobiec wyczerpaniu się miejsca na dysku w Kwarantannie, możesz ustawić próg, przy którym Kaspersky Endpoint Security wygeneruje zdarzenie *Magazyn Kwarantanny jest prawie przepełniony*. Nie można skonfigurować okresu przechowywania plików poddanych Kwarantannie, aby były one automatycznie usuwane.

Jeżeli w Twojej organizacji wdrożone jest rozwiązanie Kaspersky Anti Targeted Attack Platform (EDR), zalecamy zwiększenie rozmiaru Kwarantanny. Podczas wykonywania skanowania YARA, w aplikacji może pojawić się duży zrzut pamięci. Jeśli rozmiar zrzutu pamięci przekracza rozmiar Kwarantanny, skanowanie YARA zakończy się błędem, a zrzut pamięci nie zostanie poddany kwarantannie. Zalecamy ustawienie rozmiaru Kwarantanny równego całkowitej wielkości pamięci RAM w komputerze (na przykład 8 GB) lub wyłączenie ograniczenia rozmiaru Kwarantanny.

Jak skonfigurować maksymalny rozmiar kwarantanny w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne → Raporty i Kopia zapasowa**.
4. W sekcji **Kwarantanna** skonfiguruj rozmiar Kwarantanny:
   - **Ogranicz rozmiar Kwarantanny do N MB**. Jeśli pole jest zaznaczone, maksymalny rozmiar Kwarantanny jest ograniczony do zdefiniowanej wartości. Domyślnie wynosi on 1024 MB. Jeśli Kwarantanna osiągnie maksymalny rozmiar, Kaspersky Endpoint Security wyśle zdarzenie *Brak wystarczającej ilości miejsca w magazynie Kwarantanny* do Kaspersky Security Center i opublikuje zdarzenie w dzienniku zdarzeń Windows. W międzyczasie aplikacja przestaje poddawać nowe obiekty kwarantannie. Musisz ręcznie opróżnić Kwarantannę.

     Jeśli pole wyboru jest odznaczone, rozmiar Kwarantanny jest ograniczony przez ilość wolnego miejsca na dysku.

   - **Powiadom, gdy pamięć kwarantanny osiągnie N procent**. Wartość progowa Kwarantanny. Na przykład, możesz ustawić wartość progową Kwarantanny na 50%. Jeśli Kwarantanna osiągnie wartość progową, Kaspersky Endpoint Security wyśle odpowiednie zdarzenie do Kaspersky Security Center i opublikuje zdarzenie w Dzienniku zdarzeń Windows. W międzyczasie aplikacja kontynuuje poddawanie nowych obiektów kwarantannie.

     Jeśli to pole wyboru jest odznaczone, aplikacja nie będzie generować zdarzeń po osiągnięciu progu kwarantanny.

5. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console skonfigurować maksymalny rozmiar Kwarantanny

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami → Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne → Raporty i Kopia zapasowa**.

5. W sekcji **Kwarantanna** skonfiguruj rozmiar Kwarantanny:

   - **Ogranicz rozmiar kwarantanny**. Jeśli to pole wyboru jest zaznaczone, maksymalny rozmiar Kwarantanny jest ograniczony do określonej wartości. Jeśli pole wyboru jest odznaczone, rozmiar Kwarantanny jest ograniczony przez ilość wolnego miejsca na dysku. Może to być konieczne w przypadku skanowania YARA, ponieważ aplikacja może zapisać duży plik zrzutu pamięci.

   - **Maksymalny rozmiar kwarantanny (MB)**. Jeśli pole jest zaznaczone, maksymalny rozmiar Kwarantanny jest ograniczony do zdefiniowanej wartości. Domyślnie wynosi on 1024 MB. Jeśli Kwarantanna osiągnie maksymalny rozmiar, Kaspersky Endpoint Security wyśle zdarzenie *Brak wystarczającej ilości miejsca w magazynie Kwarantanny* do Kaspersky Security Center i opublikuje zdarzenie w dzienniku zdarzeń Windows. W międzyczasie aplikacja przestaje poddawać nowe obiekty kwarantannie. Musisz ręcznie opróżnić Kwarantannę.

     Jeśli pole wyboru jest odznaczone, rozmiar Kwarantanny jest ograniczony przez ilość wolnego miejsca na dysku.

   - **Powiadom, gdy pamięć kwarantanny osiągnie (%)**. Wartość progowa Kwarantanny. Na przykład, możesz ustawić wartość progową Kwarantanny na 50%. Jeśli Kwarantanna osiągnie wartość progową, Kaspersky Endpoint Security wyśle odpowiednie zdarzenie do Kaspersky Security Center i opublikuje zdarzenie w Dzienniku zdarzeń Windows. W międzyczasie aplikacja kontynuuje poddawanie nowych obiektów kwarantannie.

6. Zapisz swoje zmiany.

Wysyłanie danych o plikach poddanych kwarantannie do Kaspersky Security Center

Aby wykonać działania na obiektach poddanych kwarantannie w Web Console, musisz włączyć wysyłanie danych plików poddanych kwarantannie do Serwera administracyjnego. Na przykład, możesz pobrać plik z kwarantanny do analizy w Web Console. Wysyłanie danych plików poddanych kwarantannie musi zostać włączone, aby działały wszystkie funkcje Kaspersky Sandbox i Kaspersky Endpoint Detection and Response.

Jak włączyć przesyłanie danych plików poddanych kwarantannie w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasady wybierz **Ustawienia ogólne → Raporty i Kopia zapasowa**.

4. W sekcji **Przesyłanie danych do Serwera administracyjnego** kliknij przycisk **Ustawienia**.

5. W otwartym oknie zaznacz pole **Pliki kwarantanny**.

6. Zapisz swoje zmiany.

Jak włączyć przesyłanie danych plików poddanych kwarantannie w Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Integracja KSC**.
5. W sekcji **Przesyłanie danych do Serwera administracyjnego** zaznacz pole **Informacje o plikach Kwarantanny**.
6. Zapisz swoje zmiany.

W rezultacie, w konsoli Kaspersky Security Center możesz wyświetlić listę plików poddanych kwarantannie na Twoim komputerze. Można użyć konsoli Kaspersky Security Center Console do zarządzania obiektami poddanymi kwarantannie (przywróć, usuń, dodaj itd.). Więcej informacji o pracy z funkcją Kwarantanna znajdziesz w pomocy do Kaspersky Security Center.

Przywracanie plików z Kwarantanny

Domyślnie Kaspersky Endpoint Security przywraca pliki do ich oryginalnego folderu. Jeżeli folder docelowy został usunięty lub użytkownik nie ma uprawnień dostępu do tego folderu, aplikacja umieszcza plik w folderze `%DataRoot%\QB\Restored`. Następnie ręcznie przenieś plik do folderu docelowego.

W celu przywrócenia plików z Kwarantanny:

1. W oknie głównym Web Console wybierz **Operacje** → **Repozytoria** → **Kwarantanna**.
2. To spowoduje otwarcie listy plików w kwarantannie; na tej liście wybierz pliki, które chcesz przywrócić, i kliknij **Przywróć**.

   Kaspersky Endpoint Security przywraca ten plik. Jeśli w folderze docelowym znajduje się już plik o tej samej nazwie, aplikacja anuluje przywracanie pliku. W przypadku rozwiązań EDR Optimum i EDR Expert aplikacja usuwa plik po przywróceniu. W przypadku innych rozwiązań aplikacje przechowują kopię pliku w Kwarantannie.

Monitorowanie działań EDR

W Kaspersky Endpoint Security for Windows 12.9 wprowadzono centrum monitorowania działań EDR. *Centrum monitorowania działań EDR* to konsola, w której można przeglądać historię reakcji na zagrożenia dla wszystkich rozwiązań Kaspersky Detection and Response. Jeśli w organizacji wdrożono wiele rozwiązań wykrywania i reagowania (na przykład EDR Optimum i MDR), Kaspersky Endpoint Security wyświetla historię reagowania na zagrożenia dla wszystkich rozwiązań. Dzięki temu można analizować wydajność rozwiązań wykrywania i reagowania na oddzielnym komputerze i optymalizować ich ustawienia.

Centrum monitorowania udostępnia następujące informacje:

- Informacje o zadaniach reagowania na zagrożenia (np. zadanie *Zakończ proces*)
- Zmiany w zasadach izolacji sieci i zapobiegania wykonywaniu

Jeśli funkcja reagowania na zagrożenia napotka błąd związany z dostępem do udziału sieciowego, taki błąd zostanie pominięty w wyświetlanej historii funkcji reagowania na zagrożenia.

Aby przejść do centrum monitorowania działań EDR:

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasoby (urządzenia)**.
2. Wybierz komputer, dla którego chcesz skonfigurować lokalne ustawienia aplikacji.

   Spowoduje to otwarcie właściwości komputera.
3. Wybierz zakładkę **Aplikacje**.
4. Kliknij **Kaspersky Endpoint Security for Windows**.

   Spowoduje to otwarcie lokalnych ustawień aplikacji.
5. Wybierz zakładkę **Ustawienia aplikacji**.
6. Wybierz **Detection and Response** → **Historia odpowiedzi**.

Spowoduje to otwarcie centralnej konsoli monitorowania działań EDR. Za pomocą konsoli można przeglądać statusy zadań reagowania na zagrożenia, czas trwania zadań, zmiany reguł i szczegółowe informacje inicjatora.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security for Windows obsługuje rozwiązanie Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* to rozwiązanie do zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa (SIEM) dla infrastruktury IT organizacji. Platforma KUMA umożliwia wykrywanie, analizowanie i łagodzenie zagrożeń bezpieczeństwa, zanim wyrządzą szkodę.

Aplikacja Kaspersky Endpoint Security jest instalowana na pojedynczych komputerach w korporacyjnej infrastrukturze IT i cały czas monitoruje procesy, otwiera połączenia sieciowe i modyfikowane pliki. Informacje o zdarzeniach na komputerze (telemetria) są wysyłane na serwer Kaspersky Unified Monitoring and Analysis Platform (KUMA). W swojej konsoli KUMA wyświetla zdarzenia w postaci listy bez znaczników, podobnie jak dziennik zdarzeń Windows.

Kaspersky Endpoint Security nie zapewnia wszystkich funkcji agenta dla KUMA. Aplikacja wysyła do KUMA wyłącznie zdarzenia, bez znaczników. Aby uzyskać dostęp do wszystkich funkcjonalności KUMA, należy zakupić licencję i wdrożyć rozwiązanie zgodnie z przewodnikiem administratora KUMA.

Integracja Kaspersky Endpoint Security z KUMA

W celu użycia platformy KUMA spełnione muszą być następujące warunki:

- Kaspersky Security Center w wersji 14.2 lub nowszej. We wcześniejszych wersjach Kaspersky Security Center nie ma możliwości aktywowania funkcjonalności integracji platformy KUMA.
- Aplikacja jest aktywowana, a funkcjonalność jest objęta licencją.
- Komponent integracyjny KUMA jest włączony.

Konfiguracja integracji KUMA obejmuje następujące kroki:

1. **Instalowanie komponentu integracyjnego KUMA**

   Możesz wybrać komponent integracyjny KUMA podczas instalacji lub aktualizacji, a także przy użyciu zadania *Zmiana składników aplikacji*.

   Musisz ponownie uruchomić komputer, aby dokończyć aktualizację aplikacji o nowe komponenty.

2. **Aktywacja KUMA**

   Oprócz licencji na aplikację Kaspersky Endpoint Security (na przykład Kaspersky Endpoint Security for Business Standard) potrzebna jest osobna licencja na integrację Kaspersky Endpoint Security z KUMA (Kaspersky Endpoint Security for Windows KUMA Integration Add-on).

Jeśli instalujesz aplikację w trybie EDR Agent, potrzebujesz licencji na integrację Kaspersky Endpoint Security z KUMA oraz licencji Kaspersky Anti Targeted Attack Platform (KATA) lub Kaspersky Managed Detection and Response (MDR). Nie można wdrożyć EDR Agent tylko w przypadku KUMA.

Funkcjonalność staje się dostępna po dodaniu osobnego klucza KUMA. W efekcie na komputerze pojawi się kolejny aktywny klucz umożliwiający integrację Kaspersky Endpoint Security z KUMA.

Zasady udzielania licencji dla funkcjonalności KUMA są takie same jak w przypadku udzielania licencji dla Kaspersky Endpoint Security.

Upewnij się, że funkcja KUMA jest w licencji i jest uruchomiona w lokalnym interfejsie aplikacji.

3 **Łączenie z KUMA**

W celu połączenia komputera z aplikacją Kaspersky Endpoint Security z rozwiązaniem KUMA:

1. W zasadzie Kaspersky Endpoint Security dodaj adresy serwerów KUMA i określ ustawienia sieciowe połączenia.

2. W konsoli KUMA dodaj poborcę ze złączami typu tcp lub udp oraz określ podstawowe ustawienia sieciowe połączenia. Szczegółowe informacje na temat zarządzania poborcami można znaleźć w pomocy platformy Kaspersky Unified Monitoring and Analysis Platform.

Możesz nawiązać zaufane połączenie pomiędzy Kaspersky Endpoint Security a serwerami KUMA. Aby skonfigurować zaufane połączenie, musisz użyć certyfikatu TLS. Certyfikat TLS możesz uzyskać na serwerze KUMA Core (patrz ustawienia złącza typu tcp w pomocy platformy Kaspersky Unified Monitoring and Analysis Platform). Następnie musisz dodać certyfikat TLS do Kaspersky Endpoint Security (zobacz instrukcje poniżej).

Aby połączenie było bezpieczniejsze, możesz dodatkowo włączyć weryfikację komputera na platformie KUMA (uwierzytelnianie dwukierunkowe). Aby włączyć tę weryfikację, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach platformy KUMA i Kaspersky Endpoint Security. Aby korzystać z uwierzytelniania dwukierunkowego, potrzebujesz również kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Należy wygenerować certyfikat z kluczem prywatnym w formacie kontenera PKCS#12 w zewnętrznym urzędzie certyfikacji. Następnie musisz dodać archiwum PFX w konsoli KUMA i w Kaspersky Endpoint Security (zobacz ustawienia złącza typu tcp w pomocy platformy Kaspersky Unified Monitoring and Analysis Platform).

Jak połączyć komputer Kaspersky Endpoint Security z platformą KUMA przy użyciu Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.

2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

3. W oknie zasad, wybierz **$IsKUMATelemetry ? "Integracja KUMA": "Integracja SIEM**.

4. Zaznacz pole **$IsKUMATelemetry ? "Integracja KUMA": "Integracja SIEM**.

5. W sekcji **Ustawienia integracji** zaznacz pole **$IsKUMATelemetry ? "Włącz transmisję zdarzeń Windows do serwera KUMA": "Włącz transmisję zdarzeń Windows do serwera SIEM**.

6. W razie potrzeby zaznacz pole wyboru **Użyj szyfrowania TLS** w bloku **Ustawienia na potrzeby łączenia z serwerami KUMA**.

7. Skonfiguruj zaufane połączenie:

   a. Kliknij **Ustawienia na potrzeby łączenia z serwerami KUMA**.

   b. Skonfiguruj połączenie z serwerem:

   - **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera KUMA. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem KUMA.
   - **Certyfikat TLS serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem KUMA. Certyfikat TLS można uzyskać w konsoli Kaspersky Unified Monitoring and Analysis Platform (zobacz instrukcje w Kaspersky Unified Monitoring and Analysis Platform).

     Aby nawiązać zaufane połączenie, w konsoli KUMA w ustawieniach złącza tcp należy wybrać opcję tryb TLS **With verification** (patrz ustawienia złącza typu tcp w pomocy platformy Kaspersky Unified Monitoring and Analysis Platform).
   - **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a platformą KUMA. Aby skorzystać z uwierzytelniania dwukierunkowego, w konsoli KUMA w ustawieniach złącza tcp należy wybrać opcję trybu TLS **Custom PFX** (patrz ustawienia złącza typu tcp w pomocy platformy Kaspersky Unified Monitoring and Analysis Platform). Następnie musisz uzyskać kontener szyfrowania i ustawić hasło, aby chronić kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Po skonfigurowaniu ustawień platformy KUMA należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny.

     > Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.

   c. Kliknij **OK**.

8. Dodaj serwery KUMA:

   a. Kliknij **Dodaj**.

   To powoduje otwarcie formularza, w którym można dodać serwer KUMA.

   b. Wybierz protokół połączenia z serwerami KUMA: **HTTP / HTTPS**, **TCP**, **UDP**.

   Jeśli wybierzesz protokół **HTTP / HTTPS**, domyślnie aplikacja używa HTTPS do łączenia się z serwerami KUMA. Aby używać protokołu HTTP, należy ręcznie określić ten protokół w adresie serwera (na przykład `http://server.com`).

   c. Wprowadź adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.

   d. Kliknij **OK**.

   Kaspersky Endpoint Security łączy się z pierwszym serwerem KUMA na liście. Jeśli połączenie nie powiedzie się, Kaspersky Endpoint Security połączy się z drugim serwerem KUMA na liście itd.

9. W razie potrzeby skonfiguruj ustawienie **Maksymalne opóźnienie transmisji zdarzeń (s)** w bloku **Ustawienia przesyłania danych**. Kiedy upłynie określony czas, Kaspersky Endpoint Security spróbuje połączyć się z tym samym serwerem lub połączy się z kolejnym serwerem na liście, jeśli istnieje wiele serwerów. Domyślnie ustawienie to 30 sekund.

10. Zapisz swoje zmiany.

Jak połączyć komputer Kaspersky Endpoint Security z platformą KUMA przy użyciu Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Konfiguracja wbudowanych agentów** → **Integracja KUMA**.
5. Włącz przełącznik **Integracja z KUMA WŁĄCZONA**.
6. W razie potrzeby włącz przełącznik **Użyj szyfrowania TLS** w sekcji **Ustawienia połączenia z serwerem**.
7. Skonfiguruj zaufane połączenie:

   a. Kliknij **Ustawienia połączenia**.

   b. Skonfiguruj połączenie z serwerem:

   - **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera KUMA. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem KUMA.
   - **Certyfikat TLS serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem KUMA. Certyfikat TLS można uzyskać w konsoli Kaspersky Unified Monitoring and Analysis Platform (zobacz instrukcje w Kaspersky Unified Monitoring and Analysis Platform).

     Aby nawiązać zaufane połączenie, w konsoli KUMA w ustawieniach złącza tcp należy wybrać opcję tryb TLS **With verification** (patrz ustawienia złącza typu tcp w pomocy platformy Kaspersky Unified Monitoring and Analysis Platform).
   - **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a platformą KUMA. Aby skorzystać z uwierzytelniania dwukierunkowego, w konsoli KUMA w ustawieniach złącza tcp należy wybrać opcję trybu TLS **Custom PFX** (patrz ustawienia złącza typu tcp w pomocy platformy Kaspersky Unified Monitoring and Analysis Platform). Następnie musisz uzyskać kontener szyfrowania i ustawić hasło, aby chronić kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Po skonfigurowaniu ustawień platformy KUMA należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny.

     > Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.

   c. Kliknij **OK**.
8. Dodaj serwery KUMA:

   a. Kliknij **Dodaj**.

   To powoduje otwarcie formularza, w którym można dodać serwer KUMA.

b. Wybierz protokół połączenia z serwerami KUMA: **HTTP/HTTPS**, **TCP**, **UDP**.

Jeśli wybierzesz protokół **HTTP/HTTPS**, domyślnie aplikacja używa HTTPS do łączenia się z serwerami KUMA. Aby używać protokołu HTTP, należy ręcznie określić ten protokół w adresie serwera (na przykład `http://server.com`).

c. Wprowadź adres serwera (IPv4, IPv6) oraz port do połączenia z serwerem.

d. Kliknij **OK**.

Kaspersky Endpoint Security łączy się z pierwszym serwerem KUMA na liście. Jeśli połączenie nie powiedzie się, Kaspersky Endpoint Security połączy się z drugim serwerem KUMA na liście itd.

9. W razie potrzeby skonfiguruj ustawienie **Maksymalne opóźnienie przy wysyłaniu zdarzeń (sek.)** w bloku **Ustawienia połączenia z serwerem**. Kiedy upłynie określony czas, Kaspersky Endpoint Security spróbuje połączyć się z tym samym serwerem lub połączy się z kolejnym serwerem na liście, jeśli istnieje wiele serwerów. Domyślnie ustawienie to 30 sekund.

10. Zapisz swoje zmiany.

Możesz sprawdzić, czy integracja z KUMA jest poprawnie skonfigurowana w konsoli KUMA (szczegóły patrz Pomoc dla platformy Kaspersky Unified Monitoring and Analysis Platform). Sprawdź stan działania komponentu, przeglądając *Raport o stanie składników aplikacji* w konsoli Kaspersky Security Center. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Integracja KUMA** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

4 **Włączanie wysyłania danych telemetrycznych na serwer KUMA**

Wysyłanie zdarzeń na serwer KUMA jest domyślnie wyłączone. Aby zapewnić poprawne działanie serwera KUMA, należy włączyć wysyłanie danych telemetrycznych. Można wybrać źródło zdarzeń spośród standardowych dzienników: *Application*, *Security* lub *System*.

Jak włączyć wysyłanie danych telemetrycznych na serwer KUMA w konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.
3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
4. W oknie zasady wybierz **Ustawienia ogólne** → **Wykluczenia i typy obiektów**.
5. W sekcji **Ustawienia telemetrii** → **Telemetria KUMA** kliknij przycisk **Ustawienia**.
6. Wybierz dzienniki zdarzeń, których chcesz użyć jako źródła zdarzeń: *Application*, *Security* lub *System*.

   Oprócz standardowych dzienników możesz określić dziennik aplikacji innej firmy.
7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak włączyć przesyłanie danych na serwer KUMA w Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne** → **Ustawienia telemetrii**.

5. Wybierz zakładkę **Telemetria KUMA**.

6. Wybierz dzienniki zdarzeń, których chcesz użyć jako źródła zdarzeń: *Application*, *Security* lub *System*.

   Oprócz standardowych dzienników możesz określić dziennik aplikacji innej firmy.

7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Filtrowanie zdarzeń, które mają zostać wysłane do KUMA

Wysyłanie zdarzeń na serwer KUMA jest domyślnie wyłączone. Aby zapewnić poprawne działanie serwera KUMA, należy włączyć wysyłanie danych telemetrycznych. Można wybrać źródło zdarzeń spośród standardowych dzienników: *Application*, *Security* lub *System*. Aby zwiększyć wydajność i zoptymalizować transmisję danych do serwera KUMA, możesz ręcznie dodawać poszczególne zdarzenia do danych telemetrycznych lub je z nich wykluczać. Można na przykład wykluczyć zdarzenia Sysmon.

Jak utworzyć listę zdarzeń do wysłania do KUMA w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W drzewie konsoli wybierz **Zasady**.

3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

4. W oknie zasady wybierz **Ustawienia ogólne** → **Wykluczenia i typy obiektów**.

5. W sekcji **Ustawienia telemetrii** → **Telemetria KUMA** kliknij przycisk **Ustawienia**.

6. W wyświetlonym oknie skonfiguruj filtry zdarzeń, które mają być wysyłane do KUMA.

   Można skonfigurować filtrowanie zdarzeń dla standardowych dzienników *Application*, *Security*, *System* lub ręcznie dodać kolejny dziennik:

   a. Otwórz właściwości dziennika lub kliknij przycisk **Dodaj** i wpisz nazwę dziennika.

   b. Wybierz tryb wysyłania zdarzeń:

   - **Wyślij wszystkie zdarzenia**. W tym trybie aplikacja wysyła wszystkie zdarzenia z dziennika systemu Windows, z wyjątkiem zdarzeń dodanych do reguł wykluczania.
   - **Wyślij tylko wybrane zdarzenia**. W tym trybie aplikacja wysyła tylko zdarzenia dodane w regułach włączania.

   c. Utwórz listy reguł wykluczania lub reguł włączania dla odpowiedniego trybu wysyłania zdarzeń.

   Aby dodać reguły, należy określić identyfikator zdarzenia w dzienniku zdarzeń systemu Windows. W jednej regule można umieścić wiele identyfikatorów zdarzeń. Aby określić wiele identyfikatorów zdarzeń, użyj przecinka (`,`).

   d. W razie potrzeby włącz rejestrowanie zdarzeń, zaznaczając pole wyboru obok nazwy dziennika.

7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak utworzyć listę zdarzeń do wysłania do KUMA w Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Ustawienia telemetrii**.
5. Wybierz zakładkę **Telemetria KUMA**.
6. W wyświetlonym oknie skonfiguruj filtry zdarzeń, które mają być wysyłane do KUMA.

   Można skonfigurować filtrowanie zdarzeń dla standardowych dzienników *Application*, *Security*, *System* lub ręcznie dodać kolejny dziennik:

   a. Otwórz właściwości dziennika lub kliknij przycisk **Dodaj** i wpisz nazwę dziennika.

   b. Wybierz tryb wysyłania zdarzeń:

   - **Wyślij wszystkie zdarzenia**. W tym trybie aplikacja wysyła wszystkie zdarzenia z dziennika systemu Windows, z wyjątkiem zdarzeń dodanych do reguł wykluczania.
   - **Wyślij tylko wybrane zdarzenia**. W tym trybie aplikacja wysyła tylko zdarzenia dodane w regułach włączania.

   c. Utwórz listy reguł wykluczania lub reguł włączania dla odpowiedniego trybu wysyłania zdarzeń.

   Aby dodać reguły, należy określić identyfikator zdarzenia w dzienniku zdarzeń systemu Windows. W jednej regule można umieścić wiele identyfikatorów zdarzeń. Aby określić wiele identyfikatorów zdarzeń, użyj przecinka (`,`).

   d. W razie potrzeby włącz rejestrowanie zdarzeń, korzystając z przełącznika znajdującego się obok nazwy dziennika.
7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Eksportowanie i importowanie filtrów zdarzeń KUMA

Możesz wyeksportować listę wykluczeń do pliku JSON. Następnie możesz zmodyfikować plik, na przykład, aby dodać dużą liczbę identyfikatorów zdarzeń. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej filtrów zdarzeń lub przeniesienia listy na inny serwer.

Użycie zbyt wielu reguł może zwiększyć obciążenie serwera KUMA i obniżyć wydajność komputera. Zalecamy dodawanie tylko niezbędnych reguł.

Jak eksportować i importować filtry zdarzeń w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz **Zasady**.

3. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

4. W oknie zasady wybierz **Ustawienia ogólne** → **Wykluczenia i typy obiektów**.

5. W sekcji **Ustawienia telemetrii** → **Telemetria KUMA** kliknij przycisk **Ustawienia**.

6. Aby wyeksportować filtry zdarzeń:

   a. Wybierz dzienniki zdarzeń z filtrami, które chcesz wyeksportować.

   b. Kliknij przycisk → **Eksportuj**.

   c. W otwartym oknie określ nazwę pliku JSON, do którego chcesz wyeksportować filtry zdarzeń, i wybierz folder, w którym chcesz zapisać ten plik.

   d. Zapisz plik.

   Kaspersky Endpoint Security eksportuje filtry zdarzeń do pliku JSON.

7. Aby zaimportować filtry zdarzeń:

   a. Kliknij przycisk → **Importuj**.

   b. W oknie, które się otworzy, wybierz plik JSON, z którego chcesz zaimportować filtry zdarzeń.

   c. Otwórz plik.

   Jeśli na komputerze istnieją już reguły filtrowania zdarzeń, Kaspersky Endpoint Security zastąpi je podczas importowania.

8. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak eksportować i importować filtry zdarzeń w Web Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Ustawienia ogólne** → **Ustawienia telemetrii**.

5. Wybierz zakładkę **Telemetria KUMA**.

6. Aby wyeksportować filtry zdarzeń:

   a. Wybierz dzienniki zdarzeń z filtrami, które chcesz wyeksportować.

   b. Kliknij przycisk → **Eksportuj**.

   c. W otwartym oknie określ nazwę pliku JSON, do którego chcesz wyeksportować filtry zdarzeń, i wybierz folder, w którym chcesz zapisać ten plik.

   d. Zapisz plik.

   Kaspersky Endpoint Security eksportuje filtry zdarzeń do pliku JSON.

7. Aby zaimportować filtry zdarzeń:

   a. Kliknij przycisk → **Importuj**.

   b. W oknie, które się otworzy, wybierz plik JSON, z którego chcesz zaimportować filtry zdarzeń.

   c. Otwórz plik.

      Jeśli na komputerze istnieją już reguły filtrowania zdarzeń, Kaspersky Endpoint Security zastąpi je podczas importowania.

8. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Możesz również eksportować lub importować filtry zdarzeń w wierszu poleceń.

Przewodnik migracji z KSWS do KES

Począwszy od wersji 11.8.0 Kaspersky Endpoint Security for Windows obsługuje podstawową funkcjonalność rozwiązania Kaspersky Security for Windows Server (KSWS). *Kaspersky Security for Windows Server* chroni serwery działające pod kontrolą systemów operacyjnych Microsoft Windows i serwery plików podłączony do sieci przed wirusami i innymi zagrożeniami bezpieczeństwa komputera, na które serwery i serwery plików podłączone do sieci są narażone podczas wymiany plików. Szczegółowe informacje dotyczące sposobu działania rozwiązania można znaleźć w Kaspersky Security for Windows Server Help. Zaczynając od Kaspersky Endpoint Security 11.8.0, możesz przeprowadzić migrację z Kaspersky Security for Windows Server do Kaspersky Endpoint Security for Windows i używać tego samego rozwiązania do ochrony stacji roboczych i serwerów.

Wymagania systemowe

Zanim rozpoczniesz migrację z KSWS do KES, upewnij się, że Twój serwer spełnia wymagania sprzętowe i programowe Kaspersky Endpoint Security for Windows. Listy obsługiwanych wersji systemów operacyjnych są różne dla KES i KSWS. Przykładowo KES nie obsługuje serwerów z systemem Windows Server 2003.

Minimalne wymagania programowe w przypadku migracji z KSWS do KES:

- Kaspersky Endpoint Security for Windows 12.0.
- Kaspersky Security 11.0.1 for Windows Server.

  Jeśli masz zainstalowaną wcześniejszą wersję Kaspersky Security for Windows Server, zalecamy uaktualnienie aplikacji do najnowszej wersji. Kreator konwersji zasad i zadań nie obsługuje wcześniejszych wersji Kaspersky Security for Windows Server.
- Kaspersky Security Center 14.2

  Jeśli masz zainstalowaną wcześniejszą wersję Kaspersky Security Center, zaktualizuj ją do wersji 14.2 lub nowszej. W tej wersji Kaspersky Security Center Kreator konwersji zasad i zadań umożliwia migrację zasad do profilu, a nie do zasady. W tej wersji Kaspersky Security Center Kreator konwersji zasad i zadań umożliwia również migrację szerszego zakresu ustawień zasad.
- Kaspersky Endpoint Agent 3.10.

  Jeśli masz zainstalowaną wcześniejszą wersję Kaspersky Endpoint Agent, zalecamy uaktualnienie aplikacji do najnowszej wersji. Kaspersky Endpoint Security obsługuje migrację konfiguracji [KSWS+KEA] do [KES+wbudowany agent] począwszy od Kaspersky Endpoint Agent 3.10.

Zalecenia dotyczące migracji

Podczas migracji z KSWS do KES należy przestrzegać następujących zaleceń:

- Zaplanuj z wyprzedzeniem czas migracji z KSWS do KES. Wybierz czas, w którym serwery pracują z najmniejszym obciążeniem, na przykład w weekend.
- Po migracji stopniowo włączaj komponenty aplikacji. Oznacza to na przykład, że należy rozpocząć od włączenia samego składnika Ochrona plików, następnie włączyć inne składniki ochrony, potem składniki kontroli i tak dalej. Na każdym etapie musisz upewnić się, że aplikacja działa poprawnie i monitorować wydajność serwera. Architektura KES różni się od KSWS, dlatego też system operacyjny może zachowywać się inaczej.
- Migrację należy przeprowadzać stopniowo. Najpierw przeprowadź migrację pojedynczego serwera, następnie wielu serwerów, a następnie przeprowadź migrację na wszystkich serwerach organizacji.
- Przeprowadzaj migracje różnych typów serwerów oddzielnie. Oznacza to na przykład, że najpierw należy przeprowadzić migrację serwerów baz danych, następnie serwerów pocztowych i tak dalej.
- Migracja na serwery o dużym obciążeniu wiąże się z pewnymi specjalnymi kwestiami.

Etapy migracji

Migracja z KSWS do KES jest wykonywana półautomatycznie. Jest to konieczne ze względu na różne architektury aplikacji. Aby przeprowadzić migrację ustawień zasad, należy uruchomić Kreatora konwersji zasad i zadań (kreatora migracji). Po przeprowadzeniu migracji ustawień zasad należy ręcznie skonfigurować ustawienia, których kreator migracji nie może przeprowadzić automatycznie (na przykład ustawienia Ochrony hasłem). Po migracji zaleca się również sprawdzenie, czy kreator migracji poprawnie przeprowadził migrację wszystkich ustawień.

Przeprowadź migrację z KSWS do KES w następującej kolejności:

1. **Migracja zadań i zasad KSWS**

   Po przeprowadzeniu migracji zasad i zadań należy wykonać dodatkowe czynności konfiguracyjne. Zalecamy również upewnienie się, że Kaspersky Endpoint Security zapewnia wymagany poziom bezpieczeństwa po migracji z KSWS.

   > Kreator konwersji zasad i zadań dla Kaspersky Security for Windows Server jest dostępny tylko w Konsoli administracyjnej (MMC). Ustawienia zasad i zadań nie mogą być migrowane w Web Console ani Kaspersky Security Center Cloud Console.

2. **Instalowanie Kaspersky Endpoint Security**

   Możesz zainstalować Kaspersky Endpoint Security na następujące sposoby:

   - Instalowanie KES po usunięciu KSWS (zalecane).

     > Narzędzie kavremover nie obsługuje zarządzania KSWS.

   - Instalowanie KES na KSWS.

3. Aktywowanie KES przy użyciu klucza dla KSWS

4. **Potwierdzenie, że aplikacja działa po migracji**

   Upewnij się, że aplikacja po migracji z KSWS do KES działa poprawnie. Sprawdź stan serwera w konsoli (powinien być *OK*). Upewnij się, że aplikacja nie zgłasza błędów. Sprawdź również czas ostatniego połączenia z Serwerem administracyjnym, czas ostatniej aktualizacji bazy danych oraz stan ochrony serwera.

   Zwróć szczególną uwagę na migrację list wykluczeń, zaufanych aplikacji, zaufanych adresów internetowych, reguł Kontroli aplikacji.

Zgodność komponentów KSWS i KES

Podczas migracji z KSWS do KES zestaw komponentów jest migrowany tylko wtedy, gdy aplikacja jest instalowana lokalnie.

Zgodność komponentów Kaspersky Security for Windows Server i Kaspersky Endpoint Security for Windows

Komponent Kaspersky Security for Windows Server	Komponent Kaspersky Endpoint Security for Windows
Basic functionality	Jądro aplikacji
Log Inspection	Kontrola dziennika
Device Control	Kontrola urządzeń
Firewall Management	*(nieobsługiwany)* Funkcje zapory KSWS są wykonywane przez zaporę na poziomie systemu. W KES za funkcjonalność zapory sieciowej odpowiada osobny komponent. Po migracji możesz skonfigurować zaporę sieciową Kaspersky Endpoint Security.
File Integrity Monitor	Monitor integralności systemu
Exploit Prevention	Ochrona przed exploitami
System Tray Icon	*(nieobsługiwany)* Możesz skonfigurować interakcję użytkownika w ustawieniach interfejsu aplikacji.
Integration with Kaspersky Security Center	Wtyczka Network Agent Connector
Endpoint Agent	*(nieobsługiwany)* W programie Kaspersky Endpoint Security 11.9.0 pakiet dystrybucyjny Kaspersky Endpoint Agent nie jest już częścią zestawu dystrybucyjnego Kaspersky Endpoint Security. Musisz pobrać pakiet dystrybucyjny Kaspersky Endpoint Agent oddzielnie.
Network Threat Protection	Ochrona sieci
Anti-Cryptor	Wykrywanie zachowań
Anti-Cryptor for NetApp	*(nieobsługiwany)*
Traffic Security	Ochrona WWW Ochrona poczty Kontrola sieci
On-Demand Scan	Jądro aplikacji
ICAP Network Storage Protection	*(nieobsługiwany)* Kaspersky Endpoint Security nie obsługuje składników ochrony pamięci masowych podłączonych do sieci. Jeśli potrzebujesz tych komponentów, możesz kontynuować korzystanie z Kaspersky Security for Windows Server.
RPC Network Storage Protection	*(nieobsługiwany)* Kaspersky Endpoint Security nie obsługuje składników ochrony pamięci masowych podłączonych do sieci. Jeśli potrzebujesz tych komponentów, możesz kontynuować korzystanie z Kaspersky Security for Windows Server.

Komponent Kaspersky Security for Windows Server	Komponent Kaspersky Endpoint Security for Windows
Real-Time File Protection	Ochrona plików
Script Monitoring	*(nieobsługiwany)* Monitorowanie skryptów jest zarządzane przez inne komponenty, na przykład, Ochrona AMSI.
KSN Usage	Kaspersky Security Network
Applications Launch Control	Kontrola aplikacji
Performance counters	*(nieobsługiwany)*

Zgodność ustawień KSWS i KES

Podczas migrowania zasad i zadań program KES jest konfigurowany zgodnie z ustawieniami KSWS. Ustawienia składników aplikacji, których KSWS nie zawiera, posiadają domyślne wartości.

Application settings

Scalability, interface and scanning settings

Ustawienia aplikacji nie są obsługiwane w Kaspersky Endpoint Security for Windows.

Ustawienia aplikacji

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Scalability settings	*(niemigrowane)* Kaspersky Endpoint Security zarządza wszystkimi procesami pracy.
Show System Tray Icon	*(niemigrowane)* Na komputerze klienckim domyślnie dostępne są: okno główne Kaspersky Endpoint Security oraz ikona w obszarze powiadomień systemu Windows. W menu kontekstowym ikony użytkownik może przeprowadzić operacje na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetli także powiadomienia nad ikoną aplikacji. Możesz skonfigurować interakcję użytkownika w ustawieniach interfejsu aplikacji.
Restore file attributes after scanning	*(niemigrowane)* Kaspersky Endpoint Security automatycznie przywraca atrybuty plików po skanowaniu pliku.
Limit CPU usage for scanning threads	*(niemigrowane)* Kaspersky Endpoint Security nie ogranicza zużycia procesora podczas skanowania. Możesz skonfigurować zadanie do uruchamiania, gdy komputer działa z minimalnym obciążeniem.
Folder for temporary files created during scanning	*(niemigrowane)* Kaspersky Endpoint Security umieszcza pliki tymczasowe w folderze `C:\Windows\Temp`.
HSM system settings	*(niemigrowane)* Kaspersky Endpoint Security nie obsługuje systemów HSM.

Security and reliability

Ustawienia bezpieczeństwa KSWS są migrowane do sekcji **Ustawienia ogólne**, podsekcji **Ustawienia aplikacji** oraz **Interfejs**.

Ustawienia zabezpieczeń aplikacji

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Protect application processes from external threats	**Włącz Autoochronę** (podsekcja **Ustawienia aplikacji**)
Apply password protection	*(niemigrowane)* Kaspersky Endpoint Security posiada wbudowaną funkcję Ochrona hasłem (patrz podsekcja **Interfejs**).
Perform task recovery	*(niemigrowane)* Kaspersky Endpoint Security tylko automatycznie przywraca zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Kaspersky Endpoint Security uruchamia inne zadania zgodnie z terminarzem.
Do not start scheduled scan tasks	**Odrocz zaplanowane zadania podczas pracy na bateriach** (podsekcja **Ustawienia aplikacji**)
Stop current scan tasks	*(niemigrowane)* Jeśli komputer jest zasilany przez UPS, Kaspersky Endpoint Security nie zatrzymuje zadań skanowania, które są już uruchomione.

Connection settings

Ustawienia interakcji Serwera administracyjnego są migrowane do sekcji **Ustawienia ogólne**, podsekcji **Ustawienia sieciowe** oraz **Ustawienia aplikacji**.

Ustawienia interakcji Serwera administracyjnego

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Proxy server settings	**Ustawienia serwera proxy** (podsekcja **Ustawienia sieciowe**)
Do not use proxy server for local addresses	**Nie wykorzystuj serwera proxy dla adresów lokalnych** (podsekcja **Ustawienia sieciowe**)
Proxy server authentication settings	**Użyj uwierzytelniania serwera proxy** (podsekcja **Ustawienia sieciowe**) Hasło uwierzytelniające serwera proxy nie jest migrowane. Po zmigrowaniu zasady hasło należy wprowadzić ręcznie.
Use Kaspersky Security Center as a proxy server when activating the application	**Użyj Kaspersky Security Center jako serwera proxy do aktywacji** (podsekcja **Ustawienia aplikacji**)

Run local system tasks

Kaspersky Endpoint Security ignoruje ustawienia dotyczące uruchamiania lokalnych zadań systemowych Kaspersky Security for Windows Server. Korzystanie z lokalnych zadań KES możesz skonfigurować pod **Zadania lokalne**, **Zarządzanie zadaniami**. Można też skonfigurować harmonogram uruchamiania zadań *Skanowanie w poszukiwaniu złośliwego oprogramowania* i *Aktualizacja baz danych i modułów aplikacji* we właściwościach tych zadań.

Supplementary

Trusted zone

Ustawienia strefy zaufanej KSWS są przenoszone do sekcji **Ustawienia ogólne**, podsekcji **Wykluczenia**.

Ustawienia strefy zaufanej

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Object to scan (Exclusions)	**Wykluczenia ze skanowania** (Wykluczenia ze skanowania) Metody używane przez KSWS i KES do wybierania obiektów różnią się. Podczas migracji KES obsługuje wykluczenia zdefiniowane jako pojedyncze pliki lub ścieżki do piku/folderu. Jeśli KSWS posiada wykluczenia skonfigurowane jako predefiniowany obszar lub adres URL skryptu, takie wykluczenia nie zostaną przeniesione. Po migracji musisz dodać takie wykluczenia ręcznie. Wykluczenia będące wstępnie zdefiniowanymi obszarami musisz skonfigurować w ustawieniach zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Z kolei wykluczenia będące adresami sieciowymi skryptu musisz dodać do listy zaufanych adresów internetowych Ochrony WWW.
Apply also to subfolders (Exclusions)	**Włącz podfoldery** (Wykluczenia ze skanowania)
Objects to detect (Exclusions)	**Typ wykrywanych obiektów** (Wykluczenia ze skanowania)
Exclusion usage scope (Exclusions)	**Składniki ochrony** (Wykluczenia ze skanowania) Jeśli przynajmniej jeden komponent jest wybrany w KSWS, KES stosuje wykluczenia do wszystkich składników aplikacji.
Comment (Exclusions)	**Komentarz** (Wykluczenia ze skanowania)
Trusted process (Trusted process)	**Zaufane aplikacje** Metody wyboru zaufanych procesów / aplikacji różnią się w KSWS i KES. Podczas migracji KES obsługuje zaufane aplikacje skonfigurowane jako ścieżka do pliku wykonywalnego lub maski. Jeśli KSWS zawiera zaufane procesy skonfigurowane jako skrót pliku, takie zaufane procesy nie są przenoszone. Po migracji musisz ręcznie dodać takie zaufane procesy.
Do not check file backup operations (Trusted process)	**Nie monitoruj aktywności aplikacji** (Zaufane aplikacje)

Removable drives scan

Ustawienia skanowania dysków wymiennych są migrowane do sekcji **Zadania lokalne**, podsekcji Skanowanie dysków wymiennych.

Ustawienia Skanowania dysków wymiennych

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Scan removable drives on connection via USB	**Akcja po podłączeniu dysku wymiennego**
Scan removable drives if its stored data volume does not exceed (MB)	**Maksymalny rozmiar dysku wymiennego**
Scan with security level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Akcja po podłączeniu dysku wymiennego**: • **Maksymalna ochrona** • **Zalecany** Poziomy ochrony KSWS odpowiadają trybom skanowania KES w następujący sposób: • Maximum protection – Maksymalna ochrona • Recommended – Zalecany • Maximum performance – Zalecany

User permissions for application management

Kaspersky Endpoint Security nie obsługuje przypisywania uprawnień dostępu użytkownika dla zarządzania aplikacjami i zarządzania usługami aplikacji. Możesz skonfigurować ustawienia dostępu dla użytkowników i grup użytkowników dla zarządzania aplikacją w Kaspersky Security Center.

User access permissions for Kaspersky Security Service management

Kaspersky Endpoint Security nie obsługuje przypisywania uprawnień dostępu użytkownika dla zarządzania aplikacjami i zarządzania usługami aplikacji. Możesz skonfigurować ustawienia dostępu dla użytkowników i grup użytkowników dla zarządzania aplikacją w Kaspersky Security Center.

Storages

Ustawienia magazynów KSWS są migrowane do sekcji **Ustawienia ogólne**, podsekcji **Raporty i Kopia zapasowa** oraz do sekcji **Podstawowa ochrona przed zagrożeniami**, podsekcji **Ochrona sieci**.

Ustawienia magazynów

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Backup folder	*(niemigrowane)* Kaspersky Endpoint Security zapisuje kopie zapasowe plików w folderze `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.
Maximum Backup size (MB)	**Ogranicz rozmiar Kopii zapasowej do N MB** (sekcja **Ustawienia ogólne** → **Raporty i Kopia zapasowa**)
Threshold value for space available (MB)	*(niemigrowane)* Kaspersky Endpoint Security zapisuje wydarzenie *Magazyn Kwarantanny jest prawie przepełniony* po osiągnięciu 50% progu.
Target folder for restoring objects	*(niemigrowane)* Kaspersky Endpoint Security przywraca pliki do ich oryginalnego folderu.
Quarantine folder	*(niemigrowane)* Kaspersky Endpoint Security zapisuje kopie zapasowe plików w folderze `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.
Maximum Quarantine size (MB)	*(niemigrowane)* Kaspersky Endpoint Security używa Kopii zapasowej do przechowywania prawdopodobnie zainfekowanych obiektów. Podczas migracji Kaspersky Endpoint Security ignoruje ustawienia Kwarantanny.
Threshold value for space available (MB)	*(niemigrowane)* Kaspersky Endpoint Security używa Kopii zapasowej do przechowywania prawdopodobnie zainfekowanych obiektów. Podczas migracji Kaspersky Endpoint Security ignoruje ustawienia Kwarantanny.
Target folder for restoring objects	*(niemigrowane)* Kaspersky Endpoint Security przywraca pliki do ich oryginalnego folderu.
Unblock automatically in N	**Blokuj atakujące urządzenia przez N min** (sekcja **Podstawowa ochrona przed zagrożeniami** → **Ochrona sieci**)

Real-time server protection

Real-Time File Protection

Ustawienia ochrony plików w czasie rzeczywistym KSWS są migrowane do sekcji **Podstawowa ochrona przed zagrożeniami**, podsekcja **Ochrona plików**.

Ustawienia Ochrony plików w czasie rzeczywistym

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Objects protection mode: • **Smart mode** • **When run** • **On access** • **On access and modification**	**Tryb skanowania**: • **Tryb Inteligentny** • **Podczas wykonywania** • **Podczas dostępu** • **Podczas dostępu i modyfikacji**
Deeper analysis of launching processes	*(niemigrowane)* Kaspersky Endpoint Security obsługuje tylko jeden tryb analizy, tryb Optimal.
Heuristic analyzer: • **Light** • **Medium** • **Deep**	**Analiza heurystyczna**: • **Poziom niski** • **Poziom średni** • **Poziom szczegółowy**
Apply Trusted Zone	*(niemigrowane)* Kaspersky Endpoint Security stosuje strefę zaufaną do wszystkich komponentów. Możesz skonfigurować wykluczenia w ustawieniach strefy zaufanej.
Use KSN for protection	*(niemigrowane)* Kaspersky Endpoint Security używa KSN dla wszystkich składników aplikacji.
Block access to network shared resources for the hosts that show malicious activity	*(niemigrowane)* Domyślnie, Kaspersky Endpoint Security zablokuje dostęp do sieciowych zasobów współdzielonych dla hostów, które wykazują szkodliwą aktywność.
Launch critical areas scan when active infection is detected	*(niemigrowane)* Kaspersky Endpoint Security nie uruchamia zadania skanowania obszarów krytycznych po wykryciu aktywnej infekcji.
Use Kaspersky Sandbox for protection	*(niemigrowane)* Domyślnie, Kaspersky Endpoint Security wyśle obiekty do przeskanowania do Kaspersky Sandbox.
Protection scope	**Obszar ochrony**
Schedule settings	*(niemigrowane)* Kaspersky Endpoint Security używa swojego terminarza do wstrzymania Ochrony plików.

KSN Usage

Ustawienia KSWS dla Kaspersky Security Network są migrowane do sekcji **Zaawansowana ochrona przed zagrożeniami**, podsekcja **Kaspersky Security Network**.

Ustawienia Kaspersky Security Network

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky Security Network	**Oświadczenie Kaspersky Security Network** Kaspersky Endpoint Security wymaga zgody na Oświadczenie Kaspersky Security Network podczas instalowania aplikacji, tworzenia nowej zasady lub włączenia korzystania z Kaspersky Security Network.
Send data about scanned files	*(niemigrowane)* Kaspersky Endpoint Security automatycznie wyśle dane o przeskanowanych plikach, jeśli usługa KSN jest włączona.
Send data about requested URLs	*(niemigrowane)* Kaspersky Endpoint Security automatycznie wyśle dane o żądanych adresach internetowych, jeśli usługa KSN jest włączona.
Send Kaspersky Security Network statistics	**Włącz rozszerzony tryb KSN**
Accept the terms of the Kaspersky Managed Protection Statement	*(niemigrowane)* Kaspersky Endpoint Security nie zawiera usługi KMP.
Action to perform on KSN untrusted objects	*(niemigrowane)* Możesz skonfigurować Działanie podejmowane w przypadku wykrycia zagrożenia w ustawieniach składnika Ochrona i ustawieniach zadania Skanowanie.

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Do not calculate checksum before sending to KSN if file size exceeds N MB	*(niemigrowane)* Możesz skonfigurować ograniczenia skanowania dużych plików w ustawieniach składnika Ochrona i ustawieniach zadania Skanowanie.
Use Kaspersky Security Center as KSN Proxy	**Użyj serwera administracyjnego jako serwera proxy KSN**
Schedule settings	*(niemigrowane)* Nie jest możliwe skonfigurowanie oddzielnego terminarza dla komponentu. Komponent jest zawsze włączony, gdy działą program Kaspersky Endpoint Security.

Traffic Security

Ustawienia Traffic Security KSWS są migrowane do sekcji **Podstawowa ochrona przed zagrożeniami**, podsekcja Ochrona WWW oraz Ochrona poczty, sekcji **Kontrola zabezpieczeń**, podsekcja Kontrola sieci, sekcji **Ustawienia ogólne**, podsekcja Ustawienia sieciowe.

Ustawienia Traffic Security

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Apply URL-based rules	**Kontrola sieci** (podsekcja **Kontrola sieci**) Reguły oparte na adresie internetowym są przenoszone do oddzielnych reguł w Kaspersky Endpoint Security.
Apply certificate-based rules	*(niemigrowane)* Kaspersky Endpoint Security nie obsługuje reguł opartych na certyfikacie.
Apply rules for web traffic category control	**Kontrola sieci** (podsekcja **Kontrola sieci**) Blokowanie reguł kontroli kategorii ruchu sieciowego są przenoszone do pojedynczej reguły blokowania w Kaspersky Endpoint Security. Kaspersky Endpoint Security ignoruje reguły zezwalające dla kontroli kategorii. Zgodność kategorii KSWS i KES została przedstawiona poniżej.
Allow access if the web page can not be categorized	*(niemigrowane)* Kaspersky Endpoint Security zezwala na dostęp, jeśli strona internetowa nie może zostać sklasyfikowana.
Allow access to legitimate web resources that can be used to damage a protected device	*(niemigrowane)* Kaspersky Endpoint Security zezwala na dostęp do legalnych zasobów sieciowych, które mogą być używane do uszkodzenia chronionego urządzenia.
Allow access to legitimate advertisement	*(niemigrowane)* Możesz zarządzać dostępem do legalnych reklam przy użyciu kategorii zasobu sieciowego *Banery* w ustawieniach Kontroli sieci.
Operation mode: • **Driver Interceptor** • **Redirector** • **External Proxy**	*(niemigrowane)* Kaspersky Endpoint Security obsługuje tylko tryb Driver Interceptor.
ICAP-service connection settings	*(niemigrowane)* Kaspersky Endpoint Security nie obsługuje ICAP Network Storage Protection.
Check safe connections through the HTTPS protocol	Tryb **Skanuj połączenia szyfrowane** / **Zawsze skanuj połączenia szyfrowane** (podsekcja **Ustawienia sieciowe**)
Use TLS protocol version	*(niemigrowane)* Kaspersky Endpoint Security skanuje zaszyfrowany ruch sieciowy przesyłany za pośrednictwem następujących protokołów: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Możesz dodatkowo zablokować połączenia SSL 2.0 w ustawieniach skanowania szyfrowanych połączeń.
Do not trust web-servers with invalid certificate	**Adres** (podsekcja **Ustawienia sieciowe**)

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Intercept ports (Interception area)	**Monitorowane porty** (podsekcja **Ustawienia sieciowe**) Podczas migracji KES odznacza pola wyboru **Monitoruj wszystkie porty dla aplikacji z listy zalecanej przez Kaspersky** oraz **Monitoruj wszystkie porty dla określonych aplikacji**.
Exclude ports (Interception area)	*(niemigrowane)*
Exclude IP addresses (Interception area)	**Skonfiguruj zaufane adresy** (podsekcja **Ustawienia sieciowe**)
Exclude processes (Interception area)	**Skonfiguruj zaufane aplikacje** (podsekcja **Ustawienia sieciowe**) Podczas migracji KES konfiguruje następujące ustawienia dla zaufanej aplikacji: • Zaznaczone zostaje pole **Nie skanuj ruchu sieciowego**. KES nie skanuje ruchu sieciowego pod kątem jakichkolwiek zdalnych adresów IP i jakichkolwiek portów. • Pozostałe pola wyboru w ustawieniach zaufanej aplikacji zostają odznaczone.
Security port	*(niemigrowane)*
Use malicious URL database to scan web links	**Sprawdź adres internetowy w bazie danych szkodliwych adresów internetowych** (podsekcja **Ochrona WWW**)
Use anti-phishing database to scan web pages	**Sprawdź adres internetowy w bazie danych phishingowych adresów internetowych** (podsekcja **Ochrona WWW**)
Use KSN for protection	*(niemigrowane)* Kaspersky Endpoint Security używa KSN dla wszystkich składników aplikacji.
Use Trusted Zone	*(niemigrowane)* Kaspersky Endpoint Security stosuje strefę zaufaną do wszystkich komponentów. Możesz skonfigurować wykluczenia w ustawieniach strefy zaufanej.
Use heuristic analyzer	**Użyj analizy heurystycznej** (podsekcje **Ochrona WWW** i **Ochrona poczty**)
Security level	*(niemigrowane)* Kaspersky Endpoint Security posiada swoje własne poziomy ochrony komponentów Ochrona WWW i Ochrona poczty. Domyślnie, Kaspersky Endpoint Security ustawia zalecany poziom ochrony.
Enable mail threat protection	**Ochrona poczty** (podsekcja **Ochrona poczty**) **Włącz rozszerzenie Microsoft Outlook** **Tylko wiadomości przychodzące** (Obszar ochrony) **Skanuj podczas odbierania** (Ochrona poczty)
Schedule settings	*(niemigrowane)* Nie jest możliwe skonfigurowanie oddzielnego terminarza dla komponentu. Komponent jest zawsze włączony, gdy działą program Kaspersky Endpoint Security.

Exploit Prevention

Ustawienia KSWS Ochrony przed exploitami są migrowane do sekcji **Zaawansowana ochrona przed zagrożeniami**, podsekcja **Ochrona przed exploitami**.

Ustawienia Ochrony przed exploitami

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Prevent vulnerable processes exploit: • **Terminate on exploit** • **Notify only**	**Po wykryciu exploita**: • **Blokuj** • **Poinformuj**
Notify about abused processes via Terminal Service	*(niemigrowane)* Kaspersky Endpoint Security nie obsługuje usług terminalowych.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(niemigrowane)* Kaspersky Endpoint Security cały czas chroni procesy zawierające luki przed exploitami.
Protected processes	**Włącz ochronę pamięci procesów systemowych** Kaspersky Endpoint Security nie obsługuje wyboru chronionych procesów. Możesz tylko włączyć ochronę pamięci procesów systemowych.

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Exploit prevention techniques: • **Apply all available exploit prevention techniques** • **Apply selected exploit prevention techniques**	*(niemigrowane)* Kaspersky Endpoint Security stosuje wszystkie dostępne techniki ochrony przed exploitami.

Network Threat Protection

Ustawienia KSWS Ochrony sieci są migrowane do sekcji **Podstawowa ochrona przed zagrożeniami**, podsekcja Ochrona sieci.

Ustawienia Ochrony sieci

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Operation mode: • **Pass-through** • **Only inform about network attacks** • **Block connections when attack is detected**	**Ochrona sieci** Jeżeli wybrany jest tryb **Pass-through**, Ochrona sieci jest wyłączona. Jeżeli wybrany jest tryb **Only inform about network attacks** lub **Block connections when attack is detected**, Ochrona sieci jest włączona. Kaspersky Endpoint Security zawsze działa w trybie **Block connections when attack is detected**.
Do not stop traffic analysis when the task is not running	*(niemigrowane)* Kaspersky Endpoint Security analizuje ruch sieciowy cały czas, jeśli komponent jest włączony.
Do not control excluded IP addresses	**Wykluczenia**
Schedule settings	*(niemigrowane)* Nie jest możliwe skonfigurowanie oddzielnego terminarza dla komponentu. Komponent jest zawsze włączony, gdy działą program Kaspersky Endpoint Security.

Script Monitoring

Kaspersky Endpoint Security nie obsługuje komponentu Monitorowanie skryptów. Monitorowanie skryptów jest zarządzane przez inne komponenty, na przykład, Ochrona AMSI.

Website categories

Kaspersky Endpoint Security nie obsługuje wszystkich kategorii Kaspersky Security for Windows Server. Kategorie, które nie istnieją w Kaspersky Endpoint Security, nie są przenoszone. Dlatego też, reguły klasyfikacji zasobów internetowych z nieobsługiwanymi kategoriami nie są przenoszone.

Kategorie stron internetowych

Kategorie Kaspersky Security for Windows Server	Kategorie Kaspersky Endpoint Security for Windows
Wargaming	Gry wideo
Abortion	*(niemigrowane)*
Lotteries (extended)	Hazard, loterie, zakłady bukmacherskie
Alcohol	Alkohol, tytoń, narkotyki
Anonymous proxy servers	Anonimizery
Anorexia	*(niemigrowane)*
Rentals for real estate	*(niemigrowane)*
Audio, video and software	Oprogramowanie, audio, wideo
Banks	Banki
Blogs	Blogi
Military	Broń, materiały wybuchowe, tematy wojskowe
For children	*(niemigrowane)*
Discrimination	Przemoc, nietolerancja

Kategorie Kaspersky Security for Windows Server	Kategorie Kaspersky Endpoint Security for Windows
Home and family	*(niemigrowane)*
Hosting and domain services	Komunikacja przez internet
Pets and animals	*(niemigrowane)*
Law and politics	Zabronione przez prawo krajowe
Restricted by Roskomnadzor (RF)	Zabronione przez prawo Federacji Rosyjskiej
Restricted by Federal Law 436 (RF)	Zabronione przez prawo Federacji Rosyjskiej
Restricted by RF legislation	Zabronione przez prawo Federacji Rosyjskiej
Restricted by global legislation	Zabronione przez prawo krajowe
Adult dating	Treści dla dorosłych
Internet services	*(niemigrowane)*
Sex shops	Treści dla dorosłych
Information technologies	*(niemigrowane)*
Casinos, card games	Hazard, loterie, zakłady bukmacherskie
Books and writing	*(niemigrowane)*
Computer games	Gry wideo
Health and beauty	*(niemigrowane)*
Culture and society	*(niemigrowane)*
LGBT	Treści dla dorosłych
Lotteries	Hazard, loterie, zakłady bukmacherskie
Medicine	*(niemigrowane)*
Fashion	*(niemigrowane)*
Music	*(niemigrowane)*
Drugs	Alkohol, tytoń, narkotyki
Violence	Przemoc, nietolerancja
Discontent	*(niemigrowane)*
Illegal drugs	Alkohol, tytoń, narkotyki
Hate and discrimination	Przemoc, nietolerancja
Obscene vocabulary	Wulgaryzmy, nieprzyzwoitości
Lingerie	Treści dla dorosłych
News	Media informacyjne
Nudism	Treści dla dorosłych
Education	*(niemigrowane)*
Online shopping	Sklepy internetowe
All communication media	Komunikacja przez internet
Payment by credit cards	Systemy płatności
Online shopping (own payment system)	Sklepy internetowe
Online encyclopedias	*(niemigrowane)*
Online banking	Banki
Weapons	Broń, materiały wybuchowe, tematy wojskowe
Fishing and hunting	*(niemigrowane)*
Payment systems	Systemy płatności

Kategorie Kaspersky Security for Windows Server	Kategorie Kaspersky Endpoint Security for Windows
Job search	Oferty pracy
Search engines	*(niemigrowane)*
Police decision (JP)	Zakazane przez prawo Japonii
Trusted by KPSN	*(niemigrowane)*
Untrusted by KPSN	*(niemigrowane)*
Porn	Treści dla dorosłych
Media hosting and streaming	Media informacyjne
Web Mail	Poczta elektroniczna przez WWW
Traveling	*(niemigrowane)*
TV and radio	Media informacyjne
Teasers and ads services	Banery
Religion	Religie, związki wyznaniowe
Restaurants, cafe and food	*(niemigrowane)*
Dating sites	Portale randkowe
Sex education	Treści dla dorosłych
Social networks	Sieci społecznościowe
Sport	*(niemigrowane)*
Betting	Hazard, loterie, zakłady bukmacherskie
Suicide	Przemoc, nietolerancja
Tobacco	Alkohol, tytoń, narkotyki
Torrents	Torrenty
Mentioned in Federal list of extremists (RF)	Zabronione przez prawo Federacji Rosyjskiej
File sharing	Udostępnianie plików
Pharmacy	*(niemigrowane)*
Hobby and entertainment	*(niemigrowane)*
Chats and forums	Czaty, fora, komunikatory
Schools and universities pages	*(niemigrowane)*
Astrology and esoterica	*(niemigrowane)*
Extremism and racism	Przemoc, nietolerancja
E-commerce	Sklepy internetowe
Erotic	Treści dla dorosłych
Humor	*(niemigrowane)*

Local activity control

Applications Launch Control

Ustawienia Kontroli Aplikacji KSWS są migrowane do sekcji **Kontrola zabezpieczeń**, podsekcja Kontrola aplikacji.

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Operation mode: • **Statistics only** • **Active**	**Akcja** (Kontrola aplikacji): • **Przetestuj reguły**. • **Zastosuj reguły**.
Repeat action taken for the first file launch on all the subsequent launches for this file	*(niemigrowane)* Kaspersky Endpoint Security skanuje aplikację przy każdym jej uruchomieniu.
Deny the command interpreters launch with no command to execute	*(niemigrowane)* Kaspersky Endpoint Security zezwala na uruchomienie programu interpretującego polecenie, jeśli nie są zabronione przez Kontrolę aplikacji.
Rules	**Reguły kontroli aplikacji** *(obsługiwane z ograniczeniami)* Kaspersky Endpoint Security 11.11.0 wprowadza wsparcie dla migracji reguł Kontroli uruchamiania aplikacji. Funkcja migracji reguł Kontroli uruchamiania aplikacji ma pewne ograniczenia. Domyślnie Kontrola uruchamiania aplikacji KSWS zawiera dwie reguły: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** Jeżeli przynajmniej jedna źródłowa reguła KSWS ma typ **Allow**, to podczas migracji KES tworzy nową regułę zezwalającą: **Aplikacje z zaufanymi certyfikatami głównymi**. Oznacza to, że Kontrola Aplikacji KES używa pojedynczej reguły, aby umożliwić uruchamianie zaufanych skryptów, pakietów MSI i plików wykonywalnych. Jeśli obie źródłowe reguły KSWS mają typ **Deny**, KES nie dodaje reguł do zarządzania aplikacjami z zaufanymi certyfikatami głównymi.
Apply rules to executable files	*(niemigrowane)* Zakresu stosowania reguł nie można skonfigurować w ustawieniach Kontroli aplikacji KES. Kontrola aplikacji KES stosuje zasady do wszystkich typów plików: plików wykonywalnych, skryptów i pakietów MSI. Jeśli wszystkie typy plików są objęte zakresem stosowania reguł w KSWS, podczas migracji KES przenosi reguły KSWS. Jeżeli jakiś typ pliku jest wyłączony z zakresu stosowania reguł w KSWS, to podczas migracji KES przenosi również reguły KSWS, ale jako akcję Kontroli aplikacji wybiera się **Przetestuj reguły**.
Monitor loading of DLL modules	**Monitoruj ładowanie modułów DLL (znacznie zwiększa obciążenie systemu)**
Apply rules to scripts and MSI packages	*(niemigrowane)* Zakresu stosowania reguł nie można skonfigurować w ustawieniach Kontroli aplikacji KES. Kontrola aplikacji KES stosuje zasady do wszystkich typów plików: plików wykonywalnych, skryptów i pakietów MSI. Jeśli wszystkie typy plików są objęte zakresem stosowania reguł w KSWS, podczas migracji KES przenosi reguły KSWS. Jeżeli jakiś typ pliku jest wyłączony z zakresu stosowania reguł w KSWS, to podczas migracji KES przenosi reguły KSWS, ale jako akcję Kontroli aplikacji wybiera się **Przetestuj reguły**.
Deny applications untrusted by KSN	*(niemigrowane)* Kaspersky Endpoint Security nie bierze pod uwagę reputacji aplikacji i umożliwia lub zabrania uruchamiania aplikacji zgodnie z regułami.
Allow applications trusted by KSN	Podczas migracji KES dodaje nową regułę zezwalającą. Jako warunek wyzwalający regułę jest podana kategoria KL **Inne oprogramowanie\Aplikacje zaufane zgodnie z reputacją w KSN**.
Users and / or user groups allowed to run applications trusted by KSN	**Użytkownicy i ich uprawnienia** to reguła zezwalająca Kontroli aplikacji, która obejmuje kategorię KL **Inne oprogramowanie\Aplikacje zaufane zgodnie z reputacją w KSN**.
Automatically allow software distribution via applications and packages listed	Kontrola dystrybucji oprogramowania w KSWS i KES działa inaczej. Podczas migracji KES dodaje nowe reguły zezwalające dla aplikacji, które mają dozwoloną automatyczną dystrybucję oprogramowania. Jako warunek wyzwolenia reguły podana jest suma kontrolna pliku.
Always allow software distribution via Windows Installer	Kontrola dystrybucji oprogramowania w KSWS i KES działa inaczej. Podczas migracji KES dodaje nowe reguły zezwalające dla aplikacji, które mają dozwoloną automatyczną dystrybucję oprogramowania (**Software distribution applications and packages allowed**). Jako warunek wyzwolenia reguły podana jest suma kontrolna pliku. Pole wyboru **Zaufane programy aktualizujące** we właściwościach konta jest zaznaczone.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(niemigrowane)*
Software distribution applications and packages allowed	Kontrola dystrybucji oprogramowania w KSWS i KES działa inaczej. Podczas migracji KES dodaje nowe reguły zezwalające dla aplikacji, które mają dozwoloną automatyczną dystrybucję oprogramowania. Jako warunek wyzwolenia reguły podana jest suma kontrolna pliku. Pole wyboru **Zaufane programy aktualizujące** we właściwościach konta jest zaznaczone.

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Schedule settings	*(niemigrowane)* Jeśli dla komponentu w ustawieniach KSWS skonfigurowano harmonogram, komponent Kontrola aplikacji jest włączany przy migracji. Jeśli dla komponentu nie skonfigurowano harmonogramu w ustawieniach KSWS, Kontrola aplikacji jest wyłączona przy migracji. Nie jest możliwe skonfigurowanie oddzielnego terminarza dla komponentu. Komponent jest zawsze włączony, gdy działą program Kaspersky Endpoint Security.

Device Control

Ustawienia Kontroli Urządzenia KSWS są migrowane do sekcji **Kontrola zabezpieczeń**, podsekcja **Kontrola urządzeń**.

Ustawienia Kontroli urządzeń

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Operation mode: • **Active** • **Statistics only**	*(niemigrowane)* Kontrola aplikacji działa w trybie *Active*. Statystyki połączenia z urządzeniem są cały czas dostarczane przez Audyt.
Allow using all external devices when the Device Control task is not running	*(niemigrowane)* Kontrola urządzeń jest zawsze włączona, gdy działa program Kaspersky Endpoint Security.
Device Control rules	**Zaufane urządzenia** Podczas migracji Kaspersky Endpoint Security ignoruje wyłączone reguły KSWS.
Schedule settings	*(niemigrowane)* Kaspersky Endpoint Security używa swojego własnego terminarza do uzyskania dostępu do pewnych typów urządzeń.

Network-Attached Storages Protection

RPC Network Storage Protection

Kaspersky Endpoint Security nie obsługuje składników ochrony pamięci masowych podłączonych do sieci. Jeśli potrzebujesz tych komponentów, możesz kontynuować korzystanie z Kaspersky Security for Windows Server.

ICAP Network Storage Protection

Kaspersky Endpoint Security nie obsługuje składników ochrony pamięci masowych podłączonych do sieci. Jeśli potrzebujesz tych komponentów, możesz kontynuować korzystanie z Kaspersky Security for Windows Server.

Anti-Cryptor for NetApp

Kaspersky Endpoint Security nie obsługuje Anti-Cryptor for NetApp. Funkcjonalność Anti-Cryptor jest dostarczana przez inne komponenty aplikacji, takie jak Wykrywanie zachowań.

Network activity control

Firewall Management

Kaspersky Endpoint Security nie obsługuje zarządzania KSWS Firewall Management. Funkcje zapory KSWS są wykonywane przez zaporę na poziomie systemu. Po migracji możesz skonfigurować zaporę sieciową Kaspersky Endpoint Security.

Anti-Cryptor

Ustawienia sieci Anti-Cryptor są migrowane do sekcji **Zaawansowana ochrona przed zagrożeniami**, podsekcja **Wykrywanie zachowań**.

Ustawienia Anti-Cryptor

Ustawienia KSWS	Ustawienia KES
Operation mode: • **Statistics only** • **Active**	**Po wykryciu szyfrowania zewnętrznego folderów współdzielonych**: • **Poinformuj** • **Blokuj**
Heuristic analyzer	*(niemigrowane)* Kaspersky Endpoint Security nie używaj Analizy heurystycznej i Wykrywania zachowań.
Configuration of protection scope: • **All shared network folders on the protected device** • **Only specified shared folders**	*(niemigrowane)* Kaspersky Endpoint Security zapobiega szyfrowaniu wszystkich folderów sieciowych na chronionym komputerze.
Exclusions	*(niemigrowane)* Kaspersky Endpoint Security ma swoje własne wykluczenia dla komponentu Wykrywanie zachowań. Po migracji możesz ręcznie dodać wykluczenia.
Schedule settings	*(niemigrowane)* Nie jest możliwe skonfigurowanie oddzielnego terminarza dla komponentu. Komponent jest zawsze włączony, gdy działą program Kaspersky Endpoint Security.

System Inspection

File Integrity Monitor

Ustawienia Monitora integralności plików z KSWS są migrowane do sekcji **Kontrola zabezpieczeń**, podsekcji **Monitor integralności systemu**.

Ustawienia Monitora integralności plików

Ustawienia KSWS	Ustawienia KES
Log information about file operations that appear during the monitor interruption period	*(niemigrowane)* Kaspersky Endpoint Security nie rejestruje zdarzeń dla operacji na plikach wykonywanych podczas okresu przerwy w działaniu monitora.
Block attempts to compromise the USN log	*(niemigrowane)* Kaspersky Endpoint Security nie blokuje prób naruszenia dziennika USN.
Monitoring scope	**Zakres monitorowania** → **Plik** *(obsługiwane z ograniczeniami)* Wyłączone rekordy zakresu monitoringu nie są migrowane do KES. Kaspersky Endpoint Security dodaje do zakresu monitorowania tylko włączone rekordy.
Trusted users	**Zaufani użytkownicy i/lub grupy użytkowników**
File operation markers	**Markery operacji plikowej**
Calculate checksum for the file if possible	**Haszowanie**
Exclusions	**Wykluczenia** → **Plik**

Log Inspection

Ustawienia kontroli dziennika KSWS są migrowane do sekcji **Kontrola zabezpieczeń**, podsekcji **Kontrola dziennika**.

Ustawienia kontroli dziennika

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Apply custom rules for log inspection	*(niemigrowane)* Kaspersky Endpoint Security stosuje wszystkie włączone reguły niestandardowe.
Custom rules	**Reguły niestandardowe** Wstępnie zdefiniowana reguła **A service was installed in the system (for Server 2003 OS)** nie zostaje przeniesiona do KES.
Apply predefined rules for log inspection	*(niemigrowane)* Kaspersky Endpoint Security stosuje wszystkie włączone wstępnie zdefiniowane reguły.
Predefined rules	**Wstępnie zdefiniowane reguły**
Password brute-force detection	**Wykrywanie ataków siłowych**
Network logon detection	**Wykrywanie logowania do sieci**
Exclusions (IP addresses)	**Wykluczenia** (Adres IP)
Exclusions (users)	**Wykluczenia** (Użytkownicy)
Schedule settings	*(niemigrowane)* Nie jest możliwe skonfigurowanie oddzielnego terminarza dla komponentu. Komponent jest zawsze włączony, gdy działą program Kaspersky Endpoint Security.

Logs and notifications

Task logs

Ustawienia raportów KSWS są migrowane do sekcji **Ustawienia ogólne**, podsekcja **Interfejs** oraz **Raporty i Kopia zapasowa**.

Ustawienia raportów

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Event logging	**Powiadomienia** (podsekcja **Interfejs**)
Logs folder	*(niemigrowane)* Kaspersky Endpoint Security zapisuje raporty w folderze `C:\ProgramData\Kaspersky Lab\KES.14.1\Report`
Remove task logs older than N day(s)	*(niemigrowane)* Okres przechowywania raportów KES można ustawić pod **Ustawienia ogólne**, **Raporty i Kopia zapasowa**.
Remove from the audit log events N day(s)	*(niemigrowane)* Kaspersky Endpoint Security stosuje ograniczenia magazynu raportów do wszystkich raportów zawierających raportów audytu systemu.
Integration with SIEM	*(niemigrowane)* Integrację SIEM można skonfigurować w Kaspersky Security Center.

Event notifications

Ustawienia powiadomień KSWS są migrowane do sekcji **Ustawienia ogólne**, podsekcja **Interfejs**.

Ustawienia powiadomień

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Notifications	**Powiadomienia**
Notify users: • **By using terminal service** • **By using Windows Messenger Service command**	*(niemigrowane)* Kaspersky Endpoint Security nie obsługuje modyfikowania treści powiadomień. Kaspersky Endpoint Security wyświetla standardowe powiadomienia.
Notify administrators: • **By using Windows Messenger Service command** • **By running executable file** • **By sending email**	Tylko ustawienia powiadomień e-mail są migrowane do Kaspersky Endpoint Security – **Ustawienia powiadamiania przy użyciu e-mail** (blok **Powiadomienia**). Inne metody powiadamiania administratorów nie są obsługiwane.
Application database is out of date	**Wyślij powiadomienie „Bazy danych nieaktualne", jeśli bazy danych nie były aktualizowane**
Application database is extremely out of date	**Wyślij powiadomienie „Bazy danych są bardzo stare", jeśli bazy danych nie były aktualizowane**
Critical areas scan has not been performed for a long time	*(niemigrowane)* Kaspersky Endpoint Security generuje pominięte zdarzenie Skanowanie obszarów krytycznych po trzech dniach.

Interaction with Administration Server

Ustawienia interakcji Serwera administracyjnego KSWS są migrowane do sekcji **Ustawienia ogólne**, podsekcja **Raporty i Kopia zapasowa**.

Ustawienia interakcji Serwera administracyjnego

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Quarantined files	**Pliki kwarantanny**
Backed up files	**Kopie zapasowe**
Blocked hosts	*(niemigrowane)* Kaspersky Endpoint Security automatycznie wysyła dane o zablokowanych hostach.

Tasks

Activating the application

Kaspersky Endpoint Security nie obsługuje zadania *Application activation* (KSWS). Możesz utworzyć zadanie *Dodaj klucz* (KES), dodać klucz licencyjny do pakietu instalacyjnego lub włączyć automatyczną dystrybucję klucza licencyjnego.

Copying Updates

Ustawienia zadania *Copying Updates* (KSWS) są przenoszone do zadania *Aktualizacja baz danych i modułów aplikacji* (KES).

Ustawienia zadania Kopiowanie aktualizacji

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Źródło aktualizacji**: • **Kaspersky Security Center** • **Serwery aktualizacji Kaspersky** • **Określone przez użytkownika**
Use Kaspersky update servers if specified servers are not available	*(niemigrowane)* Kaspersky Endpoint Security umożliwia wybranie kilku źródeł aktualizacji, w tym serwerów aktualizacji Kaspersky. Jeśli pierwsze źródło aktualizacji nie jest dostępne, Kaspersky Endpoint Security umożliwia uzyskanie aktualizacji z innego źródła na liście.
Use proxy server settings to connect to Kaspersky update servers	*(niemigrowane)* Kaspersky Endpoint Security używa serwera proxy dla wszystkich komponentów. Możesz skonfigurować połączenie z serwerem proxy w opcjach sieciowych aplikacji.
Use proxy server settings to connect to other servers	*(niemigrowane)* Kaspersky Endpoint Security używa serwera proxy dla wszystkich komponentów. Możesz skonfigurować połączenie z serwerem proxy w opcjach sieciowych aplikacji.
Copying updates settings: • **Copy database updates** • **Copy critical software modules updates** • **Copy database updates and critical updates of application modules**	*(niemigrowane)* Kaspersky Endpoint Security kopiuje aktualizacje baz danych i krytyczne aktualizacje modułów aplikacji jako jeden pakiet.
Folder for local storage of copied updates	**Kopiuj aktualizacje do folderu**

Baseline File Integrity Monitor

Ustawienia zadania *Baseline File Integrity Monitor* (KSWS) są migrowane do zadania *Sprawdzanie integralności systemu* i do sekcji zasad **Kontrola zabezpieczeń**, podsekcja **Monitor integralności systemu**.

Ustawienia zadania Baseline File Integrity Monitor

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Hash calculation algorithm: • **MD5** • **SHA256**	*(niemigrowane)* Kaspersky Endpoint Security wykorzystuje algorytm SHA256 do obliczania sumy kontrolnej.
Scan scope	**Zakres monitorowania** (podsekcja **Monitor integralności systemu**)

Database Update

Ustawienia zadania *Database Update* (KSWS) są przenoszone do zadania *Aktualizacja baz danych i modułów aplikacji* (KES).

Ustawienia zadania aktualizacji baz danych

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Źródło aktualizacji**: • **Kaspersky Security Center** • **Serwery aktualizacji Kaspersky** • **Określone przez użytkownika**
Use Kaspersky update servers if specified servers are not available	*(niemigrowane)* Kaspersky Endpoint Security umożliwia wybranie kilku źródeł aktualizacji, w tym serwerów aktualizacji Kaspersky. Jeśli pierwsze źródło aktualizacji nie jest dostępne, Kaspersky Endpoint Security umożliwia uzyskanie aktualizacji z innego źródła na liście.

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Use proxy server settings to connect to Kaspersky update servers	*(niemigrowane)* Kaspersky Endpoint Security używa serwera proxy dla wszystkich komponentów. Możesz skonfigurować połączenie z serwerem proxy w opcjach sieciowych aplikacji.
Use proxy server settings to connect to other servers	*(niemigrowane)* Kaspersky Endpoint Security używa serwera proxy dla wszystkich komponentów. Możesz skonfigurować połączenie z serwerem proxy w opcjach sieciowych aplikacji.
Lower the load on the disk I/O	*(niemigrowane)*

Software modules updates

Ustawienia zadania *Software Modules Update* (KSWS) są przenoszone do zadania *Aktualizacja baz danych i modułów aplikacji* (KES).

Ustawienia zadania Aktualizacja modułów oprogramowania

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Źródło aktualizacji**: • **Kaspersky Security Center** • **Serwery aktualizacji Kaspersky** • **Określone przez użytkownika**
Use Kaspersky update servers if specified servers are not available	*(niemigrowane)* Kaspersky Endpoint Security umożliwia wybranie kilku źródeł aktualizacji, w tym serwerów aktualizacji Kaspersky. Jeśli pierwsze źródło aktualizacji nie jest dostępne, Kaspersky Endpoint Security umożliwia uzyskanie aktualizacji z innego źródła na liście.
Use proxy server settings to connect to Kaspersky update servers	*(niemigrowane)* Kaspersky Endpoint Security używa serwera proxy dla wszystkich komponentów. Możesz skonfigurować połączenie z serwerem proxy w opcjach sieciowych aplikacji.
Use proxy server settings to connect to other servers	*(niemigrowane)* Kaspersky Endpoint Security używa serwera proxy dla wszystkich komponentów. Możesz skonfigurować połączenie z serwerem proxy w opcjach sieciowych aplikacji.
Copy and install critical software modules updates	**Instaluj krytyczne i zatwierdzone aktualizacje**
Only check for critical software updates available	*(niemigrowane)* Kaspersky Endpoint Security nieustannie sprawdza dostępność krytycznych aktualizacji dla modułów aplikacji.
Allow operating system restart	*(niemigrowane)* Kaspersky Endpoint Security zapyta użytkownika o pozwolenie na ponowne uruchomienie komputera.
Receive information about available scheduled software modules updates	*(niemigrowane)* Kaspersky Endpoint Security wyświetla powiadomienia o aktualizacjach modułów oprogramowania.

Rollback of Application Database Update

Ustawienia zadania *Rollback of Application Database Update* (KSWS) są przenoszone do zadania *Wycofywanie aktualizacji* (KES). Nowe zadanie *Wycofywanie aktualizacji* (KES) ma terminarz uruchamiania zadania – *Ręcznie*.

On-Demand Scan

Ustawienia zadania *On-Demand Scan* (KSWS) są przenoszone do zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania* (KES).

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Scan scope	Obszar skanowania
Protection level: • Maximum protection • Recommended • Maximum performance	Poziom ochrony: • Wysoki • Zalecany • Niski Ustawienia poziomu ochrony są inne w KSWS i KES.
Objects to scan: • All objects • Objects scanned by format • Objects scanned according to list of extensions specified in anti-virus database • Objects scanned by specified list of extensions	Typy plików: • Wszystkie pliki • Pliki skanowane według formatu • Pliki skanowane według rozszerzenia Kaspersky Endpoint Security nie zezwalaj na tworzenie list niestandardowych rozszerzeń. Kaspersky Endpoint Security zamienia wartość **Objects scanned by specified list of extensions** na wartość **Pliki skanowane według rozszerzenia**.
Subfolders	Włącz podfoldery
Subfiles	*(niemigrowane)*
Scan disk boot sectors and MBR	*(niemigrowane)*
Scan alternate NTFS streams	*(niemigrowane)*
Scan only new and modified files	Skanuj tylko nowe i zmienione pliki
Scan of compound objects: • All archives • All SFX archives • All email databases • All packed objects • All plain email • All embedded OLE objects	Skanowanie plików złożonych: • Skanuj archiwa. • Skanuj archiwa zabezpieczone hasłem. • Skanuj pakiety dystrybucyjne. • Skanuj pliki formatu poczty elektronicznej. • Skanuj pliki w formatach Microsoft Office.
Action to perform on infected and other objects: • Disinfect • Disinfect. Remove if disinfection fails • Remove • Perform recommended action • Notify only	Działanie po wykryciu zagrożenia: • Wylecz; usuń, jeśli leczenie nie jest możliwe. • Wylecz; poinformuj, jeśli leczenie nie jest możliwe. • Poinformuj.
Action to perform on probably infected objects: • Quarantine • Remove • Perform recommended action • Notify only	*(niemigrowane)* Kaspersky Endpoint Security stosuje działanie, jeśli wykryto jakiekolwiek zagrożenie.
Perform actions depending on the type of object detected	*(niemigrowane)*
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	*(niemigrowane)*
Exclude files	*(niemigrowane)* Kaspersky Endpoint Security stosuje strefę zaufaną do wszystkich komponentów. Możesz skonfigurować wykluczenia w ustawieniach strefy zaufanej.
Do not detect	*(niemigrowane)*
Stop scanning if it takes longer than N sec	Pomiń pliki skanowane dłużej niż N sek
Do not scan compound objects larger than N MB	Nie rozpakowuj dużych plików złożonych
Use iSwift technology	Technologia iSwift
Use iChecker technology	Technologia iChecker

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Action on the offline files: • **Do not scan** • **Scan resident part of file only** • **Scan entire file** • **Only if the file has been accessed within the specified period (days)** • **Do not copy file to a local hard drive, if possible**	*(niemigrowane)* Kaspersky Endpoint Security skanuje pliki offline w całości.

Application Integrity Check

Ustawienia zadania *Application Integrity Control* (KSWS) są przenoszone do zadania *Sprawdzanie integralności aplikacji* (KES).

Rule Generator for Applications Launch Control

Kaspersky Endpoint Security nie obsługuje zadania *Applications Launch Control Generator*. Możesz wygenerować reguły w ustawieniach Kontroli aplikacji.

Rule Generator for Device Control

Kaspersky Endpoint Security nie obsługuje zadania *Rule Generator for Device Control*. Możesz wygenerować reguły dostępu w ustawieniach Kontroli urządzeń.

Migracja komponentów KSWS

Przed instalacją lokalną Kaspersky Endpoint Security sprawdzi komputer na obecność aplikacji Kaspersky. Jeśli program Kaspersky Security for Windows Server jest zainstalowany na komputerze, KES wykryje zestaw komponentów KSWS, które są zainstalowane, i wybierze te same komponenty do zainstalowania.

Komponenty KES, których KSWS nie zawiera, są instalowane w następujący sposób:

- Komponenty Ochrona AMSI, Ochrona przed włamaniami, Silnik korygujący są instalowane z domyślnymi ustawieniami.
- Komponenty Ochrona przed atakami BadUSB, Adaptacyjna kontrola anomalii, Szyfrowanie danych, Detection and Response są ignorowane.

Podczas zdalnej instalacji aplikacja KES ignoruje zestaw zainstalowanych komponentów KSWS. Instalator instaluje komponenty wybrane we właściwościach pakietu instalacyjnego. Po zainstalowaniu Kaspersky Endpoint Security oraz migracji zasad i zadań ustawienia KES są konfigurowane zgodnie z ustawieniami KSWS.

Migracja zadań i zasad KSWS

Możesz migrować ustawienia zasad i zadań KSWS w następujące sposoby:

- Używanie Kreatora konwersji zasad i zadań (zwany również dalej „Kreatorem migracji").

  Kreator migracji dla KSWS jest dostępny tylko w Konsoli administracyjnej (MMC). Ustawienia zasad i zadań nie mogą być migrowane w Web Console ani Cloud Console.

Kreator konwersji wsadowej działa inaczej w przypadku różnych wersji Kaspersky Security Center. Zalecamy aktualizację rozwiązania do wersji 14.2 lub nowszej. W tej wersji Kaspersky Security Center Kreator konwersji zasad i zadań umożliwia migrację zasad do profilu, a nie do zasady. W tej wersji Kaspersky Security Center Kreator konwersji zasad i zadań umożliwia również migrację szerszego zakresu ustawień zasad.

- Korzystanie z Kreatora nowej zasady dla Kaspersky Endpoint Security for Windows.

  Kreator tworzenia nowej zasady umożliwia utworzenie zasady KES w oparciu o zasadę KSWS.

Procedury migracji zasady KSWS różnią się w przypadku korzystania z Kreatora migracji i Kreatora tworzenia nowej zasady.

Kreator konwersji zasad i zadań

Kreator migracji przenosi ustawienia zasad KSWS do profilu zasad zamiast ustawień zasad KES. *Profil zasad* to zestaw ustawień zasad, który jest aktywowany na komputerze, jeśli komputer spełnia skonfigurowane reguły aktywacji. Znacznik urządzenia `UpgradedFromKSWS` jest wybrany jako kryterium wyzwalania profilu zasad. Kaspersky Security Center automatycznie dodaje znacznik `UpgradedFromKSWS` do wszystkich komputerów, na których instalujesz KES na KSWS, używając zadania zdalnej instalacji. Jeśli wybrano inną metodę instalacji, możesz ręcznie przypisać znacznik do urządzeń.

W celu dodania znacznika do urządzenia:

1. Utwórz nowy znacznik dla serwerów — `UpgradedFromKSWS`.

   Więcej informacji o tworzeniu znaczników dla urządzeń znajdziesz w pomocy do Kaspersky Security Center.

2. Utwórz nową grupę administracyjną w konsoli Kaspersky Security Center i dodaj serwery, do których chcesz przypisać znacznik do tej grupy.

   Możesz grupować serwery za pomocą narzędzia wyboru. Więcej informacji o pracy z wyborami znajdziesz w pomocy do Kaspersky Security Center.

3. Wybierz wszystkie serwery z grupy administracyjnej w konsoli Kaspersky Security Center, otwórz właściwości wybranych serwerów i przypisz znacznik.

Jeśli wykonujesz migrację wielu zasad KSWS, każda zasada jest konwertowana na profil w ramach jednej zasady nadrzędnej. Jeśli zasada KSWS zawiera już profile, te profile są również migrowane jako profile. W rezultacie otrzymasz jedną zasadę zawierającą profile odpowiadające wszystkim zasadom KSWS.

Jak używać Kreatora konwersji zasad i zadań do migracji ustawień zasad KSWS

1. W Konsoli administracyjnej wybierz Serwer administracyjny i kliknij go prawym klawiszem myszy, aby otworzyć menu kontekstowe.

2. Wybierz **Wszystkie zadania** → **Kreator konwersji zasad i zadań**.

Uruchomi się Kreator konwersji zasad i zadań. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie aplikacji, dla której konieczna jest konwersja zasad i zadań

Na tym etapie należy wybrać Kaspersky Endpoint Security for Windows. Przejdź do następnego kroku.

Krok 2. Konwersja zasad

Kreator migracji tworzy profile zasad KSWS wewnątrz zasady KES. Wybierz zasady Kaspersky Security for Windows Server, które chcesz przekonwerterować na profile zasad. Przejdź do następnego kroku.

Następnie Kreator migracji rozpocznie konwertowanie zasad. Nazwy nowych profili zasad będą odpowiadać pierwotnym zasadom KSWS.

Krok 3. Raport z migracji zasady

Kreator migracji tworzy raport z migracji zasady. Raport z migracji zasady zawiera datę i godzinę konwersji zasady, nazwę pierwotnej zasady KSWS, nazwę docelowej zasady KES oraz nazwę nowego profilu zasad.

Krok 4. Konwersja zadań

Kreator migracji tworzy nowe zadania dla Kaspersky Endpoint Security for Windows. Na liście zadań wybierz zadania KSWS, które chcesz utworzyć dla Kaspersky Endpoint Security. Nowe zadania będą posiadały nazwę *<Nazwa zadania KSWS> (przekonwertowane)*. Przejdź do następnego kroku.

Krok 5. Kończenie działania kreatora

Zakończ działanie Kreatora. W rezultacie kreator wykona następujące czynności:

- Nowe profile zasad są dodawane do zasady Kaspersky Endpoint Security.

  Zasada obejmuje profile z ustawieniami Kaspersky Security for Windows Server. Nowa zasada posiada stan *Aktywna*. Kreator pozostawia zasady KSWS bez zmian.

- Utworzy nowe zadania Kaspersky Endpoint Security.

  Nowe zadania są kopiami zadań KSWS. Kreator pozostawia zadania KSWS bez zmian.

Nowy profil zasad z ustawieniami KSWS zostanie nazwany *UpgradedFromKSWS <Nazwa zasady Kaspersky Security for Windows Server>*. We właściwościach profilu kreator migracji automatycznie wybiera znacznik urządzenia `UpgradedFromKSWS` jako kryterium wyzwalania. W ten sposób ustawienia z profilu zasad są automatycznie stosowane do serwerów.

Kreator tworzenia zasady na podstawie zasady KSWS

Gdy zasada KES jest tworzona na podstawie zasady KSWS, kreator odpowiednio przenosi ustawienia do nowej zasady. Oznacza to, że jedna zasada KES będzie odpowiadać jednej zasadzie KSWS. Kreator nie konwertuje zasady na profil.

Jak używać Kreatora nowej zasady do migracji ustawień zasady KSWS

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej wybierz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Zasady**.
4. Kliknij **Nowa zasada**.

   Zostanie uruchomiony Kreator tworzenia profilu
5. Postępuj zgodnie z instrukcjami Kreatora tworzenia profilu.

Krok 1. Wybieranie aplikacji w celu utworzenia zasad grupy

Wybierz aplikację **Kaspersky Endpoint Security for Windows (14.1)**.

Krok 2. Nadawanie nazwy zasadom grupy

Wprowadź nazwę zasad grupy, na przykład: *Zasady dla biura*.

Zaznacz pole **Użyj ustawień zasady dla wcześniejszej wersji aplikacji**. Kliknij **Przeglądaj** i wybierz zasadę KSWS.

Krok 3. Uczestnictwo w Kaspersky Security Network

Przeczytaj i zaakceptuj warunki Oświadczenia Kaspersky Security Network (KSN).

Krok 4. Wybieranie trybu użytkowania aplikacji na komputerach

Wybierz **Standardowy tryb ochrony hostów**. Kaspersky Endpoint Security zapewnia wspólną zasadę dla wszystkich trybów aplikacji i typów systemów operacyjnych.

Zalecamy używanie różnych zasad do różnych trybów i typów systemów operacyjnych.

Krok 5. Importowanie ustawień

Ten krok będzie dostępny, jeśli w kroku 4 wybrano ręczną konfigurację zasady.

Możesz utworzyć zasadę na podstawie ustawień Kaspersky Endpoint Security z pliku konfiguracyjnego CFG. Kreator nie ma dostępu do wszystkich ustawień zasady podczas importowania pliku konfiguracji aplikacji. W ustawieniach aplikacji brakuje na przykład profili zasad. Jeśli chcesz przenieść wszystkie ustawienia i profile do zasady, możesz zaimportować inną zasadę z pliku KLP.

Podczas importowania pliku konfiguracyjnego Kaspersky Endpoint Security nie przesyła haseł do kontenerów kryptograficznych. Jeśli łączysz się z serwerami za pomocą uwierzytelniania dwukierunkowego, musisz od podstaw określić hasła do kontenerów kryptograficznych.

Krok 6-10. Konfiguracja ustawień zasad

Ten krok będzie dostępny, jeśli w kroku 4 wybrano ręczną konfigurację zasady.

Wykonaj poniższe kroki, aby zarządzać ustawieniami zasad.

Krok 11. Konfigurowanie strefy zaufanej

Skonfiguruj strefę zaufaną. Możesz dodać predefiniowane wykluczenia ze skanowania i zaufane aplikacje. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach. Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje mogą także pomóc w szybkiej konfiguracji Kaspersky Endpoint Security w trybie Light Agent w środowiskach wirtualnych Citrix i VMware.

Krok 12. Wybór statusu zasady

- **Aktywny**. Po kolejnej synchronizacji, profil zostanie uzyty jako profil aktywny.

  Ustawienia aktywnego profilu zostaną zapisane na komputerach klienckich podczas synchronizacji. Nie możesz stosować jednocześnie kilku profili na jednym komputerze, dlatego tylko jeden profil może być aktywny w każdej grupie.

- **Nieaktywny**. Profil Kopii zapasowej. Jeśli to konieczne, profil nieaktywny może zostać przełączony w stan aktywny.

  Możesz utworzyć nieograniczoną liczbę nieaktywnych profili. Profil nieaktywny nie wpływa na ustawienia aplikacji na komputerach w sieci. Profile nieaktywne są przeznaczone do sytuacji wyjątkowych, takich jak atak wirusa. Jeśli dojdzie do ataku za pośrednictwem dysków flash, możesz aktywować profil, który blokuje dostęp do dysków flash. W tym przypadku profil aktywny automatycznie staje się nieaktywny.

- **Użytkownik mobilny**. Profil jest aktywowany, gdy komputer opuści sieć obwodową organizacji.

Zakończ działanie Kreatora.

Dodatkowa konfiguracja zasad i zadań po migracji

KSWS i KES mają różne zestawy komponentów i ustawień zasad, dlatego po migracji należy sprawdzić, czy ustawienia zasad spełniają Twoje korporacyjne wymagania bezpieczeństwa.

Sprawdź następujące podstawowe ustawienia zasad:

- Ochrona hasłem. Ustawienia Ochrony hasłem KSWS nie są migrowane. Kaspersky Endpoint Security ma wbudowaną funkcję Ochrony hasłem. Jeśli to konieczne, włącz Ochronę hasłem i ustaw hasło.

- Strefa zaufana. Metody używane przez KSWS i KES do wybierania obiektów różnią się. Podczas migracji KES obsługuje wykluczenia zdefiniowane jako pojedyncze pliki lub ścieżki do piku/folderu. Jeśli KSWS posiada wykluczenia skonfigurowane jako predefiniowany obszar lub adres URL skryptu, takie wykluczenia nie zostaną przeniesione. Po migracji musisz dodać takie wykluczenia ręcznie.

  > Aby upewnić się, że Kaspersky Endpoint Security działa poprawnie na serwerach, zaleca się dodanie plików ważnych dla funkcjonowania serwera do strefy zaufanej. W przypadku serwerów SQL należy dodać pliki baz danych MDF i LDF. W przypadku serwerów Microsoft Exchange należy dodać pliki CHK, EDB, JRS, LOG i JSL. Możesz użyć masek, np. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

  > Począwszy od Kaspersky Endpoint Security 12.6 for Windows, wykluczenia skanowania I zaufane aplikacje są dodawane do strefy zaufanej. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach.

- Zapora sieciowa. Funkcje zapory KSWS są wykonywane przez zaporę na poziomie systemu. W KES za funkcjonalność zapory sieciowej odpowiada osobny komponent. Po migracji możesz skonfigurować zaporę sieciową Kaspersky Endpoint Security.

- Kaspersky Security Network. Kaspersky Endpoint Security nie obsługuje konfigurowania KSN dla poszczególnych komponentów. Kaspersky Endpoint Security używa KSN dla wszystkich składników aplikacji. Aby korzystać z KSN, musisz zaakceptować nowe warunki Oświadczenia Kaspersky Security Network.

- Kontrola sieci. Blokowanie reguł kontroli kategorii ruchu sieciowego są przenoszone do pojedynczej reguły blokowania w Kaspersky Endpoint Security. Kaspersky Endpoint Security ignoruje reguły zezwalające dla kontroli kategorii. Kaspersky Endpoint Security nie obsługuje wszystkich kategorii Kaspersky Security for Windows Server. Kategorie, które nie istnieją w Kaspersky Endpoint Security, nie są przenoszone. Dlatego też, reguły klasyfikacji zasobów internetowych z nieobsługiwanymi kategoriami nie są przenoszone. Jeśli to konieczne, dodaj reguły Kontroli sieci.

- Serwer proxy. Hasło połączenia z serwerem proxy nie jest migrowane. Wprowadź ręcznie hasło, które będzie używane do łączenia się z serwerem proxy.

- Terminarze poszczególnych komponentów. Kaspersky Endpoint Security nie obsługuje konfigurowania terminarzy dla poszczególnych komponentów. Komponenty są zawsze włączone, gdy działa program Kaspersky Endpoint Security.

- Zestaw komponentów. Zestaw dostępnych funkcji Kaspersky Endpoint Security zależy od typu systemu operacyjnego: stacja robocza lub serwer. Przykładowo spośród narzędzi szyfrujących na serwerach dostępne jest tylko Szyfrowanie dysków funkcją BitLocker.

- Atrybut . Stan atrybutu nie jest migrowany. Atrybut będzie miał wartość domyślną. Domyślnie prawie wszystkie ustawienia w nowej zasadzie mają zastosowany zakaz modyfikowania ustawień w zasadach podrzędnych oraz w lokalnym interfejsie aplikacji. Atrybut ma wartość dla ustawień zasad w sekcji **Managed Detection and Response (Industrial CyberSecurity)** i w grupie ustawień **Pomoc techniczna** (sekcji **Interfejs**). W razie potrzeby skonfiguruj dziedziczenie ustawień z zasady nadrzędnej.

- Praca z aktywnymi zagrożeniami. Zaawansowane leczenie działa inaczej dla stacji roboczych i serwerów. Możesz skonfigurować zaawansowane leczenie w ustawieniach zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania* i w ustawieniach aplikacji.

- Uaktualnianie aplikacji. Aby zainstalować ważne aktualizacje i poprawki bez ponownego uruchamiania, musisz zmienić tryb aktualizacji aplikacji. Domyślnie funkcja Zainstaluj aktualizacje aplikacji bez ponownego uruchomienia jest wyłączona.

- Kaspersky Endpoint Agent. Kaspersky Endpoint Security ma wbudowanego agenta współpracującego z rozwiązaniami Detection and Response. Jeśli to konieczne, przenieś ustawienia zasad Kaspersky Endpoint Agent do zasady Kaspersky Endpoint Security.

- Zadania *Aktualizacja baz danych i modułów aplikacji*. Upewnij się, że ustawienia zadania *Aktualizacja baz danych i modułów aplikacji* zostały poprawnie zmigrowane. Zamiast trzech zadań KSWS KES używa jednego zadania KES. Możesz zoptymalizować zadania *Aktualizacja baz danych i modułów aplikacji* i usunąć zbędne zadania.

- Inne zadania. Komponenty Kontrola aplikacji, Kontrola urządzeń i Monitor integralności plików działają inaczej w KSWS i KES. KES nie używa zadań *Baseline File Integrity Monitor*, *Applications Launch Control Generator*, *Rule Generator for Device Control*. W związku z tym te zadania nie są migrowane. Po migracji możesz skonfigurować komponenty Monitor integralności plików, Kontrola aplikacji, Kontrola urządzeń.

Migracja strefy zaufanej KSWS

Strefa zaufana jest utworzoną przez administratora listą obiektów i aplikacji, które nie są monitorowane przez Kaspersky Endpoint Security. Możesz migrować obiekty strefy zaufanej z KSWS do KES za pomocą *Kreatora konwersji zasad i zadań* lub *kreatora tworzenia nowych zasad KES na podstawie zasad KSWS*. KSWS i KES mają różne zestawy składników i funkcji, dlatego po migracji musisz sprawdzić, czy wykluczenia spełniają korporacyjne wymagania bezpieczeństwa. Różnią się również metody dodawania wykluczeń do strefy zaufanej. Kreator migracji nie ma narzędzi umożliwiających migrację wszystkich wykluczeń KSWS. Oznacza to, że po migracji musisz ręcznie dodać niektóre wykluczenia KSWS.

Aby upewnić się, że Kaspersky Endpoint Security działa poprawnie na serwerach, zaleca się dodanie plików ważnych dla funkcjonowania serwera do strefy zaufanej. W przypadku serwerów SQL należy dodać pliki baz danych MDF i LDF. W przypadku serwerów Microsoft Exchange należy dodać pliki CHK, EDB, JRS, LOG i JSL. Możesz użyć masek, np. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Począwszy od Kaspersky Endpoint Security 12.6 for Windows, wykluczenia skanowania I zaufane aplikacje są dodawane do strefy zaufanej. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach.

Metody tworzenia strefy zaufanej KES i KSWS.

KSWS		KES
Object to scan		
• Predefined scope	*(niemigrowane)*	
• Disk, folder or network location	→	**Plik lub folder**
• File	→	**Plik lub folder**
• Script file or web address	*(niemigrowane)*	
Detected object	→	**Typ wykrywanych obiektów**
Trusted processes	→	**Zaufane aplikacje**

Migracja zeskanowanych obiektów

Wykluczenia KSWS z wybraną metodą **Object to scan** są migrowane do wykluczeń KES z wybraną metodą **Plik lub folder**, oczywiście z pewnymi ograniczeniami. Migracja wykluczeń zależy od metody wyboru obiektów:

- Predefined scope – *nie są migrowane*.

  Po migracji musisz dodać takie wykluczenia ręcznie. Wykluczenia będące wstępnie zdefiniowanymi obszarami musisz skonfigurować w ustawieniach zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

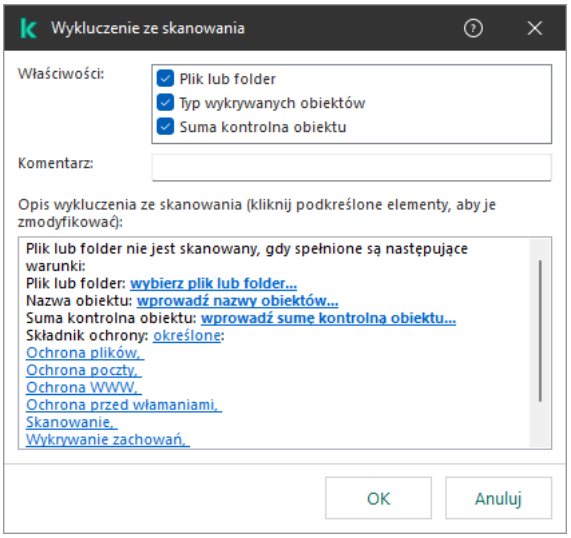
- Disk, folder or network location – migrowane do wykluczeń KES, które we właściwościach mają wybraną metodę „Plik lub folder".

- File – migrowane do wykluczeń KES, które we właściwościach mają wybraną metodę „Plik lub folder".

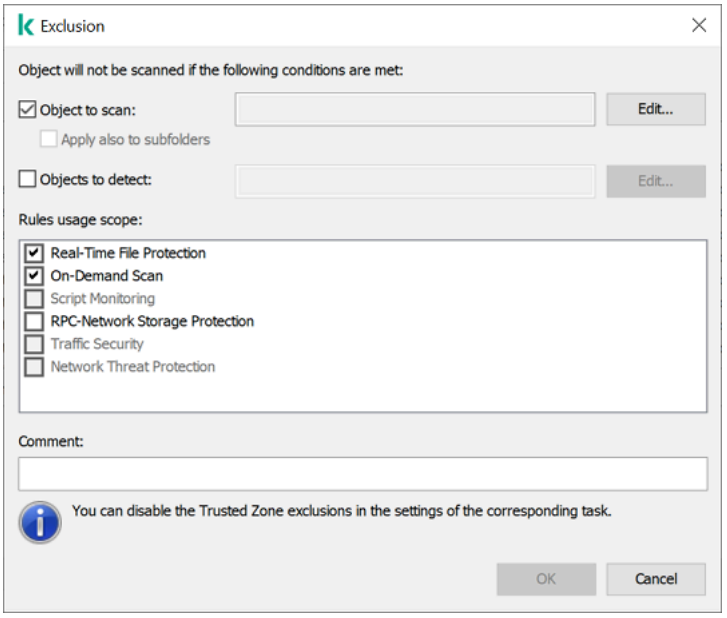
- Script file or web address – *nie są migrowane*.

  Po migracji musisz dodać takie wykluczenia ręcznie. Z kolei wykluczenia będące adresami sieciowymi skryptu musisz dodać do listy zaufanych adresów internetowych Ochrony WWW.

Jeżeli we właściwościach zeskanowanego obiektu zaznaczone jest pole wyboru **Apply also to subfolders**, ustawienie to jest migrowane do wykluczeń KES (pole wyboru **Włącz podfoldery**).



Ustawienia wykluczeń KES



Ustawienia wykluczeń KSWS

Migracja wykrytych obiektów

Wykluczenia KSWS z wybraną metodą **Detected object** są migrowane do wykluczeń KES z wybraną metodą **Typ wykrywanych obiektów**. Nazwa wykrytego obiektu odpowiada klasyfikacji z Encyklopedii Kaspersky (na przykład `Email-Worm`, `Rootkit` lub `RemoteAdmin`). Kaspersky Endpoint Security obsługuje maski ze znakami zapytania `?` (zastępuje dowolny pojedynczy znak) i gwiazdką `*` (zastępuje dowolną liczbę znaków).

Migracja zakresu użycia wykluczenia

Zakres użycia wykluczenia określa zestaw składników, do których zastosowanie ma wykluczenie. KES i KSWS mają różne zestawy składników, więc Kreator migracji nie umożliwia migracji zakresu użycia wykluczenia. W związku z tym, jeżeli przynajmniej jeden składnik jest wybrany w zakresie użycia KSWS, KES stosuje wykluczenie do wszystkich składników aplikacji.

Zakres użycia KSWS konfiguruje się w ustawieniach strefy zaufanej, a także w ustawieniach składnika ochrony KSWS. W tym celu możesz zaznaczyć pole wyboru **Apply Trusted Zone** lub usunąć jego zaznaczenie w odpowiednim obszarze zasad. Ustawienia składników ochrony KES nie mają takiego pola wyboru. Oznacza to, że po migracji stan strefy zaufanej z ustawień danego składnika zostanie utracony. Po zakończeniu migracji wybierz składniki, do których wykluczenie ma być stosowane w ustawieniach strefy zaufanej w zasadach KES.

Migracja komentarzy

Komentarze ze strefy zaufanej KSWS są migrowane do komentarzy wykluczenia KES bez żadnych zmian.

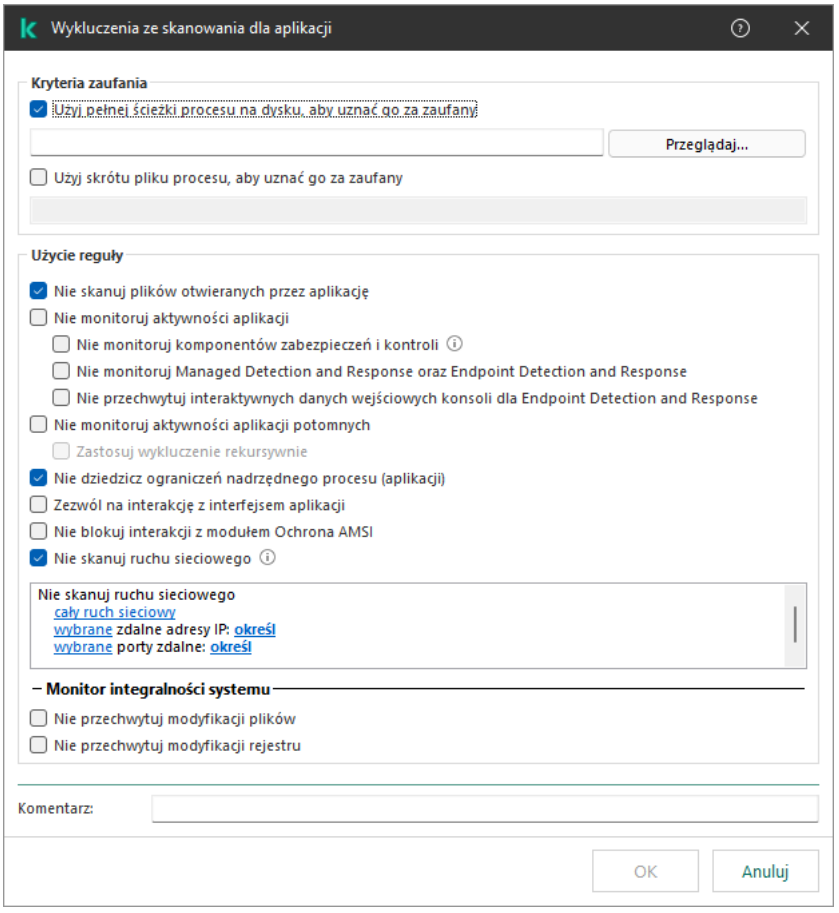
Migracja procesów zaufanych

Procesy zaufane KSWS są migrowane do procesów zaufanych KES z pewnymi ograniczeniami. Zakres migracji zaufanych procesów zależy od metody wyboru obiektów:

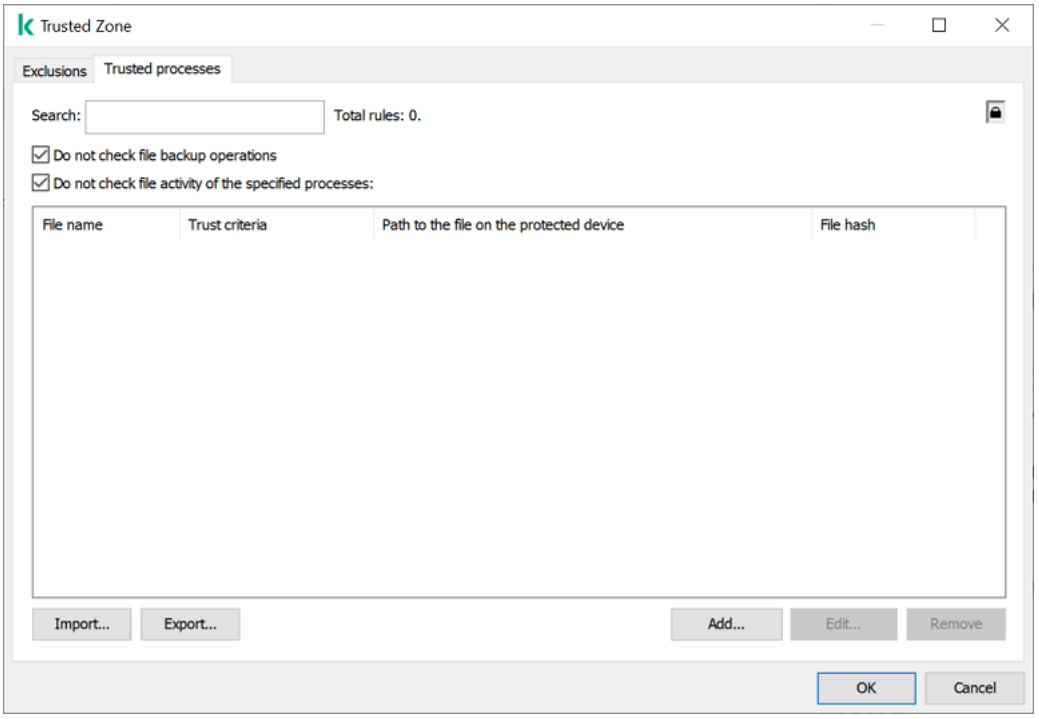
- Path to the file on the protected device – migracja do zaufanych aplikacji KES.
- File hash – *nie są migrowane*.

Jeśli KSWS zawiera zaufane procesy skonfigurowane jako skrót pliku, takie zaufane procesy nie są przenoszone. Po migracji musisz ręcznie dodać takie zaufane procesy.

Jeżeli w ustawieniach procesu zaufanego zaznaczone jest pole wyboru **Do not check file backup operations**, ustawienie to jest migrowane do aplikacji zaufanych KES (pole wyboru **Nie monitoruj aktywności aplikacji**).



Ustawienia aplikacji zaufanych KES



Ustawienia procesów zaufanych KSWS

Migracja reguł zadania Kontrola uruchamiania aplikacji KSWS

Kontrola uruchamiania aplikacji KSWS jest domyślnie blokowana. Oznacza to, że Kontrola uruchamiania aplikacji automatycznie blokuje wszystkie aplikacje, które nie są określone w regułach jako dozwolone. Dlatego kreator migracji dla Kontroli aplikacji KES automatycznie ustawia tryb kontroli **Lista zezwolonych**, który odpowiada zasadzie domyślnego blokowania.

Możesz migrować reguły z KSWS do KES za pomocą *kreatora konwersji zasad i zadań* lub *kreatora tworzenia nowych zasad KES na podstawie zasad KSWS*.

Migracja trybu zadania Kontrola uruchamiania aplikacji

Tryb zadania Kontrola uruchamiania aplikacji KSWS migruje do Kontroli aplikacji KES w następujący sposób:

- **Statistics only** → **Przetestuj reguły**;
- **Active** → **Zastosuj reguły**.

Migracja wstępnie zdefiniowanych reguł zadania Kontrola uruchamiania aplikacji KSWS

Domyślnie Kontrola uruchamiania aplikacji KSWS zawiera dwie reguły:

- **Allow scripts and MSI by OS-trusted certificate**
- **Allow executable by OS-trusted certificate**

Wstępnie zdefiniowane reguły pozwalają na uruchamianie *skryptów*, *pakietów MSI* i *plików wykonywalnych* podpisanych przez zaufany certyfikat główny. Jeśli przynajmniej jedna wstępnie zdefiniowana reguła KSWS ma typ **Allow**, to kreator migracji tworzy nową regułę zezwalającą – **Aplikacje z zaufanymi certyfikatami głównymi**. Oznacza to, że Kontrola Aplikacji KES używa pojedynczej reguły, aby umożliwić uruchamianie zaufanych skryptów, pakietów MSI i plików wykonywalnych.

Jeśli obie wstępnie zdefiniowane reguły KSWS mają typ **Deny**, KES ignoruje wstępnie zdefiniowane reguły.

Migracja reguł niestandardowych zadania Kontrola uruchamiania aplikacji KSWS

Reguły Kontroli uruchamiania aplikacji KSWS regulują wykonywanie plików według następujących kryteriów:

- Podpis z certyfikatem cyfrowym
- Suma kontrolna SHA256
- ścieżka pliku.

Reguły są tworzone inaczej w KSWS i KES, dlatego kreator migracji tworzy *kategorie aplikacji*, które obejmują warunki i wykluczenia z zasad KSWS, i dodaje te kategorie aplikacji do zasad KES. Kreator używa warunków **Certyfikat**, **Ścieżka do folderu** i **Suma kontrolna pliku** w kategoriach aplikacji. Nowe kategorie aplikacji są dostępne w Konsoli administracyjnej Kaspersky Security Center w sekcji **Zarządzanie aplikacjami** → **Kategorie aplikacji**.

Kreator migracji grupuje reguły KSWS według typu i użytkownika. Następnie kreator tworzy kategorie aplikacji obejmujące warunki i wykluczenia z reguł KSWS, a następnie dodaje kategorie aplikacji do nowych reguł KES. Kreator określa nazwy reguł KSWS w polu **Opis** reguł KES.

Migracja zaawansowanych ustawień zadania Kontrola uruchamiania aplikacji KSWS

Zasada działania zadań Kontroli uruchamiania aplikacji KSWS i Kontroli aplikacji KES jest inna, dlatego kreator migracji może przenieść podzbiór ustawień.

Ustawienia Kontroli uruchamiania aplikacji

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Repeat action taken for the first file launch on all the subsequent launches for this file	*(niemigrowane)* Kaspersky Endpoint Security skanuje aplikację przy każdym jej uruchomieniu.
Deny the command interpreters launch with no command to execute	*(niemigrowane)* Kaspersky Endpoint Security zezwala na uruchomienie programu interpretującego polecenie, jeśli nie są zabronione przez Kontrolę aplikacji.
Apply rules to executable files	*(niemigrowane)* Zakresu stosowania reguł nie można skonfigurować w ustawieniach Kontroli aplikacji KES. Kontrola aplikacji KES stosuje zasady do wszystkich typów plików: plików wykonywalnych, skryptów i pakietów MSI. Jeśli wszystkie typy plików są objęte zakresem stosowania reguł w KSWS, podczas migracji KES przenosi reguły KSWS. Jeżeli jakiś typ pliku jest wyłączony z zakresu stosowania reguł w KSWS, to podczas migracji KES przenosi również reguły KSWS, ale jako akcję Kontroli aplikacji wybiera się **Przetestuj reguły**.
Monitor loading of DLL modules	**Monitoruj ładowanie modułów DLL (znacznie zwiększa obciążenie systemu)**
Apply rules to scripts and MSI packages	*(niemigrowane)* Zakresu stosowania reguł nie można skonfigurować w ustawieniach Kontroli aplikacji KES. Kontrola aplikacji KES stosuje zasady do wszystkich typów plików: plików wykonywalnych, skryptów i pakietów MSI. Jeśli wszystkie typy plików są objęte zakresem stosowania reguł w KSWS, podczas migracji KES przenosi reguły KSWS. Jeżeli jakiś typ pliku jest wyłączony z zakresu stosowania reguł w KSWS, to podczas migracji KES przenosi reguły KSWS, ale jako akcję Kontroli aplikacji wybiera się **Przetestuj reguły**.
Deny applications untrusted by KSN	*(niemigrowane)* Kaspersky Endpoint Security nie bierze pod uwagę reputacji aplikacji i umożliwia lub zabrania uruchamiania aplikacji zgodnie z regułami.

Ustawienia Kaspersky Security for Windows Server	Ustawienia Kaspersky Endpoint Security for Windows
Allow applications trusted by KSN	Podczas migracji KES dodaje nową regułę zezwalającą. Jako warunek wyzwalający regułę jest podana kategoria KL **Inne oprogramowanie\Aplikacje zaufane zgodnie z reputacją w KSN**.
Users and / or user groups allowed to run applications trusted by KSN	**Użytkownicy i ich uprawnienia** to reguła zezwalająca Kontroli aplikacji, która obejmuje kategorię KL **Inne oprogramowanie\Aplikacje zaufane zgodnie z reputacją w KSN**.
Automatically allow software distribution via applications and packages listed	Kontrola dystrybucji oprogramowania w KSWS i KES działa inaczej. Podczas migracji KES dodaje nowe reguły zezwalające dla aplikacji, które mają dozwoloną automatyczną dystrybucję oprogramowania. Jako warunek wyzwolenia reguły podana jest suma kontrolna pliku.
Always allow software distribution via Windows Installer	Kontrola dystrybucji oprogramowania w KSWS i KES działa inaczej. Podczas migracji KES dodaje nowe reguły zezwalające dla aplikacji, które mają dozwoloną automatyczną dystrybucję oprogramowania (**Software distribution applications and packages allowed**). Jako warunek wyzwolenia reguły podana jest suma kontrolna pliku. Pole wyboru **Zaufane programy aktualizujące** we właściwościach konta jest zaznaczone.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(niemigrowane)*
Software distribution applications and packages allowed	Kontrola dystrybucji oprogramowania w KSWS i KES działa inaczej. Podczas migracji KES dodaje nowe reguły zezwalające dla aplikacji, które mają dozwoloną automatyczną dystrybucję oprogramowania. Jako warunek wyzwolenia reguły podana jest suma kontrolna pliku. Pole wyboru **Zaufane programy aktualizujące** we właściwościach konta jest zaznaczone.
Schedule settings	*(niemigrowane)* Jeśli dla komponentu w ustawieniach KSWS skonfigurowano harmonogram, komponent Kontrola aplikacji jest włączany przy migracji. Jeśli dla komponentu nie skonfigurowano harmonogramu w ustawieniach KSWS, Kontrola aplikacji jest wyłączona przy migracji. Nie jest możliwe skonfigurowanie oddzielnego terminarza dla komponentu. Komponent jest zawsze włączony, gdy działą program Kaspersky Endpoint Security.

Instalowanie KES zamiast KSWS

Możesz zainstalować Kaspersky Endpoint Security na następujące sposoby:

- Instalowanie KES po usunięciu KSWS (zalecane).
- Instalowanie KES na KSWS.

Usuwanie Kaspersky Security for Windows Server

Możesz usunąć aplikację zdalnie za pomocą zadania *Zdalna dezinstalacja aplikacji* lub lokalnie na serwerze. Po usunięciu KSWS może być konieczne ponowne uruchomienie serwera. Jeśli chcesz zainstalować Kaspersky Endpoint Security bez ponownego uruchamiania, upewnij się, że Kaspersky Security for Windows Server został całkowicie usunięty. Jeśli aplikacja nie zostanie całkowicie usunięta, instalacja Kaspersky Endpoint Security może spowodować nieprawidłowe działanie serwera. Upewnienie się, że aplikacja została całkowicie usunięta, jest również zalecane, jeśli było używane narzędzie kavremover. Narzędzie kavremover nie obsługuje zarządzania KSWS.

Jeżeli włączona jest funkcja ochrony hasłem ograniczająca dostęp do KSWS, wprowadź hasło dezinstalacyjne w ustawieniach pakietu instalacyjnego KES.

Po usunięciu KSWS zainstaluj Kaspersky Endpoint Security for Windows przy użyciu dowolnej dostępnej metody.

Instalowanie Kaspersky Endpoint Security

Podczas zdalnej instalacji KES komponenty wybrane we właściwościach pakietu instalacyjnego są instalowane na serwerze. Zalecamy wybranie domyślnych komponentów we właściwościach pakietu instalacyjnego. Ponowne uruchomienie nie jest konieczne podczas instalowania KES na KSWS.

Przed instalacją lokalną Kaspersky Endpoint Security sprawdzi komputer na obecność aplikacji Kaspersky. Jeśli program Kaspersky Security for Windows Server jest zainstalowany na komputerze, KES wykryje zestaw komponentów KSWS, które są zainstalowane, i wybierze te same komponenty do zainstalowania. Ponowne uruchomienie nie jest konieczne podczas instalowania KES na KSWS.

Jeśli instalacja KES na KSWS nie powiodła się, możesz cofnąć instalację. Po wycofaniu instalacji zaleca się ponowne uruchomienie serwera i podjęcie ponownej próby.

Ustawienia i zadania KSWS nie są przenoszone, gdy jest zainstalowany program Kaspersky Endpoint Security for Windows. Aby przeprowadzić migrację ustawień i zadań, uruchom Kreatora konwersji zasad i zadań.

Listę zainstalowanych komponentów możesz sprawdzić w sekcji **Bezpieczeństwo**, w interfejsie aplikacji, korzystając z polecenia `status`, lub w konsoli Kaspersky Security Center, we właściwościach komputera. Możesz zmienić zestaw komponentów po instalacji, używając zadania *Zmiana składników aplikacji*.

Migracja konfiguracji [KSWS+KEA] do konfiguracji [KES+wbudowany agent]

Aby wspierać korzystanie z Kaspersky Endpoint Security for Windows w ramach EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA i MDR, do aplikacji dodano wbudowanego agenta. Nie potrzebujesz już oddzielnej aplikacji Kaspersky Endpoint Agent do pracy z tymi rozwiązaniami.

Po migracji z KSWS do KES rozwiązania EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA i MDR nadal działają z wbudowanymi agentami Kaspersky Endpoint Security. Dodatkowo, Kaspersky Endpoint Agent zostanie usunięty z komputera.

Migrowanie konfiguracji [KSWS+KEA] do [KES+wbudowany agent] obejmuje następujące etapy:

1. **Migracja z KSWS do KES**

   Migracja z KSWS do KES obejmuje instalowanie Kaspersky Endpoint Security zamiast Kaspersky Security for Windows Server.

Administratorzy zazwyczaj włączają Ochronę hasłem, aby ograniczyć dostęp do KSWS i KEA. Począwszy od wersji Kaspersky Security Center Linux 15.1, możesz wprowadzić hasło dezinstalacyjne aplikacji w ustawieniach zadania *Zdalna instalacja aplikacji*. Zadanie umożliwia wprowadzenie tylko jednego hasła dezinstalacyjnego. Oznacza to, że jeśli dla KSWS i KEA zostanie ustawione to samo hasło, aplikacje KSWS i KEA zostaną pomyślnie usunięte. Jeżeli hasła są różne, usunięcie jednej z aplikacji nie powiedzie się z powodu błędu dostępu. Aby dokończyć migrację, należy wyłączyć funkcję ochrony hasłem dla aplikacji, której hasła nie można było wprowadzić w ustawieniach zadania *Zdalna instalacja aplikacji*.

Aby przeprowadzić migrację, musisz wybrać komponenty potrzebne do obsługi rozwiązań Detection and Response w ramach Kaspersky Endpoint Security. Po zainstalowaniu aplikacji Kaspersky Endpoint Security przełącza się na używanie wbudowanego agenta i usuwa Kaspersky Endpoint Agent.

2 Migrowanie zasady i zadań

Migracja polityk i zadań [KSWS+KEA] do [KES+wbudowany agent] obejmuje następujące kroki:

1. Migrowanie profili i zadań z KSWS do KES za pomocą Kreatora konwersji zasad i zadań (dostępne tylko w Konsoli administracyjnej (MMC)).

   W rezultacie profil zasad o nazwie *UpgradedFromKSWS<Nazwa zasady Kaspersky Security for Windows Server>* zostanie dodany do polityki KES. Nowe zadania KES są również tworzone z nazwami *<nazwa zadania KSWS> (przekonwertowane)*.

2. Migrowanie profili i zadań z KEA do KES przy użyciu kreatora migracji z Kaspersky Endpoint Agent (dostępne tylko w Web Console i Cloud Console).

   W rezultacie tworzona jest nowa zasada o podanej nazwie *<Nazwa zasady Kaspersky Endpoint Security> i <Nazwa zasady Kaspersky Endpoint Agent>*. Tworzone są również nowe zadania i zadania KES.

3 Funkcjonalność licencjonowania

Jeśli do aktywowania Kaspersky Endpoint Security for Windows i Kaspersky Endpoint Agent używasz wspólnej licencji dla Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security, funkcjonalność EDR Optimum zostanie aktywowana automatycznie po zaktualizowaniu aplikacji do wersji 11.7.0. Nie musisz robić nic innego.

Jeśli do aktywowania funkcjonalności EDR Optimum używasz autonomicznej licencji Kaspersky Endpoint Detection and Response Optimum Add-on, musisz upewnić się, że klucz EDR Optimum Add-on zostanie dodany do repozytorium Kaspersky Security Center, a funkcjonalność automatycznej dystrybucji klucza licencyjnego zostanie włączona. Po zaktualizowaniu aplikacji do wersji 11.7.0, funkcjonalność EDR Optimum zostanie aktywowana automatycznie.

Jeśli do aktywowania Kaspersky Endpoint Agent użyjesz licencji dla Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security, a do aktywowania Kaspersky Endpoint Security for Windows użyjesz innej licencji, musisz zastąpić klucz Kaspersky Endpoint Security for Windows standardowym kluczem Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security. Możesz zastąpić klucz przy użyciu zadania *Dodaj klucz*.

Nie musisz aktywować funkcjonalności Kaspersky Sandbox. Funkcjonalność Kaspersky Sandbox będzie dostępna natychmiast po zaktualizowaniu i aktywowaniu Kaspersky Endpoint Security for Windows.

Tylko licencja Kaspersky Anti Targeted Attack Platform może zostać użyta do aktywacji Kaspersky Endpoint Security w ramach rozwiązania Kaspersky Anti Targeted Attack Platform. Po zaktualizowaniu aplikacji do wersji 12.1, funkcjonalność EDR (KATA) zostanie aktywowana automatycznie. Nie musisz robić nic innego.

4 Sprawdzanie zdrowia Kaspersky Endpoint Detection and Response Optimum i Kaspersky Sandbox

Jeśli po aktualizacji, komputer posiada stan *Krytyczny* w konsoli Kaspersky Security Center:

- Upewnij się, że na komputerze jest zainstalowany Agent sieciowy w wersji 13.2 lub wyższej.
- Sprawdź stan działania komponentów, przeglądając *Raport o stanie składników aplikacji*. Jeśli komponent ma stan *Nie zainstalowano*, zainstaluj komponent przy użyciu zadania *Zmiana składników aplikacji*.
- Upewnij się, że akceptujesz Oświadczenie Kaspersky Security Network w nowej zasadzie Kaspersky Endpoint Security for Windows.

Upewnij się, że funkcja EDR Optimum została aktywowana za pomocą opcji *Raport o stanie składników aplikacji*. Jeśli komponent posiada stan *Nieobjęte licencją*, upewnij się, że funkcjonalność automatycznej dystrybucji klucza licencyjnego EDR Optimum jest włączona.

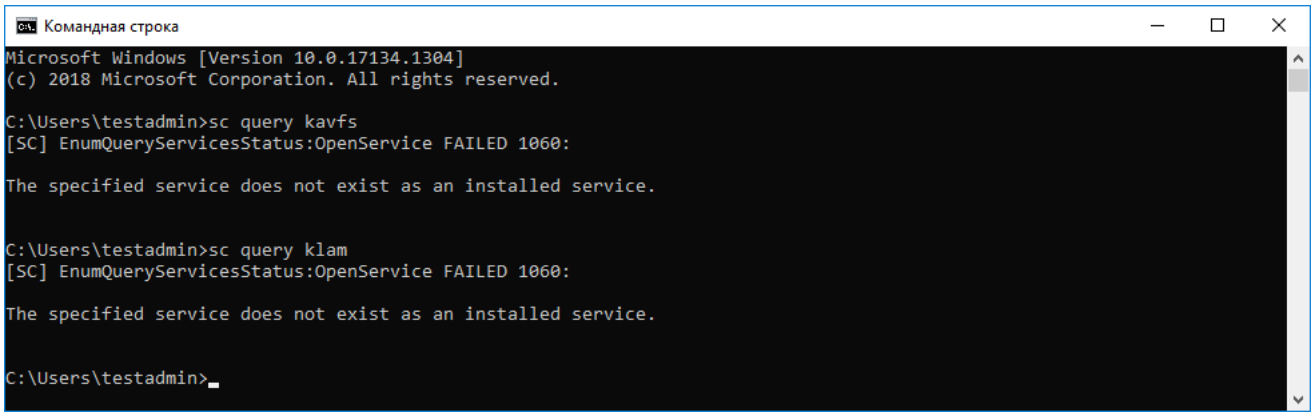
Upewnianie się, że pomyślnie usunięto Kaspersky Security for Windows Server

Upewnij się, że Kaspersky Security for Windows Server został całkowicie usunięty:

- Folder `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` nie istnieje.
- Brak następujących usług:
  - Kaspersky Security Service (KAVFS)
  - Usługa Kaspersky Security Management (KAVFSGT)
  - Usługa Kaspersky Security Exploit Prevention (KAVFSSLP)
  - Usługa Kaspersky Security Script Checker (KAVFSSCS)

  Możesz sprawdzić uruchomione usługi w Menedżerze zadań lub wywołując polecenie `sc query` (patrz rysunek poniżej).
- Brak następujących sterowników:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

Możesz sprawdzić zainstalowane sterowniki w folderze `C:\Windows\System32\drivers` lub wywołując polecenie `sc query`. Jeśli brakuje usługi lub sterownika, otrzymasz następującą odpowiedź:



Upewnij się, że usługi i sterowniki Kaspersky Security for Windows Server zostały pomyślnie usunięte

Jeśli pliki aplikacji lub sterowników pozostały na serwerze, usuń je ręcznie. Jeśli usługi Kaspersky Security for Windows Server nadal działają na serwerze, zatrzymaj (`sc stop`) i usuń (`sc delete`) usługi ręcznie. Aby zatrzymać sterownik klam.sys, użyj polecenia `fltmc unload klam`.

Aktywowanie KES przy użyciu klucza dla KSWS

Po zainstalowaniu aplikacji możesz aktywować Kaspersky Endpoint Security for Windows (KES) przy użyciu klucza licencyjnego Kaspersky Security for Windows Server (KSWS). Proces aktywacji po migracji zależy od metody aktywacji KSWS (patrz tabela poniżej).

Kaspersky Endpoint Security nie obsługuje *licencji na Kaspersky Security for Storage*. Aby pracować z tą licencją, musisz użyć Kaspersky Security for Windows Server.

Aby aktywować KES za pomocą klucza KSWS, możesz użyć tylko kodu aktywacyjnego. Jeżeli używasz pliku klucza do aktywacji aplikacji, musisz skontaktować się z Pomocą techniczną, aby uzyskać plik klucza Kaspersky Endpoint Security.

Aktywowanie Kaspersky Endpoint Security for Windows przy użyciu klucza Kaspersky Security for Windows Server

Metoda aktywacji Kaspersky Security for Windows Server	Migrowanie klucza do Kaspersky Endpoint Security for Windows.
Automatyczna dystrybucja klucza licencyjnego KSWS na komputery.	Jeśli automatyczna dystrybucja klucza jest włączona we właściwościach klucza licencyjnego KSWS, program KES jest automatycznie aktywowany przy użyciu klucza KSWS.
Klucz KSWS jest dodawany przez zadanie.	Jeśli Twój program KSWS jest aktywowany przy użyciu zadania, klucz licencyjny KSWS jest usuwany podczas migracji z KSWS. Musisz ponownie aktywować aplikację. Na przykład, możesz dodać klucz licencyjny do pakietu instalacyjnego Kaspersky Endpoint Security for Windows.
Klucz KSWS jest dodawany lokalnie w interfejsie aplikacji.	Jeśli Twój program KSWS jest aktywowany lokalnie przy użyciu Kreatora aktywacji aplikacji, klucz licencyjny KSWS jest usuwany podczas migracji z KSWS. Musisz ponownie aktywować aplikację. Na przykład, możesz dodać klucz licencyjny do pakietu instalacyjnego Kaspersky Endpoint Security for Windows.
Klucz KSWS zostanie dodany do pakietu instalacyjnego.	Jeśli Twój produkt KSWS jest aktywowany przy użyciu klucza z pakietu instalacyjnego, klucz licencyjny dla KSWS jest usuwany podczas migracji z KSWS. Musisz ponownie aktywować aplikację. Na przykład, możesz dodać klucz licencyjny do pakietu instalacyjnego Kaspersky Endpoint Security for Windows.

Metoda aktywacji Kaspersky Security for Windows Server	Migrowanie klucza do Kaspersky Endpoint Security for Windows.
Płatny obraz maszyny wirtualnej (Amazon Machine Image — AMI) w Amazon Web Services (AWS).	Jeśli zakupiono Kaspersky Security Center jako płatny obraz maszyny wirtualnej (Amazon Machine Image — AMI) w Amazon Web Services (AWS), aktywacja KES nie jest wymagana. W takim przypadku Kaspersky Security Center używa subskrypcji AWS, która jest już dodana do aplikacji.
Gotowy, bezpłatny obraz Kaspersky Security Center z własną licencją (model Bring Your Own License — BYOL).	Jeśli używasz gotowego, bezpłatnego obrazu Kaspersky Security Center z własną licencją w środowisku chmury (model Bring Your Own License — BYOL), musisz aktywować aplikację przy użyciu dowolnej dostępnej metody. Będziesz potrzebować licencji Kaspersky Hybrid Cloud Security.

Specjalne kwestie dotyczące migracji serwerów o dużym obciążeniu

Na serwerach o dużym obciążeniu ważne jest monitorowanie wydajności i unikanie błędów. Po migracji do Kaspersky Endpoint Security for Windows zalecamy tymczasowe wyłączenie składników aplikacji, które zużywają znacznie więcej zasobów serwera niż inne składniki. Po upewnieniu się, że serwer działa normalnie, możesz ponownie włączyć składniki aplikacji.

Zalecamy wykonanie migracji serwerów o dużym obciążeniu w następujący sposób:

1. Utworzenie zasady Kaspersky Endpoint Security z ustawieniami domyślnymi.

   Domyślne ustawienia są uznawane za optymalne. Te ustawienia są zalecane przez ekspertów z Kaspersky. Domyślne ustawienia zawierają zalecany poziom ochrony i optymalne zużycie zasobów.

2. Wyłączenie w ustawieniach zasad następujących komponentów: Ochrona sieci, Wykrywanie zachowań, Ochrona przed exploitami, Silnik korygujący, Kontrola aplikacji.

   Jeśli Twoja organizacja ma wdrożone rozwiązanie Kaspersky Managed Detection and Response (MDR), prześlij plik konfiguracyjny BLOB do zasady Kaspersky Endpoint Security.

3. Usunięcie Kaspersky Security for Windows Server z serwera.

4. Zainstalowanie Kaspersky Endpoint Security for Windows z domyślnym zestawem komponentów.

   Jeśli Twoja organizacja ma wdrożone rozwiązania Detection and Response, wybierz odpowiednie komponenty we właściwościach pakietu instalacyjnego.

5. Sprawdzenie ustawień aplikacji:

   - Aplikacja została aktywowana kluczem licencyjnym KSWS.
   - Została zastosowana nowa zasada. Wcześniej wybrane komponenty zostały wyłączone.

6. Upewnienie się, że serwer działa. Upewnienie się, że Kaspersky Endpoint Security for Windows nie zużywa więcej niż 1% zasobów serwera.

7. Jeśli to konieczne, utworzenie wykluczeń ze skanowania, dodanie zaufanych aplikacji, utworzenie listy zaufanych adresów internetowych.

8. Włączenie komponentów Wykrywanie zachowań, Ochrona przed exploitami, Silnik korygujący. Upewnienie się, że Kaspersky Endpoint Security for Windows nie zużywa więcej niż 1% zasobów serwera.

9. Włączenie komponentu Ochrona sieci. Upewnienie się, że Kaspersky Endpoint Security for Windows nie zużywa więcej niż 2% zasobów serwera.

10. Włączenie komponentu Kontrola aplikacji w trybie testowania reguł.

11. Upewnienie się, że Kontrola aplikacji działa. Jeśli to konieczne, dodanie nowych reguł Kontroli aplikacji i wyłączenie tryb testowania reguł po potwierdzeniu, że Kontrola aplikacji działa.

Upewnij się, że aplikacja po migracji z KSWS do KES działa poprawnie. Sprawdź stan serwera w konsoli (powinien być *OK*). Upewnij się, że aplikacja nie zgłasza błędów. Sprawdź również czas ostatniego połączenia z Serwerem administracyjnym, czas ostatniej aktualizacji bazy danych oraz stan ochrony serwera.

Zarządzanie aplikacją na serwerze w trybie Server Core

Serwer w trybie Server Core nie ma interfejsu. Dlatego też możesz zarządzać aplikacją tylko zdalnie z poziomu konsoli Kaspersky Security Center lub lokalnie z poziomu wiersza polecenia.

Zarządzanie aplikacją z poziomu konsoli Kaspersky Security Center

Instalowanie aplikacji z użyciem konsoli Kaspersky Security Center jest inne od instalowania w sposób normalny. Podczas tworzenia pakietu instalacyjnego możesz dodać klucz licencyjny do aktywowania aplikacji. Możesz użyć klucza Kaspersky Endpoint Security for Windows lub klucza Kaspersky Security for Windows Server.

> Na serwerze w trybie Server Core nie są dostępne następujące składniki aplikacji: Ochrona WWW, Ochrona poczty, Kontrola sieci, Ochrona przed atakami BadUSB, Szyfrowanie plików (FLE), Kaspersky Disk Encryption (FDE).

Ponowne uruchomienie nie jest wymagane podczas instalowania Kaspersky Endpoint Security. Ponowne uruchomienie jest wymagane tylko wtedy, gdy przed instalacją musisz usunąć niekompatybilne aplikacje. Ponowne uruchomienie może być też wymagane podczas aktualizowania wersji aplikacji. Aplikacja nie może wyświetlić okna z pytaniem użytkownika o ponowne uruchomienie serwera. Więcej informacji o potrzebie ponownego uruchomienia serwera znajdziesz w raportach, w konsoli Kaspersky Security Center.

Zarządzanie aplikacją na serwerze w trybie Server Core nie różni się od zarządzania komputerem. Możesz używać zasad i zadań do skonfigurowania aplikacji.

Zarządzanie aplikacją na serwerach w trybie Server Core obejmuje następujące specjalne kwestie:

- Serwer w trybie Server Core nie ma interfejsu, dlatego Kaspersky Endpoint Security nie wyświetla ostrzeżenia informującego użytkownika o potrzebie zaawansowanego leczenia. Aby wyleczyć zagrożenie, musisz włączyć technologię zaawansowanego leczenia w ustawieniach aplikacji oraz natychmiast włączyć Zaawansowane leczenie w ustawieniach zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Następnie musisz uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Szyfrowanie dysków funkcją BitLocker jest dostępne tylko z Trusted Platform Module (TPM). Kod PIN / hasło nie może zostać użyte do zaszyfrowania, ponieważ aplikacja nie może wyświetlić okna z pytaniem o hasło do autoryzacji przed rozruchem. Jeśli w systemie operacyjnym jest włączony tryb kompatybilności z metodą szyfrowania weryfikowanych standardem FIPS (Federal Information Processing Standard), podłącz dysk przenośny do zapisania klucza szyfrowania przed rozpoczęciem szyfrowania dysku.

Zarządzanie aplikacją z poziomu wiersza poleceń

Jeśli nie możesz użyć interfejsu, możesz zarządzać Kaspersky Endpoint Security z poziomu wiersza poleceń.

W celu zainstalowania aplikacji na serwerze w trybie Server Core uruchom następujące polecenie:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

W celu aktywowania aplikacji uruchom następujące polecenie:

```
avp.com license /add <activation code or key file>
```

W celu sprawdzenia stanów profilu uruchom następujący polecenia:

```
avp.com status
```

W celu przejrzenia listy poleceń zarządzających aplikacjami uruchom następujące polecenie:

```
avp.com help
```

Migracja konfiguracji [KSWS+KEA] do konfiguracji [KES+built-in agent]

Podczas migracji z Kaspersky Security for Windows Server (KSWS) do Kaspersky Endpoint Security (KES) możesz skorzystać z poniższych zaleceń, aby skonfigurować ochronę serwera i zoptymalizować wydajność. W tym miejscu przyjrzymy się przykładowi migracji dla pojedynczej organizacji.

Infrastruktura organizacji

Firma ma zainstalowane następujące urządzenia:

- Kaspersky Security Center 14.2

  Administrator zarządza rozwiązaniami firmy Kaspersky przy użyciu Konsoli administracyjnej (MMC). Wdrożono również rozwiązanie Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)

  W Kaspersky Security Center zostały utworzone trzy grupy administracyjne zawierające serwery organizacji: dwie grupy administracyjne dla serwerów SQL oraz grupa administracyjna dla serwerów Microsoft Exchange. Każda grupa administracyjna jest zarządzana przez własną zasadę. Zadania *Database Update* oraz *On-demand scan* zostały utworzone dla wszystkich serwerów w organizacji.

  Klucz aktywacyjny KSWS został dodany do Kaspersky Security Center. Automatyczna dystrybucja klucza została włączona.

- Serwery SQL z zainstalowanym Kaspersky Security for Windows Server 11.0.1 i Kaspersky Endpoint Agent 3.11. Serwery SQL są połączone w dwa klastry.

  KSWS jest zarządzany przez zasady *SQL_Policy(1)* oraz *SQL_Policy(2)*. Zostały również utworzone zadania *Database Update*, *On-demand scan*.

- Serwer Microsoft Exchange z zainstalowanym Kaspersky Security for Windows Server 11.0.1 i Kaspersky Endpoint Agent 3.11.

  KSWS jest zarządzany przez zasadę *Exchange_Policy*. Zostały również utworzone zadania *Database Update*, *On-demand scan*.

Planowanie migracji

Migracja obejmuje następujące etapy:

1. Migracja zadań i zasad KSWS za pomocą Kreatora konwersji zasad i zadań.
2. Migracja zasady Kaspersky Endpoint Agent przy użyciu Kreatora konwersji zasad i zadań.
3. Używanie znaczników do aktywowania profili zasad we właściwościach nowej zasady.
4. Instalowanie KES zamiast KSWS
5. Aktywacja EDR Optimum.
6. Potwierdzenie, że KES działa.

Scenariusz migracji jest początkowo wykonywany na jednym z klastrów serwerów SQL. Następnie scenariusz migracji jest wykonywany na drugim klastrze serwerów SQL. Następnie scenariusz migracji jest wykonywany na Microsoft Exchange.

Migracja zadań i zasad KSWS przy pomocy Kreatora konwersji zasad i zadań.

Aby przeprowadzić migrację zadań KSWS, możesz użyć Kreatora konwersji zasad i zadań (kreatora migracji). W efekcie zamiast zasad *SQL_Policy(1)*, *SQL_Policy(2)* oraz *Exchange_Policy*, otrzymasz pojedynczą zasadę z trzema profilami odpowiednio dla serwerów SQL i Microsoft Exchange. Nowy profil zasad z ustawieniami KSWS zostanie nazwany *UpgradedFromKSWS <Nazwa zasady Kaspersky Security for Windows Server>*. We właściwościach profilu kreator migracji automatycznie wybiera znacznik urządzenia `UpgradedFromKSWS` jako kryterium wyzwalania. W ten sposób ustawienia z profilu zasad są automatycznie stosowane do serwerów.

Migracja zasady Kaspersky Endpoint Agent przy użyciu Kreatora konwersji zasad i zadań

Aby przeprowadzić migrację zasad Kaspersky Endpoint Agent, możesz użyć Kreatora konwersji zasad i zadań. Kreator migracji zasad i zadań dla Kaspersky Endpoint Agent jest dostępny tylko w Web Console.

Używanie znaczników do aktywowania profili zasad we właściwościach nowej zasady

Wybierz znacznik urządzenia przypisany wcześniej jako warunek aktywacji profilu. Otwórz właściwości zasad i wybierz *Główne reguły dotyczące aktywacji profilu zasad* jako warunek aktywacji profilu.

Instalowanie KES zamiast KSWS

Przed zainstalowaniem KES należy wyłączyć Ochronę hasłem we właściwościach zasad KSWS.

Instalacja KES obejmuje następujące etapy:

1. Przygotowanie pakietu instalacyjnego. We właściwościach pakietu instalacyjnego wybierz pakiet dystrybucyjny Kaspersky Endpoint Security for Windows 12.0 i wybierz domyślny zestaw komponentów.
2. Utwórz zadanie *Zdalna instalacja aplikacji* dla jednej z grup administracyjnych serwera SQL.
3. Wybranie we właściwościach zadania pakietu instalacyjnego i pliku klucza licencyjnego.
4. Zaczekanie, aż zadanie zakończy się pomyślnie.
5. Powtórzenie instalacji KES dla pozostałych grup administracyjnych.

Kaspersky Security Center automatycznie dodaje znacznik `UpgradedFromKSWS` do nazw komputerów w konsoli po zakończeniu instalacji KES.

Aby sprawdzić instalację KES, możesz użyć *Raportu wdrażania ochrony*. Możesz także sprawdzić stan urządzenia. Aby potwierdzić aktywację aplikacji, możesz użyć *Raportu o użyciu kluczy licencyjnych*.

Aktywacja EDR Optimum

Funkcjonalność EDR Optimum można aktywować przy użyciu autonomicznej licencji Kaspersky Endpoint Detection and Response Optimum Add-on. Musisz potwierdzić, że klucz EDR Optimum został dodany do repozytorium Kaspersky Security Center, a funkcja automatycznej dystrybucji klucza licencyjnego została włączona.

Aby sprawdzić aktywację EDR Optimum, możesz użyć *Raport o stanie składników aplikacji*.

Potwierdzenie, że KES działa

Aby potwierdzić, że KES działa, możesz sprawdzić, czy nie są zgłaszane żadne błędy. Stan urządzenia musi być *OK*. Zadania aktualizacji i skanowania w poszukiwaniu złośliwego oprogramowania zostały pomyślnie zakończone.

Tryb Light Agent do ochrony maszyn wirtualnych

Od wersji 12.8 możesz używać Kaspersky Endpoint Security for Windows jako części rozwiązania Kaspersky Security for Virtualization Light Agent. *Kaspersky Security for Virtualization Light Agent* to zintegrowane rozwiązanie zapewniające kompleksową ochronę maszyn wirtualnych przed różnymi typami zagrożeń bezpieczeństwa informacji oraz atakami sieciowymi i phishingowymi. Aby korzystać z tego rozwiązania, należy zainstalować aplikację w trybie Light Agent.

Instalacja Kaspersky Endpoint Security w trybie Light Agent na maszynach wirtualnych opartych na architekturze ARM nie jest obsługiwana.

Od wersji 6.2 możesz używać Kaspersky Endpoint Security w trybie Light Agent jako części rozwiązania Kaspersky Security for Virtualization Light Agent.

Po uruchomieniu klienta Light Agent nawiązuje on i utrzymuje połączenie z maszyną wirtualną SVM (Secure Virtual Machine). Serwer ochrony jest wdrażany na maszynie SVM. Ten *serwer ochrony* jest komponentem rozwiązania Kaspersky Security for Virtualization Light Agent, który skanuje pliki w poszukiwaniu wirusów i innego złośliwego oprogramowania, aktualizuje bazy danych wirusów i zarządza kluczami licencyjnymi. Light Agent wysyła do maszyny SVM pliki lub ich fragmenty wymagające skanowania. Wyniki skanowania są dostępne dla wszystkich maszyn wirtualnych z zainstalowanym klientem Light Agent (technologia SharedCache). Ta technologia zwiększa wydajność rozwiązania i umożliwia szybszą reakcję na zagrożenia.

Infrastruktura organizacji może zawierać wiele maszyn wirtualnych z zainstalowanym klientem Light Agent i wiele maszyn SVM. Serwer integracji obsługuje interakcję między maszynami wirtualnymi a maszynami SVM. *Serwer integracji* to składnik rozwiązania Kaspersky Security for Virtualization Light Agent, który generuje listę dostępnych maszyn SVM i przesyła te dane do agentów Light Agent, uczestniczy w wykrywaniu maszyn SVM przez agentów Light Agent, chroni połączenie między agentami Light Agent a maszynami SVM oraz pełni inne funkcje.

Specjalne uwagi dotyczące trybu Light Agent

Zarządzanie programem Kaspersky Endpoint Security w trybie standardowym i Light Agent odbywa się przy użyciu zasad i zadań Kaspersky Endpoint Security. W trybie Light Agent niektóre komponenty i funkcje aplikacji są niedostępne.

Aktualizowanie baz danych i modułów aplikacji

Rozwiązanie Kaspersky Endpoint Security w trybie Light Agent wykorzystuje specjalne bazy danych złośliwego oprogramowania, których aplikacja wymaga do działania w ramach rozwiązania Kaspersky Security for Virtualization Light Agent. Kaspersky Endpoint Security pobiera aktualizacje baz danych i modułów aplikacji z serwera ochrony.

Bazy danych i moduły na chronionych maszynach wirtualnych są aktualizowane przy użyciu specjalnego zadania *Aktualizacja baz danych i modułów aplikacji*, w ramach którego źródłem aktualizacji jest określony folder na maszynie SVM. Light Agent automatycznie uruchamia zadanie *Aktualizacja baz danych i modułów aplikacji*. Nie można wybrać innego źródła aktualizacji, skonfigurować harmonogramu zadania ani usunąć zadania.

Serwer ochrony zarządza również procesem wycofywania najnowszej aktualizacji bazy danych złośliwego oprogramowania. Po wycofaniu aktualizacji baz danych i modułów aplikacji na maszynie SVM na chronionej maszynie wirtualnej uruchamiane jest specjalne lokalne zadanie *Aktualizacja baz danych i modułów aplikacji*. To zadanie sprawia, że Light Agent powraca do korzystania z poprzedniego zestawu baz danych złośliwego oprogramowania.

Kaspersky Endpoint Security w trybie Light Agent nie obsługuje zadania *Wycofywanie aktualizacji*.

Aktywacja klienta Light Agent

Aby aktywować aplikację, musisz dodać klucz licencyjny do maszyny SVM, z którą połączony jest klient Light Agent. Nie ma potrzeby osobnej aktywacji aplikacji.

Inne specjalne uwagi dotyczące trybu Light Agent

- Podczas tworzenia zasad dla aplikacji zalecamy wybranie trybu Light Agent. W tym trybie Kreator nowych zasad wyświetla monit z prośbą o skonfigurowanie połączenia SVM. Ustawienia te są wymagane, aby aplikacja mogła działać w trybie Light Agent.
- W trybie Light Agent nie można zainstalować komponentów Szyfrowania danych i Adaptacyjnej kontroli anomalii. Zestaw komponentów zależy również od typu gościnnego systemu operacyjnego: stacja robocza lub serwer.
- Light Agent nie obsługuje integracji z rozwiązaniami Kaspersky Endpoint Detection and Response Expert i Kaspersky Endpoint Detection and Response Expert (cloud).
- Klientem Light Agent można zarządzać za pośrednictwem Konsoli administracyjnej (MMC) i Kaspersky Security Center Web Console. Nie można zarządzać Light Agent w konsoli Kaspersky Security Center Cloud Console.
- Nie można zmieniać zestawu komponentów aplikacji na maszynach wirtualnych VDI.
- Kaspersky Endpoint Security komunikuje się z serwerami KSN poprzez serwer proxy KSN. Bezpośrednia komunikacja z KSN nie jest obsługiwana.
- Tryb chmury Kaspersky Security Network nie jest obsługiwany.
- Używanie serwera proxy aplikacji podczas łączenia się z serwerem integracyjnym (VIIS), serwerem ochrony (SVM) i serwerami KSN.

Wstępna konfiguracja maszyny wirtualnej

Kaspersky Endpoint Security można zainstalować na maszynie wirtualnej wykorzystującej technologię platformy wirtualnej. Kaspersky Endpoint Security obsługuje platformy wirtualne VMware, Microsoft Hyper-V, Citrix. Przed instalacją należy wykonać wstępną konfigurację maszyn wirtualnych.

Zgodność z technologią Citrix App Layering

Jeśli zamierzasz użyć Full User Layer, aby zapisać stan tymczasowych maszyn wirtualnych, przed przystąpieniem do instalacji na szablonie maszyny wirtualnej należy wykonać następujące czynności:

1. Utwórz plik C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt i dodaj do niego następujące wykluczenia:

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. W rejestrze systemu operacyjnego, w kluczu HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr, utwórz nową wartość DWORD o nazwie MiniFilterBypass i ustaw ją na 1.

3. W rejestrze systemu operacyjnego, w kluczu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd, utwórz nową wartość MULTI_SZ o nazwie ExcludeKey i ustaw ją na \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. Uruchom ponownie maszynę wirtualną.

W przypadku instalacji na maszynach wirtualnych w infrastrukturze korzystającej z funkcji Citrix App Layering należy wykonać następujące czynności:

1. Zainstaluj agenta administracyjnego Kaspersky Security Center i Kaspersky Endpoint Security for Windows na szablonie maszyny wirtualnej w warstwie aplikacji.

2. Utwórz obraz maszyny wirtualnej składający się z wielu warstw.

3. Wdróż utworzony obraz na hiperwizorach obsługujących rozwiązanie Citrix App Layering.

4. Skonfiguruj tworzenie tymczasowych maszyn wirtualnych z utworzonego obrazu.

Aby uzyskać szczegółowe informacje na temat instalacji oprogramowania antywirusowego wraz z funkcją Citrix App Layering, zapoznaj się z dokumentem Dokumentacja Citrix App Layering.

Zgodność z technologią Citrix Provisioning (Citrix Provisioning Services)

Aby mieć pewność, że aplikacja jest zgodna z technologią Citrix Provisioning (Citrix Provisioning Services):

- Jeśli na maszynie wirtualnej zainstalowane jest oprogramowanie Citrix Provisioning Target Device, przed zainstalowaniem aplikacji Kaspersky Endpoint Security należy je usunąć (szczegółowe informacje można znaleźć na stronie wsparcia technicznego Citrix). Po zainstalowaniu aplikacji należy przeinstalować Citrix Provisioning Target Device.
- Podczas instalowania aplikacji korzystającej z kreatora instalacji lub zdalnie za pomocą Kaspersky Security Center, musisz zaznaczyć pole wyboru **Zapewnij zgodność z Citrix PVS**.

Zgodność z technologią Omnissa App Volumes

Przed przystąpieniem do instalacji na szablonie maszyny wirtualnej należy utworzyć plik %SVAgent%\Config\Custom\snapvol.cfg i dodać do niego następujące wykluczenia:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`

- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

Więcej informacji znajdziesz w dokumentacji Omnissa.

Instalowanie klienta Light Agent

Instalacja Kaspersky Endpoint Security w trybie Light Agent na maszynach wirtualnych opartych na architekturze ARM nie jest obsługiwana.

Instalacja aplikacji w trybie Light Agent przebiega tak samo jak w trybie standardowym. Przed zainstalowaniem Light Agent na maszynie wirtualnej należy upewnić się, że zainstalowany jest klient Kaspersky Security Center Network Agent. *Agent sieciowy* upraszcza interakcję Serwera administracyjnego z maszyną wirtualną.

Klienta Light Agent można zainstalować na komputerze stosując jeden z poniższych sposobów:

- Zdalnie, przy użyciu Kaspersky Security Center.
- Lokalnie, przy pomocy Kreatora Setup.
- Lokalnie, przy użyciu wiersza poleceń.

Aby zainstalować Light Agent, należy wybrać odpowiednią konfigurację w ustawienia pakietu instalacyjnego lub w Kreatorze Setup.

Podczas instalacji Light Agent na serwerze zaawansowane komponenty ochrony (Wykrywanie zachowań, Ochrona przed exploitami, Silnik korygujący) są wyłączone z domyślnej konfiguracji aplikacji. Domyślne ustawienia aplikacji zapewniają zalecany poziom ochrony i optymalne wykorzystanie zasobów serwera. Podczas instalacji Light Agent na stacji roboczej w domyślnej konfiguracji aplikacji uwzględniane są zaawansowane komponenty ochronne.

Podczas instalacji klienta Light Agent zalecamy wybranie wykluczeń i zaufanych aplikacji wstępnie zdefiniowanych dla danego środowiska wirtualnego. Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają w szybkiej konfiguracji aplikacji i uniknięciu problemów ze zgodnością środowiska wirtualnego. Można także skonfigurować wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje w zasadach po instalacji.

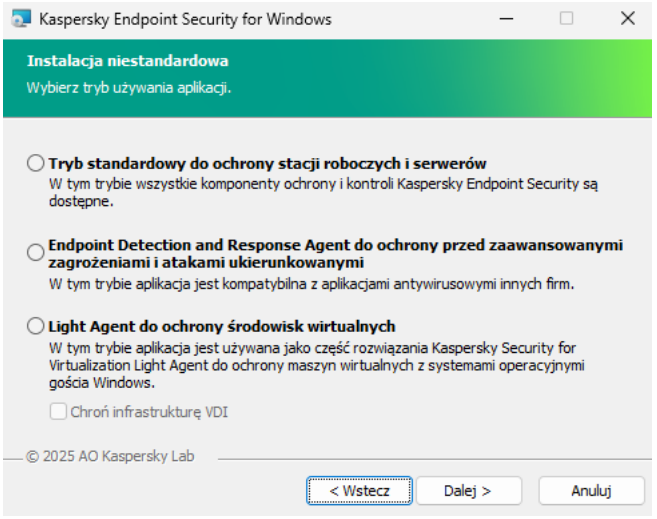
Podczas instalowania klienta Light Agent na trwałych maszynach wirtualnych może być konieczna zmiana algorytmu generowania identyfikatora Sensor ID. Identyfikator Sensor ID jest wykorzystywana w rozwiązaniu Kaspersky Anti Targeted Attack Platform do identyfikowania komputerów wysyłających dane telemetryczne na serwer. Aby utworzyć unikalny identyfikator Sensor ID, wybierz ustawienie `EnableUniqueSensorID=1` podczas instalacji aplikacji za pomocą wiersza poleceń.

Instalacja Light Agent przy pomocy Kreatora Setup.

1. Skopiuj folder pakietu dystrybucyjnego na maszynę wirtualną.
2. Uruchom setup_kes.exe.

Zostanie uruchomiony Kreator instalacji.

Konfiguracja Kaspersky Endpoint Security



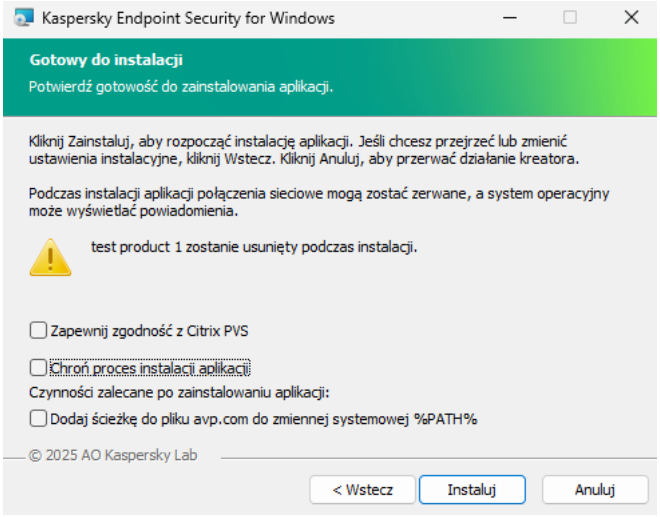
Wybór konfiguracji aplikacji

Wybierz konfigurację **Light Agent do ochrony środowisk wirtualnych**. Ta konfiguracja jest przeznaczona do aplikacji stanowiącej część rozwiązania Kaspersky Security for Virtualization Light Agent. Klienta Light Agent należy zainstalować na każdej maszynie wirtualnej, która ma być chroniona za pomocą tego rozwiązania. W tej konfiguracji nie można używać komponentów Szyfrowania danych ani Adaptacyjnej kontroli anomalii. Jeśli instalujesz klienta Light Agent na szablonie maszyny wirtualnej, który będzie używany do tworzenia *nietrwałych maszyn wirtualnych*, zaznacz pole **Chroń infrastrukturę VDI** (VDI oznacza Virtual Desktop Infrastructure). Tryb ochrony VDI pomaga zoptymalizować działanie Kaspersky Endpoint Security na nietrwałych maszynach wirtualnych. W tym trybie Light Agent odrzuca aktualizacje aplikacji wymagające ponownego uruchomienia maszyny wirtualnej. Po otrzymaniu aktualizacji aplikacji wymagających ponownego uruchomienia Light Agent generuje zdarzenie informujące o konieczności zaktualizowania szablonu chronionych maszyn wirtualnych.

Komponenty Kaspersky Endpoint Security

Wybierz komponenty, które chcesz zainstalować (patrz rysunek poniżej). Możesz zmienić dostępne komponenty aplikacji po zainstalowaniu aplikacji. Aby to zrobić, musisz ponownie uruchomić Kreatora instalacji i wybrać zmianę dostępnych składników.

Ustawienia zaawansowane



Zaawansowane ustawienia instalacji aplikacji

Chroń proces instalacji aplikacji. Ochrona instalacji obejmuje ochronę przed zastąpieniem pakietu dystrybucyjnego szkodliwymi aplikacjami, blokowaniem dostępu do folderu instalacyjnego Kaspersky Endpoint Security, a także blokowaniem dostępu do sekcji rejestru systemu zawierającego klucze aplikacji. Jeżeli aplikacja nie może zostać zainstalowana (na przykład podczas zdalnej instalacji przy użyciu Windows Remote Desktop), zalecane jest wyłączenie ochrony procesu instalacji.

Zapewnij zgodność z Citrix PVS. Możesz włączyć obsługę Citrix Provisioning Services, aby zainstalować Kaspersky Endpoint Security na maszynie wirtualnej.

Dodaj ścieżkę do pliku avp.com do zmiennej systemowej %PATH%. Możesz dodać ścieżkę instalacji do zmiennej %PATH% dla wygodnego korzystania z interfejsu wiersza poleceń.

Instalacja Light Agent przy pomocy wiersza poleceń

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się pakiet dystrybucyjny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
```

LUB

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
```

Opcja `VDI` włącza tryb ochrony VDI (Virtual Desktop Infrastructure). Tryb ochrony VDI pomaga zoptymalizować działanie Kaspersky Endpoint Security na nietrwałych maszynach wirtualnych. W tym trybie Light Agent odrzuca aktualizacje aplikacji wymagające ponownego uruchomienia maszyny wirtualnej. Po otrzymaniu aktualizacji aplikacji wymagających ponownego uruchomienia Light Agent generuje zdarzenie informujące o konieczności zaktualizowania szablonu chronionych maszyn wirtualnych. Domyślnie, tryb ochrony VDI jest wyłączony.

W rezultacie klient Light Agent jest instalowany na maszynie wirtualnej z domyślnym zestawem komponentów. Możesz edytować zestaw komponentów i określić zaawansowane ustawienia za pomocą pliku setup.ini. Możesz także określić ustawienia instalacji w wierszu poleceń.

Instalacja Light Agent przy pomocy Konsoli administracyjnej (MMC)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz folder **Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

   Spowoduje to otwarcie listy pakietów instalacyjnych, które zostały pobrane do Kaspersky Security Center.
3. Otwórz właściwości pakietu instalacyjnego Kaspersky Endpoint Security for Windows.

   Jeśli to konieczne, utwórz nowy pakiet instalacyjny.
4. Przejdź do sekcji **Ustawienia**.
5. Wybierz konfigurację **Klient Light Agent do ochrony środowisk wirtualnych**. Ta konfiguracja jest przeznaczona do aplikacji stanowiącej część rozwiązania Kaspersky Security for Virtualization Light Agent. Klienta Light Agent należy zainstalować na każdej maszynie wirtualnej, która ma być chroniona za pomocą tego rozwiązania. W tej konfiguracji nie można używać komponentów Szyfrowania danych ani Adaptacyjnej kontroli anomalii. Jeśli instalujesz klienta Light Agent na szablonie maszyny wirtualnej, który będzie używany do tworzenia *nietrwałych maszyn wirtualnych*, zaznacz pole **Chroń infrastrukturę VDI** (VDI oznacza Virtual Desktop Infrastructure). Tryb ochrony VDI pomaga zoptymalizować działanie Kaspersky Endpoint Security na nietrwałych maszynach wirtualnych. W tym trybie Light Agent odrzuca aktualizacje aplikacji wymagające ponownego uruchomienia maszyny wirtualnej. Po otrzymaniu aktualizacji aplikacji wymagających ponownego uruchomienia Light Agent generuje zdarzenie informujące o konieczności zaktualizowania szablonu chronionych maszyn wirtualnych.
6. Wybierz składniki, które chcesz zainstalować.

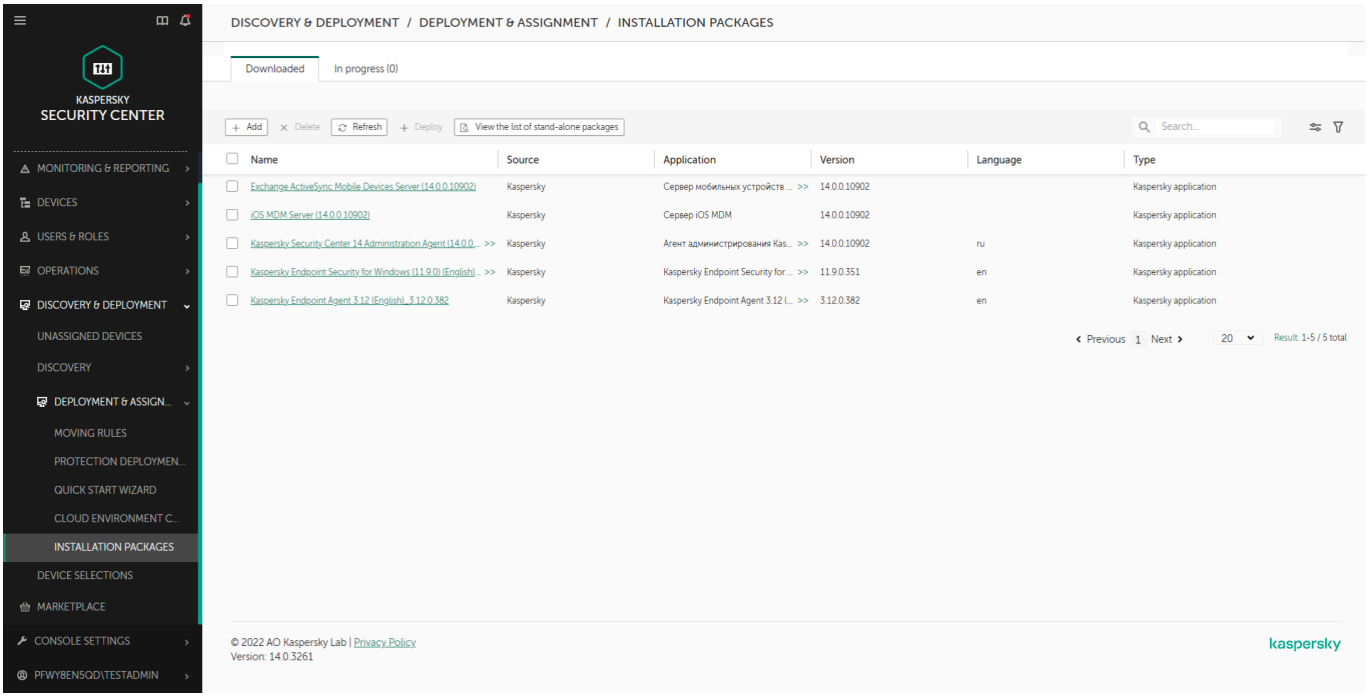
   Możesz zmienić dostępne komponenty aplikacji po zainstalowaniu aplikacji.
7. Skonfiguruj strefę zaufaną. Wybierz wstępnie zdefiniowane wykluczenia skanowania i zaufane aplikacje dla środowiska wirtualnego, w którym instalujesz aplikację.

   Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają w szybkiej konfiguracji aplikacji i uniknięciu problemów ze zgodnością środowiska wirtualnego.
8. Zapisz swoje zmiany.
9. Utwórz zadanie zdalnej instalacji. We właściwościach zadania wybierz utworzony pakiet instalacyjny.

Instalacja Light Agent przy użyciu Web Console

1. W oknie głównym Web Console wybierz **Wykrywanie i wdrażanie → Wdrażanie i przypisywanie → Pakiety instalacyjne**.

Spowoduje to otwarcie listy pakietów instalacyjnych, które zostały pobrane do Kaspersky Security Center.



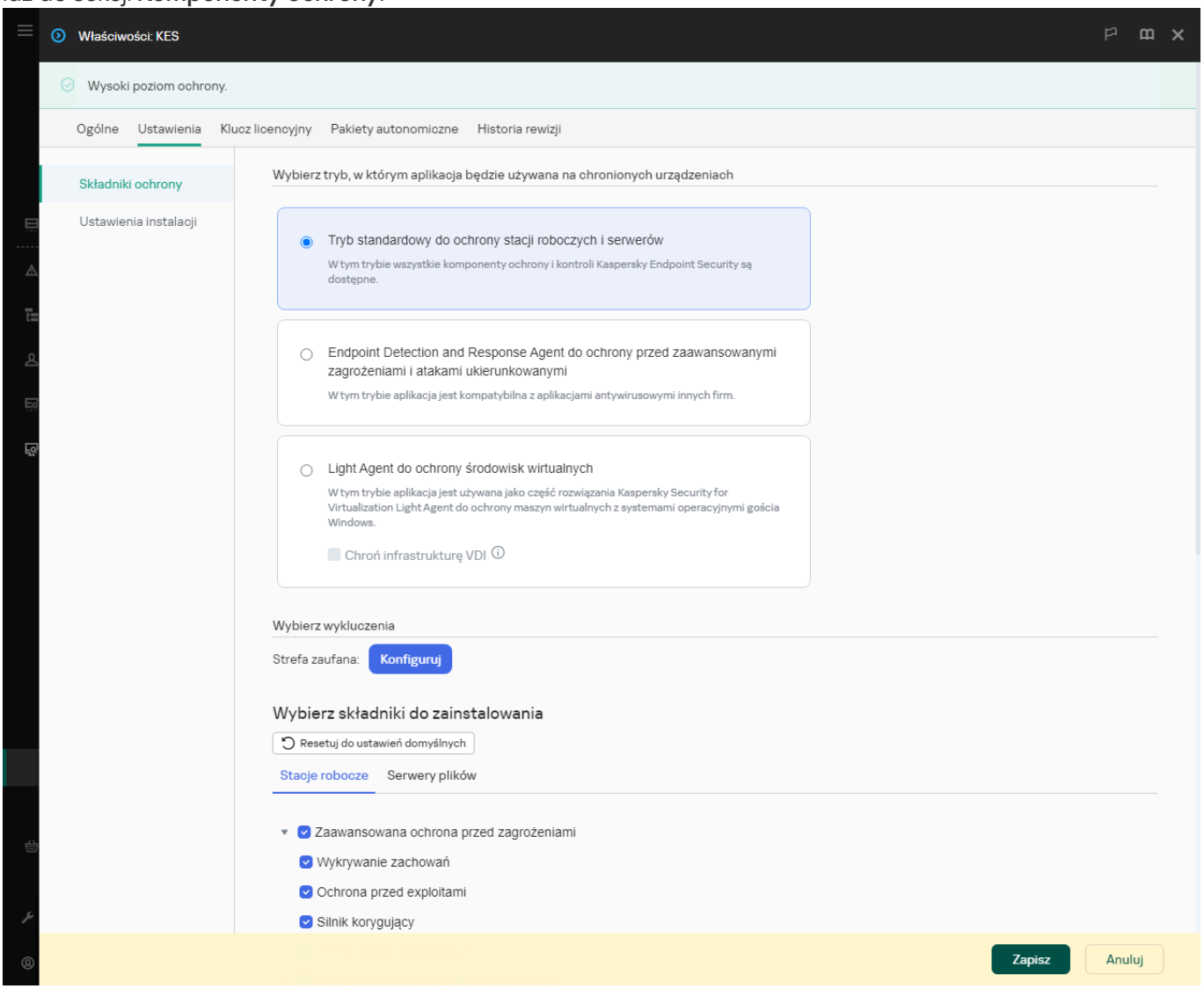
Lista pakietów instalacyjnych

2. Otwórz właściwości pakietu instalacyjnego Kaspersky Endpoint Security for Windows.

   Jeśli to konieczne, utwórz nowy pakiet instalacyjny.

3. Wybierz zakładkę **Ustawienia**.

4. Idź do sekcji **Komponenty ochrony**.



Komponenty zawarte w pakiecie instalacyjnym

5. Wybierz konfigurację **Light Agent do ochrony środowisk wirtualnych**. Ta konfiguracja jest przeznaczona do aplikacji stanowiącej część rozwiązania Kaspersky Security for Virtualization Light Agent. Klienta Light Agent należy zainstalować na każdej maszynie wirtualnej, która ma być chroniona za pomocą tego rozwiązania. W tej konfiguracji nie można używać komponentów Szyfrowania danych ani Adaptacyjnej kontroli anomalii. Jeśli instalujesz klienta Light Agent na szablonie maszyny wirtualnej, który będzie używany do tworzenia *nietrwałych maszyn wirtualnych*, zaznacz pole **Chroń infrastrukturę VDI** (VDI oznacza Virtual Desktop Infrastructure). Tryb ochrony VDI pomaga zoptymalizować działanie Kaspersky Endpoint Security na nietrwałych maszynach wirtualnych. W tym trybie Light Agent odrzuca aktualizacje aplikacji wymagające ponownego uruchomienia maszyny wirtualnej. Po otrzymaniu aktualizacji aplikacji wymagających ponownego uruchomienia Light Agent generuje zdarzenie informujące o konieczności zaktualizowania szablonu chronionych maszyn wirtualnych.

6. Wybierz składniki, które chcesz zainstalować.

   Możesz zmienić dostępne komponenty aplikacji po zainstalowaniu aplikacji.

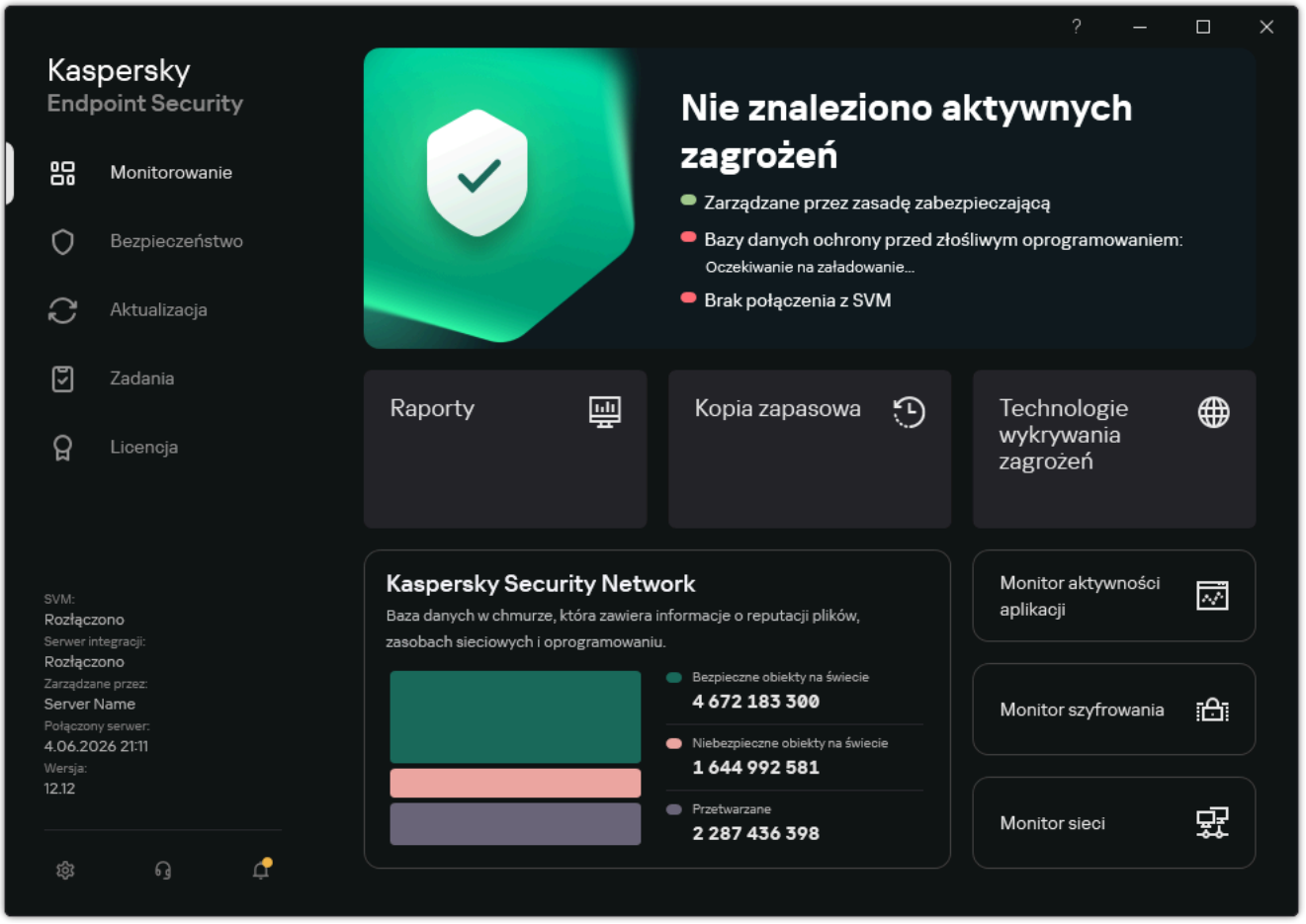
7. Skonfiguruj strefę zaufaną. Wybierz wstępnie zdefiniowane wykluczenia skanowania i zaufane aplikacje dla środowiska wirtualnego, w którym instalujesz aplikację.

   Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają w szybkiej konfiguracji aplikacji i uniknięciu problemów ze zgodnością środowiska wirtualnego.

8. Zapisz swoje zmiany.

9. Utwórz zadanie zdalnej instalacji. We właściwościach zadania wybierz utworzony pakiet instalacyjny.

W rezultacie klient Light Agent jest instalowany na maszynie wirtualnej. Możesz skorzystać z interfejsu aplikacji, a w obszarze powiadomień wyświetlana jest ikona aplikacji . Teraz trzeba skonfigurować połączenie klienta Light Agenta z maszyną SVM.



Główne okno klienta Light Agent

Łączenie klienta Light Agent z maszyną SVM

Rozwiązanie Kaspersky Security for Virtualization Light Agent wymaga ciągłej komunikacji pomiędzy klientem Light Agentem a maszyną SVM. Pliki wysyłane przez klienta Light Agent muszą być skanowane w poszukiwaniu wirusów i innego złośliwego oprogramowania. Klient Light Agent nie może wysyłać plików do skanowania, jeśli maszyna SVM nie jest połączona. Jeśli przez ponad pięć minut nie można nawiązać połączenia, skanowanie kończy się błędem.

Połączenie klienta Light Agent z maszyną SVM przebiega w następujący sposób:

1. Light Agent otrzymuje listę dostępnych maszyn SVM.
2. Light Agent ustala dostępny serwer ochrony (SVM), który jest optymalny do nawiązania połączenia według algorytmu wyboru SVM.
3. Light Agent sprawdza dodatkowe ustawienia połączenia maszyny SVM: znaczniki, stan ochrony połączenia, funkcje aplikacji objęte licencją.
4. Łączenie klienta Light Agent z maszyną SVM.

Informacje o stanie połączenia klienta Light Agent z maszyną SVM można uzyskać w programie Kaspersky Endpoint Security lub za pomocą polecenia w aplikacji. Aplikacja generuje zdarzenie za każdym razem, gdy połączenie klienta Light Agent z maszyną SVM zostanie utracone lub nawiązane, a następnie wysyła je do Kaspersky Security Center. Jeśli do wykrywania maszyn SVM używasz serwera integracyjnego, możesz uzyskać informacje o stanie maszyny SVM i liczbie połączonych klientów Light Agent w konsoli serwera integracyjnego. Szczegółowe informacje na temat monitorowania stanu maszyny SVM można znaleźć w artykule Pomoc dotycząca Kaspersky Security for Virtualization Light Agent.

Wykrywanie maszyn SVM

Możesz wybrać jedną z metod wykrywania SVM dla klienta Light Agent:

- Korzystanie z serwera integracyjnego (VIIS).

  Serwer integracji to komponent rozwiązania, który umożliwia współdziałanie Kaspersky Security for Virtualization Light Agent z infrastrukturą wirtualną i generuje listę maszyn SVM dostępnych do nawiązania połączenia. Light Agent nawiązuje połączenie z serwerem integracyjnym i pobiera listę adresów SVM.

  Serwer integracji jest najbardziej przydatny w dużych infrastrukturach wirtualnych, ponieważ automatycznie równoważy obciążenie między maszynami SVM, pobiera informacje o dostępnych maszynach SVM, analizuje te informacje i udostępnia agentom Light Agent listę Serwerów ochrony (SVM) optymalnych do nawiązania połączenia.

  Aby klient Light Agent mógł uzyskać listę maszyn SVM, wystarczy wprowadzić adres serwera integracyjnego.

- Korzystanie z listy adresów SVM.

  Jeśli chcesz określić poszczególne maszyny SVM, z którymi klient Light Agent ma się łączyć, możesz przygotować listę ręcznie.

  Należy podać adresy dostępnych maszyn SVM, z którymi Light Agent może się połączyć.

Jak skonfigurować wykrywanie maszyn SVM przez klienta Light Agent w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Tryb Light Agent** → **Ustawienia wykrywania SVM**.
4. Wybierz metodę wykrywania maszyn SVM.
   - **Użyj serwera integracji**. Wprowadź ustawienia połączenia z serwerem integracyjnym. Wprowadź adres IP w formacie IPv4 lub pełną nazwę domeny (FQDN) urządzenia, na którym zainstalowany jest serwer integracyjny.
   - **Użyj niestandardowej listy adresów SVM**. Utwórz listę maszyn SVM, z którymi Light Agent może się połączyć. Wprowadź adres IP w formacie IPv4 lub pełną nazwę domeny (FQDN) maszyny SVM. Każdy element listy musi być wpisany w nowym wierszu lub oddzielony od poprzedniego elementu średnikiem (`;`).

     Na liście adresów SVM należy podawać tylko pełne nazwy domen (FQDN), które odpowiadają pojedynczemu adresowi IP. Użycie pełnej nazwy domeny odpowiadającej wielu adresom IP może powodować błędy w rozwiązaniu.
5. Zapisz swoje zmiany.

Jak skonfigurować wykrywanie maszyn SVM przez klienta Light Agent w Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Tryb Light Agent** → **Ustawienia wykrywania SVM**.
5. Wybierz metodę wykrywania maszyn SVM.

   - **Użyj serwera integracji**. Wprowadź ustawienia połączenia z serwerem integracyjnym. Wprowadź adres IP w formacie IPv4 lub pełną nazwę domeny (FQDN) urządzenia, na którym zainstalowany jest serwer integracyjny.
   - **Użyj niestandardowej listy adresów SVM**. Utwórz listę maszyn SVM, z którymi Light Agent może się połączyć. Wprowadź adres IP w formacie IPv4 lub pełną nazwę domeny (FQDN) maszyny SVM. Każdy element listy musi być wpisany w nowym wierszu lub oddzielony od poprzedniego elementu średnikiem (`;`).

     Na liście adresów SVM należy podawać tylko pełne nazwy domen (FQDN), które odpowiadają pojedynczemu adresowi IP. Użycie pełnej nazwy domeny odpowiadającej wielu adresom IP może powodować błędy w rozwiązaniu.
6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak skonfigurować wykrywanie maszyn SVM przez klienta Light Agent w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji kliknij kafelek **Ustawienia wykrywania SVM** w obszarze **Tryb Light Agent**.
3. Wybierz metodę wykrywania maszyn SVM.

   - **Użyj serwera integracji**. Wprowadź ustawienia połączenia z serwerem integracyjnym. Wprowadź adres IP w formacie IPv4 lub pełną nazwę domeny (FQDN) urządzenia, na którym zainstalowany jest serwer integracyjny.
   - **Użyj niestandardowej listy adresów SVM**. Utwórz listę maszyn SVM, z którymi Light Agent może się połączyć. Wprowadź adres IP w formacie IPv4 lub pełną nazwę domeny (FQDN) maszyny SVM. Każdy element listy musi być wpisany w nowym wierszu lub oddzielony od poprzedniego elementu średnikiem (`;`).

     Na liście adresów SVM należy podawać tylko pełne nazwy domen (FQDN), które odpowiadają pojedynczemu adresowi IP. Użycie pełnej nazwy domeny odpowiadającej wielu adresom IP może powodować błędy w rozwiązaniu.
4. Zapisz swoje zmiany.

Konfigurowanie algorytmu wyboru SVM na potrzeby klienta Light Agent

Infrastruktura organizacji może mieć wiele wdrożonych maszyn SVM, z którymi klienty Light Agent mogą się łączyć. Aby zrównoważyć obciążenie sieci i zasobów infrastruktury wirtualnej, należy rozdzielić klienty Light Agent między maszyny SVM.

Klienty Light Agent mogą stosować następujące algorytmy wyboru SVM w celu nawiązania połączenia:

Standardowy algorytm (domyślnie)

Jeśli ten algorytm zostanie zastosowany, po zainstalowaniu i uruchomieniu agent Light Agent na maszynie wirtualnej wybierze do połączenia maszynę SVM, która jest *lokalna* względem Light Agent.

To, czy maszyna SVM jest uznawana za lokalną względem Light Agent, zależy od typu infrastruktury wirtualnej:

- W infrastrukturze wirtualnej opartej na Basis Dynamix Enterprise za lokalną względem Light Agent uznaje się maszynę SVM wdrożoną na tym samym węźle co maszyna wirtualna z zainstalowanym agentem Light Agent.
- W infrastrukturze wirtualnej opartej na Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer lub Basis Dynamix Standard za lokalną względem Light Agent uznaje się maszynę SVM wdrożoną na tym samym hiperwizorze co maszyna wirtualna z zainstalowanym agentem Light Agent.
- W infrastrukturze wirtualnej działającej na platformie OpenStack lub VK Private Cloud można określić sposób ustalania lokalności maszyny SVM względem Light Agent za pomocą parametru `StandardAlgorithmSvmLocality` w sekcji `HypervisorSpecificSettings:Openstack` pliku konfiguracyjnego Serwera integracji appsettings.json. W zależności od wersji Serwera integracji plik znajduje się w jednej z następujących ścieżek:
  - /var/opt/kaspersky/viis/common/ dla Serwera integracji opartego na systemie Linux
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ dla Serwera integracji opartego na systemie Windows

  Parametr `StandardAlgorithmSvmLocality` może przyjmować następujące wartości:

  - `ServerGroup` – jeśli wybrano tę wartość, maszyna SVM jest uznawana za lokalną względem Light Agent, jeśli znajduje się w tej samej grupie serwerów co maszyna wirtualna z zainstalowanym agentem Light Agent. Ta wartość jest używana domyślnie.
  - `Project` – jeśli wybrano tę wartość, maszyna SVM jest uznawana za lokalną względem Light Agent, jeśli jest wdrożona w tym samym projekcie OpenStack co maszyna wirtualna z zainstalowanym agentem Light Agent.
  - `AvailabilityZone` – jeśli wybrano tę wartość, maszyna SVM jest uznawana za lokalną względem Light Agent, jeśli znajduje się w tej samej strefie dostępności co maszyna wirtualna z zainstalowanym agentem Light Agent.

Jeśli nie ma lokalnych maszyn SVM dostępnych do połączenia, agent Light Agent wybiera maszynę SVM z najmniejszą liczbą połączonych agentów Light Agent, niezależnie od ścieżki SVM w infrastrukturze wirtualnej.

Aplikacja nie ustala, czy maszyna SVM jest lokalna względem Light Agent, jeśli dla Serwera ochrony na maszynie SVM włączony jest tryb ochrony dużej infrastruktury. W takim przypadku zaleca się użycie rozszerzonego algorytmu wyboru SVM i wybranie Serwera integracji jako metody wykrywania SVM.

Rozszerzony algorytm

Jeśli ten algorytm zostanie zastosowany, można zdefiniować następujące ustawienia wyboru SVM:

- czy uwzględniać, czy ignorować lokalizację maszyn SVM w infrastrukturze podczas wybierania maszyn SVM do połączenia
- jeśli lokalizacja maszyn SVM jest uwzględniana, metoda ustalania lokalności maszyny SVM względem Light Agent

Jeśli klienty Light Agent ignorują lokalizację maszyn SVM w infrastrukturze, będą mogły łączyć się z dowolnymi maszynami SVM dostępnymi do połączenia.

Jeśli klienty Light Agent muszą uwzględniać lokalizację maszyn SVM w infrastrukturze, należy wybrać typ ścieżki SVM, który będzie brany pod uwagę podczas ustalania lokalności maszyny SVM względem Light Agent. To, czy maszyna SVM jest uznawana za lokalną względem Light Agent, zależy od typu infrastruktury wirtualnej.

W infrastrukturze wirtualnej opartej na Basis Dynamix Enterprise maszynę SVM można uznać za lokalną względem Light Agent w dowolnym z następujących przypadków:

- Maszyna SVM jest wdrożona na tym samym węźle co maszyna wirtualna z zainstalowanym agentem Light Agent.
- Maszyna SVM jest wdrożona w tej samej strefie co maszyna wirtualna z zainstalowanym agentem Light Agent.
- Maszyna SVM jest wdrożona w tym samym centrum danych co maszyna wirtualna z zainstalowanym agentem Light Agent.

W infrastrukturze wirtualnej opartej na Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer lub Basis Dynamix Standard maszynę SVM można uznać za lokalną względem Light Agent w dowolnym z następujących przypadków:

- Maszyna SVM jest wdrożona na tym samym hiperwizorze co maszyna wirtualna z zainstalowanym agentem Light Agent.
- Maszyna SVM jest wdrożona w tym samym klastrze hiperwizorów co maszyna wirtualna z zainstalowanym agentem Light Agent.
- Maszyna SVM jest wdrożona w tym samym centrum danych co maszyna wirtualna z zainstalowanym agentem Light Agent.

W infrastrukturze wirtualnej działającej na platformie OpenStack lub VK Private Cloud maszynę SVM można uznać za lokalną względem Light Agent w dowolnym z następujących przypadków:

- Maszyna SVM znajduje się w tej samej grupie serwerów co maszyna wirtualna z zainstalowanym agentem Light Agent.
- Maszyna SVM jest wdrożona w tym samym projekcie OpenStack co maszyna wirtualna z zainstalowanym agentem Light Agent.
- Maszyna SVM znajduje się w tej samej strefie dostępności co maszyna wirtualna z zainstalowanym agentem Light Agent.

Jeśli klienty Light Agent uwzględniają lokalizację maszyn SVM w infrastrukturze podczas wybierania maszyny SVM do połączenia, mogą łączyć się wyłącznie z lokalnymi maszynami SVM.

Na przykład jeśli jako typ ścieżki SVM zostanie określony klaster hiperwizorów, wszystkie maszyny SVM wdrożone w tym klastrze hiperwizorów będą uznawane za lokalne względem Light Agent, a Light Agent będzie mógł połączyć się tylko z jedną z tych maszyn SVM. Jeśli w tym samym klastrze, w którym działa Light Agent, nie ma maszyn SVM dostępnych do połączenia, Light Agent nie łączy się z maszyną SVM.

Podczas wybierania maszyn SVM klienty Light Agent uwzględniają również liczbę podłączonych klientów Light Agent, aby zapewnić równomierne rozmieszczenie klientów Light Agent między maszynami SVM dostępnymi do połączenia.

Jeśli Light Agent używa rozszerzonego algorytmu wyboru SVM, metoda wykrywania SVM jest ustawiona na listę adresów SVM, a na maszynie SVM włączony jest tryb ochrony dużej infrastruktury, połączenie Light Agent z tą maszyną SVM jest możliwe tylko wtedy, gdy ścieżka SVM jest ignorowana.

Połączenia klientów Light Agent z maszynami SVM można kontrolować także za pomocą znaczników, a nie tylko algorytmów połączenia SVM.

Jak skonfigurować algorytm wyboru SVM na potrzeby klienta Light Agent w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Tryb Light Agent** → **Algorytm wyboru SVM**.
4. Wybierz algorytm:
   - **Użyj standardowego algorytmu wyboru SVM**. Light Agent wybiera maszyny SVM wdrożone w tym samym hipernadzorcy.
   - **Użyj rozszerzonego algorytmu wyboru SVM**. Light Agent wybiera maszyny SVM wdrożone przy użyciu wybranego typu ścieżki maszyny SVM (domyślnie **Hypervisor**).

5. W razie potrzeby wybierz ścieżkę maszyny SVM na potrzeby rozszerzonego algorytmu wyboru SVM:

- **Hypervisor**. Light Agent wybiera do połączenia maszynę SVM spełniającą określone kryteria (zależnie od typu infrastruktury wirtualnej):

  - Maszyny SVM są wdrożone na tym samym hiperwizorze co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej opartej na Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer lub Basis Dynamix Standard).

  - Maszyna SVM znajduje się w tej samej grupie serwerów co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej działającej na platformie OpenStack lub VK Private Cloud).

  - Maszyna SVM znajduje się na tym samym węźle co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej Basis Dynamix Enterprise).

  Jeśli na tym samym hiperwizorze lub w tej samej grupie serwerów, w której znajduje się maszyna wirtualna z agentem Light Agent, nie ma maszyn SVM dostępnych do połączenia, Light Agent nie łączy się z maszyną SVM.

- **Grupa**. Light Agent wybiera do połączenia maszynę SVM, która spełnia kryteria (w zależności od typu infrastruktury wirtualnej):

  - Maszyny SVM są wdrożone w tym samym klastrze hiperwizorów co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej opartej na Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer lub Basis Dynamix Standard).

  - Maszyny SVM są wdrożone w tym samym projekcie OpenStack co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej działającej na platformie OpenStack lub VK Private Cloud).

  - Maszyna SVM znajduje się w tej samej strefie co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej Basis Dynamix Enterprise).

  Jeśli w tym samym klastrze hiperwizorów lub w tym samym projekcie OpenStack, w którym znajduje się maszyna wirtualna z agentem Light Agent, nie ma maszyn SVM dostępnych do połączenia, Light Agent nie łączy się z maszyną SVM.

- **Centrum danych**. Light Agent wybiera do połączenia maszynę SVM, która spełnia kryteria (w zależności od typu infrastruktury wirtualnej):

  - Maszyny SVM są wdrożone w tym samym centrum danych co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej opartej na Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer lub Basis Dynamix Standard).

  - Maszyny SVM znajdują się w tej samej strefie dostępności co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej działającej na platformie OpenStack lub VK Private Cloud).

  - Maszyna SVM znajduje się w tym samym centrum danych co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej Basis Dynamix Enterprise).

Jeśli w tym samym centrum danych lub w tej samej strefie dostępności, w której znajduje się maszyna wirtualna z klientem Light Agent, nie ma maszyn SVM dostępnych do połączenia, Light Agent nie połączy się z maszyną SVM.

- **Ignoruj**. Light Agent ignoruje ścieżkę maszyny SVM podczas łączenia się z serwerem ochrony. Light Agent bierze pod uwagę także inne kryteria: znaczniki, liczbę klientów Light Agent połączonych z maszyną SVM itp.

6. Zapisz swoje zmiany.

Jak skonfigurować algorytm wyboru SVM na potrzeby klienta Light Agent w Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Tryb Light Agent** → **Algorytm wyboru SVM**.
5. Wybierz algorytm:

   - **Użyj standardowego algorytmu wyboru SVM**. Light Agent wybiera maszyny SVM wdrożone w tym samym hipernadzorcy.
   - **Użyj rozszerzonego algorytmu wyboru SVM**. Light Agent wybiera maszyny SVM wdrożone przy użyciu wybranego typu ścieżki maszyny SVM (domyślnie **Hypervisor**).
6. W razie potrzeby wybierz ścieżkę maszyny SVM na potrzeby rozszerzonego algorytmu wyboru SVM:

   - **Hypervisor**. Light Agent wybiera do połączenia maszynę SVM, która spełnia kryteria (w zależności od typu infrastruktury wirtualnej):

     - Maszyny SVM są wdrożone na tym samym hiperwizorze co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej opartej na Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer lub Basis Dynamix Standard).
     - Maszyna SVM znajduje się w tej samej grupie serwerów co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej działającej na platformie OpenStack lub VK Private Cloud).
     - Maszyna SVM znajduje się na tym samym węźle co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej Basis Dynamix Enterprise).

     Jeśli na tym samym hiperwizorze lub w tej samej grupie serwerów, w której znajduje się maszyna wirtualna z agentem Light Agent, nie ma maszyn SVM dostępnych do połączenia, Light Agent nie łączy się z maszyną SVM.

- **Grupa**. Light Agent wybiera do połączenia maszynę SVM, która spełnia kryteria (w zależności od typu infrastruktury wirtualnej):

  - Maszyny SVM są wdrożone w tym samym klastrze hiperwizorów co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej opartej na Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer lub Basis Dynamix Standard).

  - Maszyny SVM są wdrożone w tym samym projekcie OpenStack co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej działającej na platformie OpenStack lub VK Private Cloud).

  - Maszyna SVM znajduje się w tej samej strefie co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej Basis Dynamix Enterprise).

  Jeśli w tym samym klastrze hiperwizorów lub w tym samym projekcie OpenStack, w którym znajduje się maszyna wirtualna z agentem Light Agent, nie ma maszyn SVM dostępnych do połączenia, Light Agent nie łączy się z maszyną SVM.

- **Centrum danych**. Light Agent wybiera do połączenia maszynę SVM, która spełnia kryteria (w zależności od typu infrastruktury wirtualnej):

  - Maszyny SVM są wdrożone w tym samym centrum danych co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej opartej na Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer lub Basis Dynamix Standard).

  - Maszyny SVM znajdują się w tej samej strefie dostępności co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej działającej na platformie OpenStack lub VK Private Cloud).

  - Maszyna SVM znajduje się w tym samym centrum danych co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej Basis Dynamix Enterprise).

  Jeśli w tym samym centrum danych lub w tej samej strefie dostępności, w której znajduje się maszyna wirtualna z klientem Light Agent, nie ma maszyn SVM dostępnych do połączenia, Light Agent nie połączy się z maszyną SVM.

- **Ignoruj**. Light Agent ignoruje ścieżkę maszyny SVM podczas łączenia się z serwerem ochrony. Light Agent bierze pod uwagę także inne kryteria: znaczniki, liczbę klientów Light Agent połączonych z maszyną SVM itp.

7. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak skonfigurować algorytm wyboru SVM na potrzeby klienta Light Agent w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji kliknij kafelek **Ustawienia wykrywania SVM** w obszarze **Tryb Light Agent**.

3. Wybierz algorytm:

   - **Użyj standardowego algorytmu wyboru SVM**. Light Agent wybiera maszyny SVM wdrożone w tym samym hipernadzorcy.

   - **Użyj rozszerzonego algorytmu wyboru SVM**. Light Agent wybiera maszyny SVM wdrożone przy użyciu wybranego typu ścieżki maszyny SVM (domyślnie **Hypervisor**).

4. W razie potrzeby wybierz ścieżkę maszyny SVM na potrzeby rozszerzonego algorytmu wyboru SVM:

- **Hypervisor**. Light Agent wybiera do połączenia maszynę SVM, która spełnia kryteria (w zależności od typu infrastruktury wirtualnej):

  - Maszyny SVM są wdrożone na tym samym hiperwizorze co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej opartej na Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer lub Basis Dynamix Standard).

  - Maszyna SVM znajduje się w tej samej grupie serwerów co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej działającej na platformie OpenStack lub VK Private Cloud).

  - Maszyna SVM znajduje się na tym samym węźle co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej Basis Dynamix Enterprise).

  Jeśli na tym samym hiperwizorze lub w tej samej grupie serwerów, w której znajduje się maszyna wirtualna z agentem Light Agent, nie ma maszyn SVM dostępnych do połączenia, Light Agent nie łączy się z maszyną SVM.

- **Grupa**. Light Agent wybiera do połączenia maszynę SVM, która spełnia kryteria (w zależności od typu infrastruktury wirtualnej):

  - Maszyny SVM są wdrożone w tym samym klastrze hiperwizorów co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej opartej na Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer lub Basis Dynamix Standard).

  - Maszyny SVM są wdrożone w tym samym projekcie OpenStack co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej działającej na platformie OpenStack lub VK Private Cloud).

  - Maszyna SVM znajduje się w tej samej strefie co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej Basis Dynamix Enterprise).

  Jeśli w tym samym klastrze hiperwizorów lub w tym samym projekcie OpenStack, w którym znajduje się maszyna wirtualna z agentem Light Agent, nie ma maszyn SVM dostępnych do połączenia, Light Agent nie łączy się z maszyną SVM.

- **Centrum danych**. Light Agent wybiera do połączenia maszynę SVM, która spełnia kryteria (w zależności od typu infrastruktury wirtualnej):

  - Maszyny SVM są wdrożone w tym samym centrum danych co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej opartej na Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer lub Basis Dynamix Standard).

  - Maszyny SVM znajdują się w tej samej strefie dostępności co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej działającej na platformie OpenStack lub VK Private Cloud).

  - Maszyna SVM znajduje się w tym samym centrum danych co maszyna wirtualna z zainstalowanym agentem Light Agent (w infrastrukturze wirtualnej Basis Dynamix Enterprise).

Jeśli w tym samym centrum danych lub w tej samej strefie dostępności, w której znajduje się maszyna wirtualna z klientem Light Agent, nie ma maszyn SVM dostępnych do połączenia, Light Agent nie połączy się z maszyną SVM.

- **Ignoruj**. Light Agent ignoruje ścieżkę maszyny SVM podczas łączenia się z serwerem ochrony. Light Agent bierze pod uwagę także inne kryteria: znaczniki, liczbę klientów Light Agent połączonych z maszyną SVM itp.

5. Zapisz swoje zmiany.

Dystrybucja połączeń klientów Light Agent z maszynami SVM (znaczniki)

Z maszyną SVM może łączyć się wiele klientów Light Agent. Aby zrównoważyć połączenia klienta Light Agent, możesz określ osobną listę maszyn SVM. Jeśli używasz serwera integracyjnego do wykrywania maszyn SVM, możesz użyć *znaczników*, aby zrównoważyć połączenia klienta Light Agent z maszynami SVM. Oznacza to, że w przypadku klienta Light Agent można przypisać listę maszyn SVM, które mają łączyć się za pomocą znacznika. Aby to zrobić, musisz przypisać znacznik do klienta Light Agent i określić go w ustawieniach maszyny SVM. Szczegółowe informacje na temat określania znaczników w ustawieniach maszyn SVM zawiera artykuł Pomoc dotycząca Kaspersky Security for Virtualization Light Agent.

Przykład: Rozwiązanie Kaspersky Endpoint Detection and Response Optimum jest wdrażane w infrastrukturze na wyznaczonych hostach maszyn wirtualnych. W tym przypadku możesz przypisać znacznik `[EDROptimum]` do klienta Light Agent, aby łączyć go z maszynami SVM, do których dodano klucz licencyjny EDR Optimum (dodatek EDR Optimum). Dzięki temu możesz korzystać z funkcji EDR Optimum na maszynie wirtualnej z klientem Light Agent. Podczas łączenia klienta Light Agent z maszyną SVM bez klucza licencyjnego EDR Optimum funkcja Kaspersky Endpoint Detection and Response Optimum jest niedostępna.

Jak przypisać znacznik połączenia maszyny SVM do klienta Light Agent w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Tryb Light Agent** → **Znacznik połączenia SVM**.
4. Zaznacz pole **Użyj znacznika połączenia** i wprowadź znacznik połączenia maszyny SVM.

   Jako znacznik można wprowadzić ciąg tekstowy o długości do 255 znaków. Można używać wszystkich znaków z wyjątkiem `;`.
5. Zapisz swoje zmiany.

Jak przypisać znacznik połączenia maszyny SVM do klienta Light Agent w Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Tryb Light Agent** → **Znacznik połączenia SVM**.

5. Zaznacz pole **Użyj znacznika połączenia** i wprowadź znacznik połączenia maszyny SVM.

   Jako znacznik można wprowadzić ciąg tekstowy o długości do 255 znaków. Można używać wszystkich znaków z wyjątkiem `;`.

6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak przypisać znacznik połączenia maszyny SVM do klienta Light Agent w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji kliknij kafelek **Znacznik połączenia SVM** w obszarze **Tryb Light Agent**.
3. Zaznacz pole **Użyj znacznika połączenia** i wprowadź znacznik połączenia maszyny SVM.

   Jako znacznik można wprowadzić ciąg tekstowy o długości do 255 znaków. Można używać wszystkich znaków z wyjątkiem `;`.

4. Zapisz swoje zmiany.

Ochrona połączenia między klientem Light Agent a maszyną SVM

Można skonfigurować szyfrowanie połączenia między klientami Light Agent a serwerem ochrony. Aby to zrobić, należy włączyć szyfrowanie kanału danych pomiędzy klientem Light Agent a serwerem ochrony w ustawieniach serwera ochrony na maszynie SVM i w ustawieniach klienta Light Agent.

Klient Light Agent, dla którego włączono ochronę połączenia, może łączyć się wyłącznie z maszynami SVM, dla których włączono szyfrowanie kanału danych między klientem Light Agent a serwerem ochrony. Klient Light Agent, dla którego wyłączono ochronę połączenia, może łączyć się wyłącznie z maszynami SVM, dla których wyłączono szyfrowanie kanału lub w przypadku których dozwolone jest niezabezpieczone połączenie między serwerem ochrony a klientem Light Agent.

Aby uzyskać szczegółowe informacje na temat konfigurowania ochrony połączenia na serwerze ochrony, patrz Pomoc dotycząca Kaspersky Security for Virtualization Light Agent.

Ochrona połączenia przy użyciu szyfrowania może obniżyć wydajność Kaspersky Security for Virtualization Light Agent.

Jak skonfigurować ochronę połączenia w kliencie Light Agent w Konsoli administracyjnej (MMC)

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Tryb Light Agent** → **Ochrona połączenia**.
4. Zaznacz pole **Szyfruj kanał danych między agentami Light Agent a serwerem Protection Server**.
5. Zapisz swoje zmiany.

Jak skonfigurować ochronę połączenia w kliencie Light Agent w Web Console

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Tryb Light Agent** → **Ochrona połączenia**.
5. Zaznacz pole **Szyfruj kanał danych między agentami Light Agent a serwerem Protection Server**.
6. Aby zastosować zasadę do komputerów, zamknij ikony kłódek i zapisz zmiany.

Jak skonfigurować ochronę połączenia w kliencie Light Agent w interfejsie aplikacji

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji kliknij kafelek **Ochrona połączenia** w obszarze **Tryb Light Agent**.
3. Zaznacz pole **Szyfruj kanał danych między agentami Light Agent a serwerem Protection Server**.
4. Zapisz swoje zmiany.

Aktywacja klienta Light Agent

Jeśli rozwiązanie Kaspersky Endpoint Security jest używane w trybie Light Agent do ochrony środowisk wirtualnych, nie ma potrzeby oddzielnej aktywacji aplikacji. Aby aktywować aplikację, należy dodać klucz licencyjny do SVM. Klucz licencyjny można dodać do SVM przy użyciu specjalnego zadania w konsoli Kaspersky Security Center. W interfejsie Light Agent nie można zarządzać kluczami licencyjnymi, można jednak przeglądać informacje o licencji (patrz poniższy rysunek). Informacje o licencjonowaniu Light Agent można wyświetlić także w wierszu poleceń (zobacz instrukcje poniżej). Light Agent pobiera te informacje z maszyny SVM. Szczegółowe informacje na temat aktywacji rozwiązania i zarządzania kluczami licencyjnymi można znaleźć w artykule Pomoc dotycząca Kaspersky Security for Virtualization Light Agent.

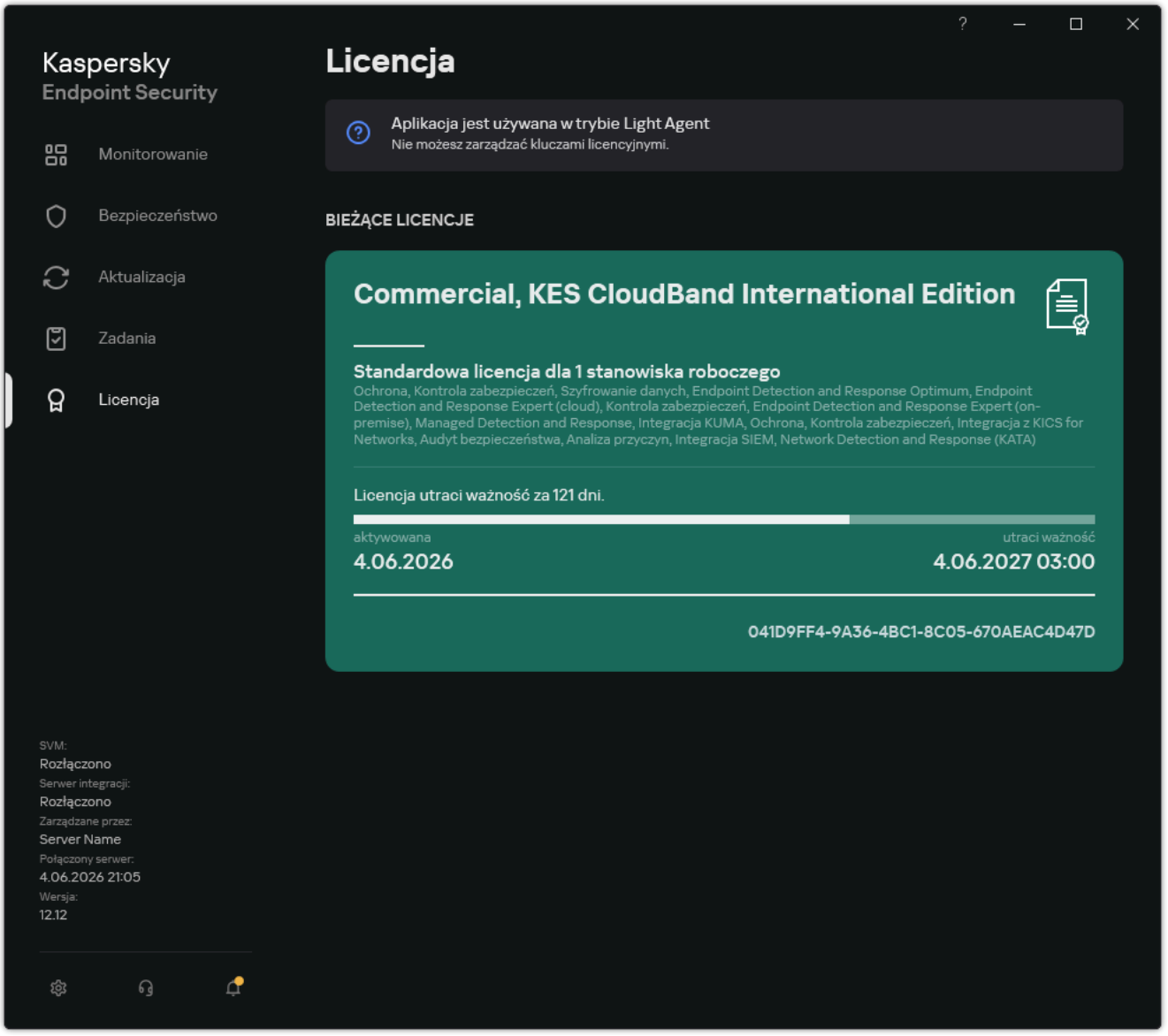
Aby wyświetlić informacje o licencjonowaniu Light Agent:

1. Uruchom wiersz poleceń (cmd) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

3. Uruchom następujące polecenie:

```
avp.com LICENSE /CHECK
```

W rezultacie Kaspersky Endpoint Security wyświetla informacje o licencji: adres maszyny SVM, z którą połączony jest klient Light Agent, liczbę dni do wygaśnięcia licencji i inne informacje. Jeśli podczas aktywacji Light Agent wystąpią jakiekolwiek problemy, zapoznaj się z Bazą wiedzy pomocy technicznej.



Okno Licencjonowanie

Przewodnik migracji z KSVLA Light Agent do KES Light Agent

Kaspersky Security for Virtualization 5.2 Light Agent zawiera składnik Light Agent dla systemu Windows 5.2 (określany dalej również jako „KSVLA Light Agent"). W rozwiązaniu Kaspersky Security for Virtualization Light Agent 6.2 funkcja Kaspersky Endpoint Security w trybie Light Agent jest używana jako komponent Light Agent. Aby zaktualizować rozwiązanie do wersji 6.2, należy przeprowadzić migrację z KSVLA Light Agent 5.2 do Kaspersky Endpoint Security w trybie Light Agent (zwanym dalej także „KES Light Agent"). Szczegółowe informacje na temat aktualizacji wersji rozwiązania Kaspersky Security for Virtualization Light Agent można znaleźć w artykule Pomoc dotycząca Kaspersky Security for Virtualization Light Agent.

Wymagania systemowe

Zanim rozpoczniesz migrację z KSVLA Light Agent do KES Light Agent, upewnij się, że Twoja maszyna wirtualna spełnia wymagania sprzętowe i programowe Kaspersky Endpoint Security for Windows. Listy obsługiwanych wersji systemów operacyjnych są różne dla KES i KSWS. Przykładowo KES nie obsługuje serwerów z systemem Windows Server 2003.

Minimalne wymagania programowe migracji z wersji KSVLA Light Agent do KES Light Agent:

- Kaspersky Endpoint Security for Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (w tym serwer ochrony i serwer integracyjny).
- Kaspersky Security Center 14.2

  Jeśli masz zainstalowaną wcześniejszą wersję Kaspersky Security Center, zaktualizuj ją do wersji 14.2 lub nowszej. W tej wersji Kaspersky Security Center Kreator konwersji zasad i zadań umożliwia migrację zasad do profilu, a nie do zasady. W tej wersji Kaspersky Security Center Kreator konwersji zasad i zadań umożliwia również migrację szerszego zakresu ustawień zasad.

Etapy migracji

Migracja z wersji KSVLA Light Agent do KES Light Agent odbywa się częściowo automatycznie. Jest to konieczne ze względu na różne architektury aplikacji.

Migracja z wersji KSVLA Light Agent do KES Light Agent przebiega w następującej kolejności:

1. **Migracja zadań i zasad KSVLA Light Agent**

   Aby przeprowadzić migrację ustawień zasad, należy uruchomić Kreatora konwersji zasad i zadań (kreatora migracji). Po przeprowadzeniu migracji ustawień zasad należy ręcznie skonfigurować ustawienia, których kreator migracji nie może przeprowadzić automatycznie (na przykład ustawienia aktualizacji baz danych). Po migracji zaleca się również sprawdzenie, czy kreator migracji poprawnie przeprowadził migrację wszystkich ustawień.

   Jeśli włączono ochronę dostępu do KSVLA Light Agent hasłem, przed instalacją KES Light Agent należy wyłączyć ochronę hasłem w zasadach KSVLA Light Agent. Nie można wprowadzić hasła dezinstalacyjnego w ustawieniach pakietu instalacyjnego KES Light Agent. Po zakończeniu instalacji KES Light Agent zastępującej KSVLA Light Agent należy włączyć ochronę hasłem w zasadzie KES.

2. **Instalowanie Kaspersky Endpoint Security w trybie Light Agent**

   KES Light Agent można zainstalować w następujące sposoby:

   - Instalacja KES Light Agent po usunięciu KSVLA Light Agent (zalecane)
   - Instalowanie KES Light Agent na KSVLA Light Agent

3. **Potwierdzenie, że aplikacja działa po migracji**

   Upewnij się, że aplikacja działa poprawnie po migracji z wersji KSVLA Light Agent do KES Light Agent. Aktywuj przekonwertowane zasady. Sprawdź stan maszyny wirtualnej w konsoli Kaspersky Security Center (powinien być oznaczony jako *OK*). Upewnij się, że aplikacja nie zgłasza błędów, sprawdź także czas ostatniego połączenia z SVM i stan ochrony maszyny wirtualnej. Nie musisz aktywować Light Agent, ponieważ klucz licencyjny zostanie dodany do SVM.

Instalowanie KES Light Agent zamiast KSVLA Light Agent

KES Light Agent można zainstalować w następujące sposoby:

- Instalacja KES Light Agent po usunięciu KSVLA Light Agent (zalecane)
- Instalowanie KES Light Agent na KSVLA Light Agent

Usunięcie KSVLA Light Agent

Aplikację można usunąć zdalnie, korzystając z zadania *Zdalna instalacja aplikacji* lokalnie na maszynie wirtualnej lub w szablonie maszyny wirtualnej. Po usunięciu KSVLA Light Agent może być konieczne ponowne uruchomienie maszyny wirtualnej.

Po usunięciu KSVLA Light Agent zainstaluj KES Light Agent za pomocą dowolnej metody.

Instalowanie Kaspersky Endpoint Security

> Jeśli włączono ochronę dostępu do KSVLA Light Agent hasłem, przed instalacją KES Light Agent należy wyłączyć ochronę hasłem w zasadach KSVLA Light Agent. Nie można wprowadzić hasła dezinstalacyjnego w ustawieniach pakietu instalacyjnego KES Light Agent. Po zakończeniu instalacji KES Light Agent zastępującej KSVLA Light Agent należy włączyć ochronę hasłem w zasadzie KES.

Podczas instalowania Kaspersky Endpoint Security musisz wybrać tryb **Light Agent do ochrony środowisk wirtualnych**. Przed zainstalowaniem KES Light Agent na maszynie wirtualnej instalator wykrywa KSVLA Light Agent jako niezgodne oprogramowanie i je usuwa. Migracja konfiguracji KSVLA Light Agent nie jest obsługiwana. Oznacza to, że podczas instalacji KES Light Agent zestaw komponentów do instalacji jest ustalany na podstawie wyboru dokonanego we właściwościach pakietu instalacyjnego lub w kreatorze instalacji. Po usunięciu KSVLA Light Agent będzie konieczne ponowne uruchomienie maszyny wirtualnej.

Ustawienia i zadania KSVLA Light Agent nie ulegają migracji podczas instalacji KES Light Agent. Aby przeprowadzić migrację ustawień i zadań, uruchom Kreatora konwersji zasad i zadań.

Listę zainstalowanych komponentów możesz sprawdzić w sekcji **Bezpieczeństwo**, w interfejsie aplikacji, korzystając z polecenia `status`, lub w konsoli Kaspersky Security Center, we właściwościach komputera. Możesz zmienić zestaw komponentów po instalacji, używając zadania *Zmiana składników aplikacji*.

Zgodność komponentów KSVLA Light Agent i KES Light Agent

Zestawy komponentów KSVLA Light Agent i KES Light Agent są niemal identyczne. KES Light Agent ma więcej ustawień niż KSVLA Light Agent. Po ukończeniu migracji nowe ustawienia będą miały wartości domyślne.

Zgodność komponentów KSVLA Light Agent i KES Light Agent

Light Agent 5.2	KES Light Agent
Scan kernel	Jądro aplikacji
File Anti-Virus	Ochrona plików
Mail Anti-Virus	Ochrona poczty
Web Anti-Virus	Ochrona WWW
Firewall	Zapora sieciowa
Network Attack Blocker	Ochrona sieci
Application Privilege Control	Ochrona przed włamaniami
Applications Launch Control	Kontrola aplikacji
Web Control	Kontrola sieci
Device Control	Kontrola urządzeń
System Watcher	W Kaspersky Endpoint Security komponent ten jest podzielony na następujące składniki: • Ochrona przed exploitami • Wykrywanie zachowań • Silnik korygujący
System Integrity Monitoring	Monitor integralności systemu
Integration with Kaspersky Endpoint Agent	*(nieobsługiwany)* Począwszy od Kaspersky Endpoint Security for Windows 11.9.0 pakiet dystrybucyjny Kaspersky Endpoint Agent nie jest już częścią zestawu dystrybucyjnego.
AMSI Protection	Ochrona AMSI

Migracja zadań i zasad KSVLA Light Agent

Ustawienia zasad i zadań klienta KSVLA Light Agent można migrować za pomocą Kreatora konwersji zasad i zadań (zwanego dalej również „Kreatorem migracji").

Kreator migracji dla KSVLA Light Agent jest dostępny tylko w Konsoli administracyjnej (MMC). Ustawienia zasad i zadań nie mogą być migrowane w Web Console ani Cloud Console.

Podczas migrowaniu zasad i zadań należy zwrócić szczególną uwagę na następujące kwestie:

- Nowe zasady mają nazwę *<Zasady> (przekształcone)*.
- Nowa zasada posiada stan *Zasada nieaktywna*.
- Zakaz modyfikowania ustawień (tzw. kłódka) nie podlega migracji. Kreator migracji ustawia wartości domyślne.
- Profile zasad nie podlegają migracji. Należy ręcznie dodać profile zasad.

- Ulepszone zarządzanie strefą zaufaną. W KSVLA Light Agent można było dodawać wstępnie zdefiniowane wykluczenia tylko podczas tworzenia zasad. We właściwościach zasad można było następnie skonfigurować dodane wcześniej wstępnie zdefiniowane wykluczenia lub dodać je ręcznie. Nie można dodawać wstępnie zdefiniowanych wykluczeń we właściwościach zasad. W KES Light Agent wstępnie zdefiniowane wykluczenia są dostępne zarówno podczas tworzenia zasad, jak i we właściwościach utworzonych zasad. Można również wybrać wstępnie zdefiniowane wykluczenia w pakiecie instalacyjnym.

- Konfigurację interfejsu użytkownika aplikacji w Kaspersky Endpoint Security przeniesiono z instalatora do zasad. Jeśli na przykład chcesz ukryć interfejs użytkownika aplikacji, musisz zmienić ustawienia zasad.

- Zestawy funkcji umożliwiające konfigurację kontroli dostępu opartej na uprawnieniach (RBAC) różnią się w produktach Kaspersky Endpoint Security i KSVLA Light Agent. Należy od podstaw skonfigurować uprawnienia dostępu użytkowników do obszarów funkcjonalnych.

Jak używać Kreatora konwersji zasad i zadań do migracji ustawień zasad KSVLA Light Agent

1. W Konsoli administracyjnej wybierz Serwer administracyjny i kliknij go prawym klawiszem myszy, aby otworzyć menu kontekstowe.

2. Wybierz **Wszystkie zadania** → **Kreator konwersji zasad i zadań**.

Uruchomi się Kreator konwersji zasad i zadań. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Wybieranie aplikacji, dla której konieczna jest konwersja zasad i zadań

Na tym etapie należy wybrać Kaspersky Endpoint Security for Windows. Przejdź do następnego kroku.

Krok 2. Konwersja zasad

Wybierz zasady Kaspersky Security for Virtualization 5.2 Light Agent for Windows, które chcesz przekonwertować. Przejdź do następnego kroku.

Następnie Kreator migracji rozpocznie konwertowanie zasad. Podczas konwersji zasady Kreator migracji poprosi o zaakceptowanie Oświadczenia KSN. Nowe zasady mają nazwę *<Zasady> (przekształcone)*.

Krok 3. Konwersja zadań

Kreator migracji tworzy nowe zadania dla Kaspersky Endpoint Security for Windows. Na liście zadań wybierz zadania KSVLA Light Agent, które chcesz utworzyć dla Kaspersky Endpoint Security. Nowe zadania będą posiadały nazwę *<Nazwa zadania> (przekonwertowane)*. Przejdź do następnego kroku.

Krok 4. Kończenie działania kreatora

Zakończ działanie Kreatora.

Po wykonaniu migracji zasad musisz otworzyć właściwości zasady, sprawdzić jej ustawienia i ją zapisać. Jeśli nie wykonasz tych kroków, KES Light Agent może zignorować przekonwertowaną zasadę.

Zwróć szczególną uwagę na migrację list wykluczeń w ustawieniach połączenia maszyny SVM klienta Light Agent, zaufanych aplikacji, zaufanych adresów internetowych, reguł Kontroli aplikacji.

Migracja konfiguracji [KSVLA Light Agent+KEA] do konfiguracji [KES Light Agent+wbudowany agent]

Aby wspierać korzystanie z Kaspersky Endpoint Security for Windows w ramach EDR (KATA), EDR Optimum i Kaspersky Sandbox, do aplikacji dodano wbudowanego agenta. Nie potrzebujesz już oddzielnej aplikacji Kaspersky Endpoint Agent do pracy z tymi rozwiązaniami.

Po migracji z KSVLA Light Agent do KES Light Agent rozwiązania EDR (KATA), EDR Optimum i Kaspersky Sandbox nadal działają z wbudowanymi agentami Kaspersky Endpoint Security. Dodatkowo, Kaspersky Endpoint Agent zostanie usunięty z komputera.

Przed migracją z KSVLA Light Agent do KES Light Agent należy zaktualizować wszystkie komponenty Kaspersky Security for Virtualization, w tym serwer ochrony i serwer integracyjny, do wersji 6.2. Szczegółowe informacje na temat aktualizacji wersji rozwiązania Kaspersky Security for Virtualization Light Agent można znaleźć w artykule Pomoc dotycząca Kaspersky Security for Virtualization Light Agent.

Migracja konfiguracji [KSVLA Light Agent+KEA] do konfiguracji [KES Light Agent+wbudowany agent] obejmuje następujące kroki:

1. **Migrowanie zasady i zadań**

   Migracja zasad i zadań [KSVLA Light Agent+KEA] do [KES Light Agent+wbudowany agent] obejmuje następujące kroki:

   1. Migrowanie profili i zadań z KSVLA Light Agent do KES Light Agent za pomocą Kreatora konwersji zasad i zadań (dostępne tylko w Konsoli administracyjnej MMC).

      W rezultacie tworzona jest nowa zasada o nazwie *<Zasada> (przekonwertowana)*. Nowe zadania KES są również tworzone z nazwami *<Nazwa zadania> (przekonwertowane)*.

   2. Migrowanie profili i zadań z KEA do KES przy użyciu kreatora migracji z Kaspersky Endpoint Agent (dostępne tylko w Web Console i Cloud Console).

      W rezultacie tworzona jest nowa zasada o podanej nazwie *<Nazwa zasady Kaspersky Endpoint Security> i <Nazwa zasady Kaspersky Endpoint Agent>*. Tworzone są również nowe zadania i zadania KES.

2. **Migracja z KSVLA Light Agent do KES Light Agent**

Migracja z KSVLA Light Agent do KES Light Agent wymaga instalacji KES Light Agent zamiast KSVLA Light Agent.

Administratorzy zazwyczaj włączają Ochronę hasłem, aby ograniczyć dostęp do KSVLA Light Agent i KEA. Hasło dezinstalacyjne KEA można wprowadzić tylko we właściwościach zadania *Zdalna instalacja aplikacji*. Na potrzeby migracji należy wyłączyć ochronę hasłem oprogramowania KSVLA Light Agent.

Aby przeprowadzić migrację, musisz wybrać komponenty potrzebne do obsługi rozwiązań Detection and Response w ramach Kaspersky Endpoint Security. Po zainstalowaniu aplikacji Kaspersky Endpoint Security przełącza się na używanie wbudowanego agenta i usuwa Kaspersky Endpoint Agent.

3. **Funkcjonalność licencjonowania**

   Jeśli aplikacja jest używana w trybie Light Agent, nie trzeba jej aktywować. Aby aktywować aplikację, należy dodać klucz licencyjny do SVM. Należy również dodać klucz licencyjny w celu aktywacji dodatkowych funkcji (np. EDR Optimum) w SVM. Oznacza to, że licencjonowanie funkcji odbywa się automatycznie w ramach migracji.

4. **Sprawdzanie zdrowia Kaspersky Endpoint Detection and Response Optimum i Kaspersky Sandbox**

   Jeśli po aktualizacji, komputer posiada stan *Krytyczny* w konsoli Kaspersky Security Center:

   - Upewnij się, że na komputerze jest zainstalowany Agent sieciowy w wersji 13.2 lub wyższej.
   - Sprawdź stan działania komponentów, przeglądając *Raport o stanie składników aplikacji*. Jeśli komponent ma stan *Nie zainstalowano*, zainstaluj komponent przy użyciu zadania *Zmiana składników aplikacji*.
   - Upewnij się, że akceptujesz Oświadczenie Kaspersky Security Network w nowej zasadzie Kaspersky Endpoint Security for Windows.
   - Upewnij się, że funkcja EDR Optimum została aktywowana za pomocą opcji *Raport o stanie składników aplikacji*. Jeśli komponent posiada stan *Nieobjęte licencją*, upewnij się, że funkcjonalność automatycznej dystrybucji klucza licencyjnego EDR Optimum jest włączona.
   - Sprawdź stan połączenia maszyny wirtualnej z SVM. Informacje o stanie połączenia klienta Light Agent z maszyną SVM można uzyskać w programie Kaspersky Endpoint Security lub za pomocą polecenia w aplikacji.

Zarządzanie aplikacją z poziomu wiersza poleceń

Możesz zarządzać Kaspersky Endpoint Security z poziomu wiersza poleceń. Możesz wyświetlić listę poleceń do zarządzania aplikacją, uruchamiając polecenie `avp.com HELP`. Aby zapoznać się z informacjami o składni konkretnego polecenia, wpisz `avp.com HELP <command>`.

Znaki specjalne w poleceniu muszą zostać pominięte. Aby pominąć znaki `&`, `|`, `(`, `)`, `<`, `>`, `^`, użyj znaku `^` (na przykład, aby użyć znaku `&`, wprowadź `^&`). Aby pominąć znak `%`, wprowadź `%%`.

Zamiast wartości `1` możesz użyć wartości `yes`, `on`, `enable`, `enabled`, and `true`. Zamiast wartości `0` możesz użyć wartości `no`, `off`, `disable`, `disabled`, and `false`.

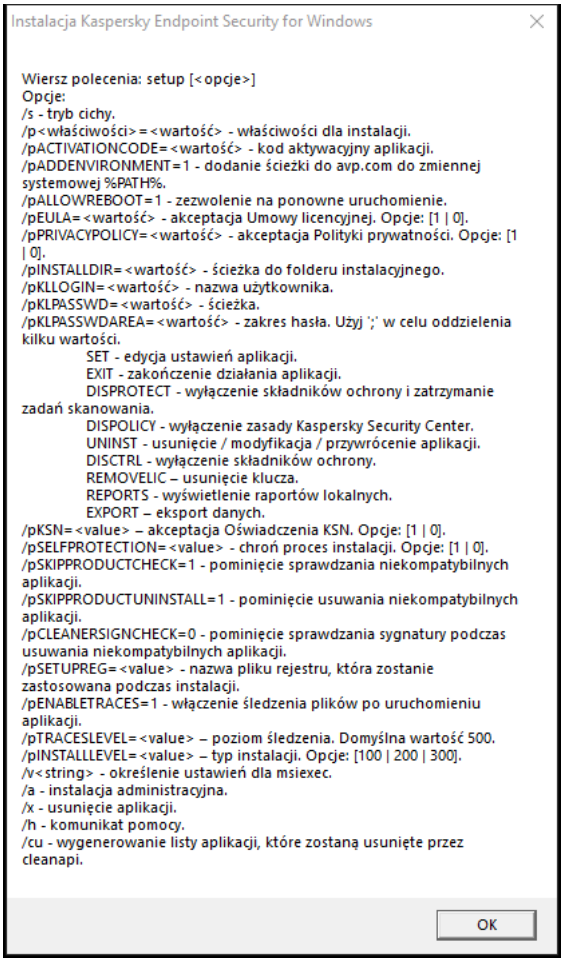
Setup. Instalowanie aplikacji

Kaspersky Endpoint Security może zostać zainstalowany z poziomu wiersza poleceń w jednym z następujących trybów:

- W trybie interaktywnym, korzystając z Kreatora instalacji aplikacji.
- W trybie cichym. Po uruchomieniu instalacji w trybie cichym nie jest wymagany udział w procesie instalacji (instalacja dyskretna). Aby zainstalować aplikację w trybie cichym, użyj przełączników `/s` i `/qn`.

  Przed zainstalowaniem aplikacji w trybie cichym należy otworzyć i przeczytać Umowę licencyjną i Politykę prywatności. Umowa licencyjna oraz Polityka prywatności znajdują się w pakiecie dystrybucyjnym Kaspersky Endpoint Security. Przejście do instalacji aplikacji jest możliwe tylko wtedy, gdy w pełni przeczytałeś, zrozumiałeś i zaakceptowałeś warunki Umowy licencyjnej, przeczytałeś i zrozumiałeś, że Twoje dane będą przetwarzane i przesyłane (w tym do innych krajów) zgodnie z Polityką prywatności oraz w pełni przeczytałeś i zrozumiałeś Politykę prywatności. Jeśli nie akceptujesz warunków i postanowień Umowy licencyjnej i Polityki prywatności, nie instaluj ani nie używaj Kaspersky Endpoint Security.

Możesz wyświetlić listę poleceń do zarządzania aplikacją, uruchamiając polecenie `/h`. Aby uzyskać pomoc dotyczącą składni polecenia instalacji, należy wpisać `setup_kes.exe /h`. W efekcie instalator wyświetla okno z opisem opcji polecenia (patrz rysunek poniżej).



Opis opcji polecenia instalacji

W celu zainstalowania aplikacji lub zaktualizowania poprzedniej wersji aplikacji:

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się pakiet dystrybucyjny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

LUB

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

W wyniku tego działania aplikacja zostanie zainstalowana na komputerze. Możesz potwierdzić, że aplikacja jest zainstalowana i sprawdzić ustawienia aplikacji, publikując polecenie `status`.

`EULA=1`	Akceptacja lub odrzucenie warunków Umowy licencyjnej. Umowa licencyjna jest zawarta w pakiecie dystrybucyjnym Kaspersky Endpoint Security. Akceptacja warunków Umowy licencyjnej jest niezbędna do zainstalowania aplikacji lub jej aktualizacji.
`PRIVACYPOLICY=1`	Akceptacja Polityki prywatności. Treść Polityki prywatności znajduje się w pakiecie dystrybucyjnym Kaspersky Endpoint Security. Aby zainstalować aplikację lub zaktualizować wersję aplikacji, musisz zaakceptować Politykę prywatności.
`KSN`	Akceptacja lub odmowa uczestnictwa w Kaspersky Security Network (KSN). Jeśli nie ustawiono wartości dla tego parametru, Kaspersky Endpoint Security wyświetli monit o potwierdzenie zgody lub odmowę uczestniczenia w KSN przy pierwszym uruchomieniu Kaspersky Endpoint Security. Dostępne wartości: • `1` – zgoda na uczestniczenie w KSN. • `0` – odmowa uczestniczenia w KSN (wartość domyślna). Pakiet dystrybucyjny Kaspersky Endpoint Security jest zoptymalizowany do użycia z Kaspersky Security Network. Jeśli zdecydowałeś się nie uczestniczyć w Kaspersky Security Network, powinieneś zaktualizować Kaspersky Endpoint Security od razu po zakończeniu instalacji.
`CONFIGPATH=<path to the configuration file>`	Instalowanie aplikacji ze wstępnie zdefiniowanymi ustawieniami. Aby to zrobić, musisz przesłać plik, który definiuje ustawienia Kaspersky Endpoint Security. Możesz utworzyć plik konfiguracyjny w interfejsie lokalnym aplikacji.
`ALLOWREBOOT=1`	Automatyczne ponowne uruchamianie komputera, jeśli jest wymagane po zainstalowaniu lub zaktualizowaniu aplikacji. Jeśli dla tego parametru nie zostanie ustawiona żadna wartość, automatyczne ponowne uruchomienie komputera zostanie zablokowane. Ponowne uruchomienie nie jest wymagane podczas instalowania Kaspersky Endpoint Security. Ponowne uruchomienie jest wymagane tylko wtedy, gdy przed instalacją musisz usunąć niekompatybilne aplikacje. Ponowne uruchomienie może być też wymagane podczas aktualizowania wersji aplikacji.
`SKIPPRODUCTCHECK=1`	Wyłącz sprawdzanie zainstalowanego oprogramowania. Lista oprogramowania, które może być przyczyną problemów ze zgodnością jest dostępna w pliku incompatible.txt, który znajduje się w pakiecie dystrybucyjnym. Jeśli dla tego parametru nie zostanie ustawiona żadna wartość i zostanie wykryte oprogramowanie z listy, instalacja Kaspersky Endpoint Security zostanie zakończona.
`SKIPPRODUCTUNINSTALL=1`	Wyłącz automatyczne usuwanie wykrytego oprogramowania z listy w pliku incompatible.txt. Jeśli dla tego parametru nie zostanie ustawiona żadna wartość, Kaspersky Endpoint Security spróbuje usunąć oprogramowanie, które może powodować problemy z kompatybilnością. Automatyczne usuwanie oprogramowania nie może być włączone podczas instalacji Kaspersky Endpoint Security za pomocą instalatora msiexec. Aby automatycznie usunąć oprogramowanie, które może powodować problemy z kompatybilnością, użyj pliku setup_kes.exe.
`CLEANERSIGNCHECK=0|1`	Weryfikacja podpisów cyfrowych plików wykrytego oprogramowania z listy incompatible.txt. Aby usunąć oprogramowanie, Kaspersky Endpoint Security uruchamia plik instalatora oprogramowania. Jeśli w pliku instalatora nie ma podpisu cyfrowego, Kaspersky Endpoint Security uznaje plik za niezaufany i wstrzymuje usuwanie oprogramowania, aby uniknąć uruchomienia potencjalnie szkodliwego kodu. Jeśli aplikacja nie może zweryfikować podpisu cyfrowego pliku wykrytego oprogramowania, instalacja Kaspersky Endpoint Security zostanie zatrzymana z błędem. Wartość domyślna różni się w zależności od metody instalacji oprogramowania: • `0` oznacza, że weryfikacja podpisu cyfrowego jest wyłączona (wartość domyślna, jeśli została wdrożona za pośrednictwem Kaspersky Security Center). • `1` oznacza, że weryfikacja podpisu cyfrowego jest włączona (wartość domyślna, jeśli aplikacja jest instalowana lokalnie).
`STANDALONEMODE=1`	Instalacja aplikacji w konfiguracji Endpoint Detection and Response Agent (EDR Agent) do integracji z rozwiązaniem Kaspersky Endpoint Detection and Response (KATA) lub Kaspersky Endpoint Detection and Response Expert (on-premises). Ta konfiguracja jest potrzebna, jeśli Platforma ochrony punktów końcowych (EPP) innej firmy jest wdrażana w Twojej organizacji wraz z rozwiązaniem klasy Kaspersky Endpoint Detection and Response. Dzięki temu Kaspersky Endpoint Security w konfiguracji Endpoint Detection and Response Agent jest kompatybilny z aplikacjami EPP innych firm.
`KLLOGIN`	Ustaw nazwę użytkownika, aby uzyskać dostęp do funkcji i ustawień Kaspersky Endpoint Security (komponent Ochrona hasłem). Nazwa użytkownika jest ustawiana wraz z parametrami `KLPASSWD` i `KLPASSWDAREA`. Nazwa użytkownika KLAdmin jest używana domyślnie.

KLPASSWD	Określ hasło dostępu do funkcji i ustawień Kaspersky Endpoint Security (hasło jest określane wraz z parametrami KLLOGIN i KLPASSWDAREA). Jeśli określiłeś hasło, ale nie określiłeś nazwy użytkownika z parametrem KLLOGIN, domyślnie używana będzie nazwa użytkownika KLAdmin.
KLPASSWDAREA	Zakres działania hasła dostępu do funkcji i ustawień Kaspersky Endpoint Security. Jeśli użytkownik spróbuje wykonać działanie, które znajduje się w tym obszarze, Kaspersky Endpoint Security wyświetli monit o podanie danych uwierzytelniających konta użytkownika (parametry KLLOGIN i KLPASSWD). Użyj znaku ;, aby określić kilka wartości. Dostępne wartości: • SET – modyfikowanie ustawień aplikacji. • EXIT – zakończenie działania aplikacji. • DISPROTECT – wyłączanie komponentów ochrony i zatrzymywanie zadań skanowania. • DISPOLICY – wyłączanie zasady Kaspersky Security Center. • UNINST – usunięcie aplikacji z komputera. • DISCTRL – wyłączenie składników kontroli. • REMOVELIC – usuwanie klucza. • REPORTS – wyświetlanie raportów. • EXPORT – eksportowanie ustawień aplikacji. Na przykład, KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT. Konto KLAdmin posiada prawo do wykonania dowolnego działania, które jest chronione hasłem. W związku z tym skonfigurowanie zakresu hasła dla konta KLAdmin jest niemożliwe. Jeśli spróbujesz skonfigurować zakres hasła dla konta KLAdmin, aplikacja zablokuje określone działania dla grupy „Wszyscy”.
PROTECTOSSERVICES	Ochrona funkcjonalności usług systemu operacyjnego. Ochrona usług systemu operacyjnego zapobiega zakłócaniu ich działania przez aplikacje innych firm. Do takich usług zalicza się na przykład usługę automatycznego uruchamiania aplikacji. • 1 oznacza, że ochrona usług systemu operacyjnego jest włączona (wartość domyślna). • 0 oznacza, że ochrona usług systemu operacyjnego jest wyłączona.
ENABLETRACES	Włączanie lub wyłączanie śledzenia aplikacji. Po uruchomieniu program Kaspersky Endpoint Security zapisuje pliki śledzenia w folderze %ProgramData%\Kaspersky Lab\KES.14.1\Traces. Dostępne wartości: • 1 – śledzenie jest włączone. • 0 – śledzenie jest wyłączone (wartość domyślna).
TRACESLEVEL	Poziom szczegółowości śledzenia. Dostępne wartości: • 100 (krytyczny). Tylko wiadomości dotyczące błędów krytycznych. • 200 (wysoki). Wiadomości o wszystkich błędach, w tym błędach krytycznych. • 300 (diagnostyczny). Wiadomości o wszystkich błędach, a także ostrzeżenia. • 400 (ważny). Wszystkie wiadomości o błędach, ostrzeżenia i dodatkowe informacje. • 500 (normalny). Wiadomości o wszystkich błędach i ostrzeżeniach, a także szczegółowe informacje o działaniu aplikacji w trybie normalnym (domyślnie). • 600 (niski). Wszystkie wiadomości.
ENABLEAZURESUPPORT	Włączanie lub wyłączanie trybu zgodności Azure WVD. Dostępne wartości: • 1 – Tryb zgodności Azure WVD jest włączony. • 0 – Tryb zgodności Azure WVD jest wyłączony (wartość domyślna). Ta funkcja zapewnia prawidłowe wyświetlanie stanu maszyny wirtualnej Azure w konsoli Kaspersky Anti Targeted Attack Platform. Aby monitorować wydajność komputera, Kaspersky Endpoint Security wysyła dane telemetryczne do serwerów KATA. Dane telemetryczne obejmują identyfikator komputera (Sensor ID). Tryb zgodności Azure WVD umożliwia przypisanie do tych maszyn wirtualnych trwałego unikatowego identyfikatora Sensor ID. Jeśli tryb zgodności jest wyłączony, Sensor ID może ulec zmianie po ponownym uruchomieniu komputera ze względu na sposób działania maszyn wirtualnych platformy Azure. Może to spowodować pojawienie się duplikatów maszyn wirtualnych w konsoli.
AMPPL	Włącza lub wyłącza ochronę procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL (Antimalware Protected Process Light). Więcej informacji na temat technologii AM-PPL znajdziesz na stronie internetowej firmy Microsoft. Technologia AM-PPL jest dostępna dla systemu Windows 10 w wersji 1703 (RS2) lub nowszej oraz systemów operacyjnych Windows Server 2019. Dostępne wartości: • 1 – ochrona procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL jest włączona. • 0 – ochrona procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL jest wyłączona.

`UPGRADEMODE`	Tryb aktualizacji aplikacji: • `Seamless` oznacza aktualizację aplikacji z ponownym uruchomieniem komputera (wartość domyślna). • `Force` oznacza aktualizację aplikacji bez konieczności ponownego uruchomienia. Począwszy od wersji 11.10.0 możesz aktualizować aplikację bez konieczności ponownego uruchamiania. Aby zaktualizować wcześniejszą wersję aplikacji, musisz ponownie uruchomić komputer. Począwszy od wersji 11.11.0 możesz aktualizować aplikację bez konieczności ponownego uruchamiania. Ponowne uruchomienie nie jest wymagane podczas instalowania Kaspersky Endpoint Security. Tak więc tryb aktualizacji aplikacji zostanie określony w ustawieniach aplikacji. Parametr ten możesz zmienić w ustawieniach aplikacji lub w zasadach. Podczas aktualizacji już zainstalowanej aplikacji priorytet parametru wiersza poleceń jest niższy niż parametru określonego w ustawieniach aplikacji lub w pliku setup.ini. Na przykład, jeśli w wierszu poleceń zostanie określony tryb aktualizacji `Force`, a w ustawieniach aplikacji zostanie określony tryb `Seamless`, aktualizacja zostanie zainstalowana z ponownym uruchomieniem komputera (`Seamless`).
`RESTAPI`	Zarządzanie aplikacją za pośrednictwem interfejsu API REST. Aby zarządzać aplikacją za pośrednictwem interfejsu API REST, należy podać nazwę użytkownika (parametr `RESTAPI_User`). Dostępne wartości: • `1` – zarządzanie za pośrednictwem interfejsu API REST jest dozwolone. • `0` – zarządzanie za pośrednictwem interfejsu API REST jest zablokowane (wartość domyślna). Aby zarządzać aplikacją za pośrednictwem interfejsu API REST, zarządzanie przy użyciu systemów administracyjnych musi być dozwolone. W tym celu ustaw parametr `AdminKitConnector=1`. Jeśli zarządzasz aplikacją za pośrednictwem interfejsu API REST, zarządzanie aplikacją przy użyciu systemów administracyjnych firmy Kaspersky jest niemożliwe.
`RESTAPI_User`	Nazwa użytkownika konta domeny Windows używanego do zarządzania aplikacją za pośrednictwem interfejsu API REST. Zarządzanie aplikacją za pośrednictwem interfejsu API REST jest dostępne tylko dla tego użytkownika. Wpisz nazwę użytkownika w formacie `<DOMAIN>\<UserName>` (na przykład: `RESTAPI_User=COMPANY\Administrator`). Możesz wybrać tylko jednego użytkownika do pracy z interfejsem API REST. Dodanie nazwy użytkownika jest wymaganiem wstępnym zarządzania aplikacją za pośrednictwem interfejsu API REST.
`RESTAPI_Port`	Port używany do zarządzania aplikacją za pośrednictwem interfejsu API REST. Domyślnie używany jest port 6782. Upewnij się, że port jest wolny.
`RESTAPI_Certificate`	Certyfikat do identyfikowania żądań (na przykład, `RESTAPI_Certificate=C:\cert.pem`). Bezpieczna interakcja Kaspersky Endpoint Security z klientem REST wymaga skonfigurowania identyfikacji żądania. W tym celu należy zainstalować certyfikat i podpisać ładunek każdego żądania.
`ADMINKITCONNECTOR`	Zarządzanie aplikacjami za pomocą systemów administracyjnych. Systemy administracyjne obejmują, na przykład, Kaspersky Security Center. Oprócz systemów administracyjnych Kaspersky możesz korzystać z rozwiązań innych firm. Kaspersky Endpoint Security oferuje w tym celu interfejs API. Dostępne wartości: • `1` – dozwolone jest zarządzanie aplikacjami za pomocą systemów administracyjnych (wartość domyślna). • `0` – zarządzanie aplikacjami jest dozwolone tylko przez interfejs lokalny.
`EnableUniqueSensorID`	Tworzenie unikalnego identyfikatora komputera (Sensor ID) podczas instalacji lub aktualizacji aplikacji. Identyfikator Sensor ID jest wykorzystywana w rozwiązaniu Kaspersky Anti Targeted Attack Platform do identyfikowania komputerów wysyłających dane telemetryczne na serwer. Podczas tworzenia Sensor ID aplikacja wykorzystuje algorytm uwzględniający konfigurację komputera, np. numer seryjny płyty głównej. W niektórych przypadkach, na przykład podczas korzystania z aplikacji w środowisku wirtualnym, identyfikator Sensor ID może być zduplikowany. W rezultacie Kaspersky Anti Targeted Attack Platform nie może zidentyfikować komputera, z którego wysłano dane telemetryczne. Aby utworzyć unikalny Sensor ID, należy ustawić parametr `EnableUniqueSensorID=1`. W rezultacie aplikacja użyje innego algorytmu do utworzenia Sensor ID, który bierze pod uwagę również inne dane dotyczące komputera. Dzięki temu identyfikator Sensor ID jest unikalny. Domyślnie parametr nie jest ustawiony. Aplikacja dziedziczy Sensor ID w następujących przypadkach: • Aktualizacja wersji aplikacji • migracja konfiguracji [KES+KEA] do konfiguracji [KES+wbudowany agent] Instalator próbuje odziedziczyć identyfikator <1> w ramach jej naprawy.Sensor ID. Jeśli identyfikatora Sensor ID nie można przywrócić, aplikacja utworzy nowy identyfikator Sensor ID.
`SKIPKB5007186CHECK=1`	Wyłączenie sprawdzania zainstalowanej aktualizacji KB5007186 systemu operacyjnego. Przed zainstalowaniem aplikacji instalator sprawdza zainstalowane aktualizacje systemu operacyjnego. Aktualizacja KB5007186 znajduje się na liście aktualizacji systemu operacyjnego, które mogą powodować problemy z aplikacją. Aby uzyskać szczegółowe informacje, zapoznaj się z Bazą wiedzy na stronie działu pomocy technicznej. Dlatego instalator przerwie instalację, jeśli wykryje tę aktualizację. Aby kontynuować instalację, ustaw `SKIPKB5007186CHECK=1`.

Na przykład

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Po zainstalowaniu Kaspersky Endpoint Security licencja testowa zostanie aktywowana, chyba że nie dostarczyłeś kodu aktywacyjnego w pliku setup.ini. Licencja testowa ma zazwyczaj krótki okres ważności. Po wygaśnięciu licencji testowej wszystkie funkcje programu Kaspersky Endpoint Security stają się niedostępne. Aby kontynuować korzystanie z aplikacji, należy aktywować aplikację z licencją komercyjną przy użyciu Kreatora aktywacji aplikacji lub specjalnego polecenia.

Podczas instalacji aplikacji lub uaktualniania jej wersji w trybie cichym używane są następujące pliki:

- setup.ini – ustawienia ogólne instalacji aplikacji.

  Aby zastosować ustawienia z pliku setup.ini, umieść ten plik w folderze zawierającym pakiet dystrybucyjny Kaspersky Endpoint Security.

- install.cfg – ustawienia działania Kaspersky Endpoint Security

  Aby zastosować ustawienia z pliku konfiguracyjnego install.cfg, musisz określić ścieżkę do pliku w następującym poleceniu instalacji aplikacji: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – klucze rejestru.

  Klucze rejestru z pliku setup.reg zostają zapisane do rejestru tylko wtedy, gdy w pliku setup.ini, dla parametru `SetupReg` ustawiono wartość `setup.reg`. Plik setup.reg jest generowany przez ekspertów z Kaspersky. Nie jest zalecane modyfikowanie zawartości tego pliku. Aby zastosować ustawienia z pliku setup.reg, umieść ten plik w folderze zawierającym pakiet dystrybucyjny Kaspersky Endpoint Security. Możesz także umieścić plik setup.reg w innym folderze. Jeśli to konieczne, musisz określić ścieżkę do pliku w następującym poleceniu instalacji aplikacji: `SETUPREG=<path to the setup.reg file>`.

Setup /x. Dezinstalacja aplikacji

Kaspersky Endpoint Security może zostać odinstalowany z poziomu wiersza poleceń w jeden z następujących sposobów:

- W trybie interaktywnym, korzystając z Kreatora instalacji aplikacji.

- W trybie cichym. W tym trybie nie jest wymagany udział użytkownika w procesie dezinstalacji (dezinstalacja dyskretna). Aby odinstalować aplikację w trybie cichym, użyj przełączników `/s` i `/qn`.

W celu odinstalowania aplikacji w trybie cichym:

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.

2. Przejdź do folderu, w którym znajduje się pakiet dystrybucyjny Kaspersky Endpoint Security.

3. Uruchom następujące polecenie:

- Jeśli proces dezinstalacji nie jest chroniony hasłem:

  ```
  setup_kes.exe /s /x
  ```

  LUB

  ```
  msiexec.exe /x <GUID> /qn
  ```

  `<GUID>` jest unikatowym identyfikatorem aplikacji. Możesz znaleźć identyfikator GUID aplikacji w Bazie wiedzy pomocy technicznej lub za pomocą następującego polecenia:

  ```
  wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
  ```

- Jeśli proces dezinstalacji jest chroniony hasłem:

  ```
  setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
  ```

  LUB

  ```
  msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
  ```

Można również użyć parametru `SAVEQB` w celu zachowania plików przeskanowanych przez aplikację i umieszczonych w kopii zapasowej. Kopie zapasowe plików są przechowywane w folderze `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`. Zapisywanie plików w kopii zapasowej jest domyślnie wyłączone (`SAVEQB=0`).

Na przykład

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. Odzyskiwanie aplikacji

Podczas odzyskiwania aplikacja sprawdza i przywraca integralność wszystkich uszkodzonych modułów aplikacji i kluczy rejestru systemowego utworzonych w ramach procesu instalacji aplikacji.

Kaspersky Endpoint Security można przywrócić z poziomu wiersza poleceń w jednym z następujących trybów:

- W trybie interaktywnym, korzystając z Kreatora instalacji aplikacji.
- W trybie cichym. Po rozpoczęciu przywracania w trybie cichym nie jest wymagany udział użytkownika.

Jeśli instalator Kaspersky Endpoint Security działa w trybie odzyskiwania, a aplikacja go nie wymaga, instalator nie wprowadza żadnych zmian.

Jeśli instalator Kaspersky Endpoint Security działa w trybie odzyskiwania, a aplikacja nie jest zainstalowana, instalator rozpocznie proces instalacji.

W celu odzyskania aplikacji w trybie cichym:

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się pakiet dystrybucyjny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:
   - Jeśli proces odzyskiwania nie jest chroniony hasłem:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     <GUID> jest unikatowym identyfikatorem aplikacji. Możesz znaleźć identyfikator GUID aplikacji w Bazie wiedzy pomocy technicznej lub za pomocą następującego polecenia:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Jeśli proces odzyskiwania jest chroniony hasłem:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Na przykład

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

Polecenia AVP

W celu zarządzania Kaspersky Endpoint Security z poziomu wiersza poleceń:

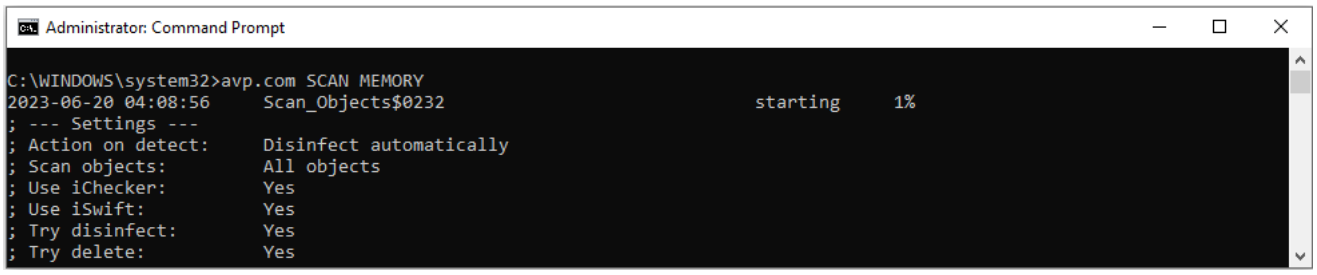
1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

   Możesz dodać ścieżkę do pliku wykonywalnego do zmiennej systemowej %PATH% podczas instalacja aplikacji.

3. Aby wykonać polecenie, użyj następującego szablonu:

```
avp.com <command> [options]
```

W rezultacie Kaspersky Endpoint Security wykona polecenie (patrz rysunek poniżej).



Zarządzanie aplikacją z poziomu wiersza poleceń

SCAN. Skanowanie w poszukiwaniu złośliwego oprogramowania

Uruchamianie zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

Obszar skanowania	
`<files to scan>`	Rozdzielona spacjami lista plików i folderów. Długie ścieżki muszą być ujęte w cudzysłów. Krótkie ścieżki (format MS-DOS) nie muszą być ujęte w cudzysłów. Na przykład: • `"C:\Program Files (x86)\Example Folder"` – długa ścieżka. • `C:\PROGRA~2\EXAMPL~1` – krótka ścieżka.
`/ALL`	Uruchamia zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Kaspersky Endpoint Security skanuje następujące obiekty: • Pamięć jądra • Obiekty uruchamiane wraz ze startem systemu operacyjnego • Sektory startowe • Kopię zapasową systemu operacyjnego • Wszystkie dyski twarde i wymienne W programie Kaspersky Endpoint Security for Windows 12.12 poczta e-mail jest wykluczona z zakresu skanowania aplikacji. Skanowanie przychodzących i wychodzących wiadomości e-mail odbywa się za pomocą komponentu Ochrona poczty. Jeśli używasz starszej wersji wtyczki zarządzającej, aplikacja wyklucza pocztę e-mail z zakresu skanowania, nawet jeśli zasady je uwzględniają.
`/MEMORY`	Skanuje pamięć jądra
`/STARTUP`	Skanuje obiekty uruchamiane wraz ze startem systemu operacyjnego

`/REMDRIVES`	Skanuje nośniki wymienne.
`/FIXDRIVES`	Skanuje dyski twarde.
`/NETDRIVES`	Skanuje dyski sieciowe.
`/QUARANTINE`	Skanuje pliki w Kopii zapasowej Kaspersky Endpoint Security.
`/@:<file list.lst>`	Skanuje pliki i foldery z listy. Każdy plik na liście musi znajdować się w nowym wierszu. Długie ścieżki muszą być ujęte w cudzysłów. Krótkie ścieżki (format MS-DOS) nie muszą być ujęte w cudzysłów. Na przykład: • `"C:\Program Files (x86)\Example Folder"` – długa ścieżka. • `C:\PROGRA~2\EXAMPL~1` – krótka ścieżka.

Działanie podejmowane w przypadku wykrycia zagrożenia	
`/i0`	**Poinformuj**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików.
`/i1`	**Wylecz; poinformuj, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeśli leczenie się nie powiedzie, Kaspersky Endpoint Security doda informacje o wykrytych zainfekowanych plikach do listy aktywnych zagrożeń.
`/i2`	**Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik. To ustawienie jest wybrane domyślnie.
`/i3`	**Usuń, jeżeli leczenie nie jest możliwe**. Usunie także pliki złożone (na przykład, archiwa), jeśli zainfekowanego pliku nie można wyleczyć ani usunąć.
`/i4`	**Usuń**. Usunie także pliki złożone (na przykład, archiwa), jeśli zainfekowanego pliku nie można usunąć.

Typy plików	
`/fe`	**Pliki skanowane według rozszerzenia**. Jeżeli wybierzesz tę opcję, aplikacja będzie skanować tylko infekowalne pliki. Format pliku będzie określany w oparciu o jego rozszerzenie.
`/fi`	**Pliki skanowane według formatu**. Jeżeli wybierzesz tę opcję, aplikacja będzie skanować tylko infekowalne pliki. Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików.
`/fa`	**Wszystkie pliki**. Jeżeli wybierzesz tę opcję, aplikacja będzie skanować wszystkie pliki bez wyjątku (wszystkie formaty i rozszerzenia). Jest to ustawienie domyślne.

Wykluczenia ze skanowania	
`-e:a`	Archiwa RAR, ARJ, ZIP, CAB, LHA, JAR i ICE są wyłączone z obszaru skanowania.
`-e:<file mask>`	Pliki odpowiadające masce pliku są wykluczone z obszaru skanowania. Na przykład: • Maska `*.exe` będzie zawierała wszystkie ścieżki do plików, które posiadają rozszerzenie exe. • Maska `example*` będzie zawierała wszystkie ścieżki do plików o nazwie EXAMPLE.
`-e:<seconds>`	Pliki, których skanowanie trwa dłużej niż określony limit czasu (w sekundach) są wykluczane z obszaru skanowania.
`-es:<megabytes>`	Pliki większe niż określony limit rozmiaru (w megabajtach) są wykluczane z obszaru skanowania.

Tryb zapisywania zdarzeń do pliku raportu (tylko dla profili Skanuj, Aktualizuj i Wycofaj)	
`/R:<report file>`	Zapisuje tylko krytyczne zdarzenia do pliku raportu.
`/RA:<report file>`	Zapisuje wszystkie zdarzenia do pliku raportu.

Technologie skanowania	
`/iChecker=on|off`	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).
`/iSwift=on|off`	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.

Ustawienia zaawansowane	
`/C:<file with scan settings>`	Plik z ustawieniami zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Plik należy utworzyć ręcznie i zapisać w formacie TXT. Plik może mieć następującą zawartość: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Na przykład

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Aktualizowanie baz danych i modułów aplikacji

Uruchamianie zadania *Aktualizacja baz danych i modułów aplikacji*.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Tego polecenia nie można uruchomić, jeśli aplikacja jest zainstalowana w trybie Light Agent.

Składnia polecenia

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Ustawienia zadania aktualizacji	
`local`	Uruchom zadanie *Aktualizacja baz danych i modułów aplikacji*, które zostało utworzone automatycznie po zainstalowaniu aplikacji. Możesz zmienić ustawienia zadania *Aktualizacja baz danych i modułów aplikacji* w lokalnym interfejsie aplikacji lub w konsoli Kaspersky Security Center. Jeśli to ustawienie nie zostało skonfigurowane, Kaspersky Endpoint Security uruchamia zadanie *Aktualizacja baz danych i modułów aplikacji* z domyślnymi ustawieniami lub z ustawieniami określonymi w poleceniu. Możesz skonfigurować ustawienia zadania *Aktualizacja baz danych i modułów aplikacji* w następujący sposób: • `UPDATE` uruchamia zadanie *Aktualizacja baz danych i modułów aplikacji* z ustawieniami domyślnymi: źródło uaktualnień to serwery aktualizacji Kaspersky, konto to System i inne ustawienia domyślne. • `UPDATE local` uruchamia zadanie *Aktualizacja baz danych i modułów aplikacji*, które zostało utworzone automatycznie po instalacji (predefiniowane zadanie). • `UPDATE <update settings>` uruchamia zadanie *Aktualizacja baz danych i modułów aplikacji* z ręcznie zdefiniowanymi ustawieniami (patrz poniżej).

Źródło aktualizacji	
`"<update source>"`	Adres serwera HTTP lub FTP lub folderu współdzielonego z pakietem aktualizacji. Możesz określić tylko jedno źródło uaktualnień. Jeśli źródło uaktualnień nie zostało określone, Kaspersky Endpoint Security korzysta z domyślnego źródła: serwery aktualizacji Kaspersky.

Tryb zapisywania zdarzeń do pliku raportu (tylko dla profili Skanuj, Aktualizuj i Wycofaj)	
`/R:<report file>`	Zapisuje tylko krytyczne zdarzenia do pliku raportu.
`/RA:<report file>`	Zapisuje wszystkie zdarzenia do pliku raportu.

Ustawienia zaawansowane	
`/C:<file with update settings>`	Plik z ustawieniami zadania *Aktualizacja baz danych i modułów aplikacji*. Plik należy utworzyć ręcznie i zapisać w formacie TXT. Plik może mieć następującą zawartość: `["<update source>"] [/R[A]:<report file>]`.

Na przykład

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Wycofanie ostatniej aktualizacji

Wycofanie ostatniej aktualizacji antywirusowych baz danych. Umożliwi to w razie czego wycofanie baz danych i modułów aplikacji do ich poprzedniej wersji, na przykład, gdy nowa wersja baz danych zawiera nieprawidłową sygnaturę powodującą, że Kaspersky Endpoint Security blokuje bezpieczną aplikację.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Tego polecenia nie można uruchomić, jeśli aplikacja jest zainstalowana w trybie Light Agent.

Składnia polecenia

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Tryb zapisywania zdarzeń do pliku raportu (tylko dla profili Skanuj, Aktualizuj i Wycofaj)	
`/R:<report file>`	Zapisuje tylko krytyczne zdarzenia do pliku raportu.
`/RA:<report file>`	Zapisuje wszystkie zdarzenia do pliku raportu.

Na przykład

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Śledzenie

Pliki śledzenia są przechowywane na komputerze tak długo, jak aplikacja jest używana i są trwale usuwane, gdy aplikacja jest usuwana. Pliki śledzenia, z wyjątkiem plików śledzenia Agenta autoryzacji, są przechowywane w folderze `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. Domyślnie śledzenie jest wyłączone.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Poziom śledzenia	
`<tracing level>`	Poziom szczegółowości śledzenia. Dostępne wartości: • `100` (krytyczny). Tylko wiadomości dotyczące błędów krytycznych. • `200` (wysoki). Wiadomości o wszystkich błędach, w tym błędach krytycznych. • `300` (diagnostyczny). Wiadomości o wszystkich błędach, a także ostrzeżenia. • `400` (ważny). Wszystkie wiadomości o błędach, ostrzeżenia i dodatkowe informacje. • `500` (normalny). Wiadomości o wszystkich błędach i ostrzeżeniach, a także szczegółowe informacje o działaniu aplikacji w trybie normalnym (domyślnie). • `600` (niski). Wszystkie wiadomości.

Ustawienia zaawansowane	
`all`	Uruchamia polecenie z parametrami `file` i `mem`.
`file`	Zapisuje jeden plik śledzenia (bez ograniczenia rozmiaru).
`rot`	Zapisuje ślady do ograniczonej liczby zestawów plików o ograniczonym rozmiarze i nadpisuje starsze pliki po osiągnięciu maksymalnego rozmiaru.
`mem`	Zapisuje ślady do plików zrzutów.

Na przykład

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Uruchamianie profilu

Uruchamianie profilu (na przykład, aby zaktualizować bazy danych lub włączyć składnik ochrony).

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com START <profile> [/R[A]:<report file>]
```

Profil	
`<profile>`	Nazwa profilu. *Profil* to komponent, zadanie lub funkcja Kaspersky Endpoint Security. Listę dostępnych profili można wyświetlić, wykonując polecenie `HELP START`.

Tryb zapisywania zdarzeń do pliku raportu (tylko dla profili Skanuj, Aktualizuj i Wycofaj)	
`/R:<report file>`	Zapisuje tylko krytyczne zdarzenia do pliku raportu.
`/RA:<report file>`	Zapisuje wszystkie zdarzenia do pliku raportu.

Na przykład

```
avp.com START Scan_Objects
```

STOP. Zatrzymywanie profilu

Zatrzymanie wykonywania profilu (na przykład zatrzymanie skanowania dysków wymiennych lub wyłączenie składnika ochrony).

Aby wykonać to polecenie, Ochrona hasłem musi być włączona. Użytkownik musi mieć uprawnienia **Wyłączenie składników ochrony** i **Wyłączenie składników kontroli**.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Nazwa profilu. *Profil* to komponent, zadanie lub funkcja Kaspersky Endpoint Security. Listę dostępnych profili można wyświetlić, wykonując polecenie `HELP STOP`.

Autoryzacja	
`/login=<user name> /password=<password>`	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem.

STAN. Stan profilu

Wyświetlanie informacji o stanie dla profili aplikacji (na przykład: `running` lub `completed`). Listę dostępnych profili można wyświetlić, wykonując polecenie `HELP STATUS`.

Kaspersky Endpoint Security wyświetla również informacje o stanie profili usług. Informacje o stanie profili usług mogą być wymagane podczas kontaktu z pomocą techniczną Kaspersky.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com STATUS [<profile>]
```

Jeśli wprowadzisz polecenie bez profilu, Kaspersky Endpoint Security wyświetli stan dla wszystkich profili aplikacji.

STATISTICS. Statystyki działania profilu

Wyświetlanie statystyk dotyczących profilu aplikacji (na przykład, czasu trwania skanowania lub liczby wykrytych zagrożeń). Listę dostępnych profili można wyświetlić, wykonując polecenie `HELP STATISTICS`.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com STATISTICS <profile>
```

RESTORE. Przywracanie plików z Kopii zapasowej

Przywracanie pliku z Kopii zapasowej do jego oryginalnego folderu. Jeżeli plik o tej samej nazwie istnieje już w podanej ścieżce, aplikacja poprosi o potwierdzenie, aby zastąpić plik. Przywracany plik jest kopiowany z zachowaniem oryginalnej nazwy.

Aby wykonać to polecenie, Ochrona hasłem musi być włączona. Użytkownik musi mieć uprawnienie **Przywróć z Kopii zapasowej**.

Kopia zapasowa przechowuje zapasowe kopie plików, które zostały usunięte lub zmodyfikowane podczas leczenia. *Kopia zapasowa* to kopia pliku utworzona przed wyleczeniem lub usunięciem pliku. Kopie zapasowe plików są przechowywane w specjalnym formacie i nie stanowią zagrożenia.

Kopie zapasowe plików są przechowywane w folderze `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

Użytkownicy należący do grupy Administratorzy mają nadane pełne uprawnienie dostępu do tego folderu. Ograniczone uprawnienia dostępu do tego folderu są nadawane użytkownikom, których konto zostało użyte do zainstalowania Kaspersky Endpoint Security.

Kaspersky Endpoint Security nie oferuje możliwości skonfigurowania uprawnień dostępu użytkownika do kopii zapasowych plików.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Ustawienia zaawansowane	
`/REPLACE`	Nadpisuje istniejący plik.
`<file name>`	Nazwa pliku, który ma zostać przywrócony.

Autoryzacja	
`/login=<user name> /password=<password>`	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem.

Na przykład

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Eksportowanie ustawień aplikacji

Eksportowanie ustawień Kaspersky Endpoint Security do pliku. Jeśli polecenie zawiera tylko nazwę pliku, do którego chcesz wyeksportować ustawienia, aplikacja umieści plik w następujący sposób:

- Jeśli ścieżka do avp.com zostanie dodana do zmiennej systemowej %PATH%, aplikacja umieści plik w folderze `C:\Windows\SysWOW64`.
- Jeśli uruchomisz polecenie z folderu instalacyjnego aplikacji, eksport nie powiedzie się, ponieważ autoochrona aplikacji blokuje utworzenie nowego pliku w folderze aplikacji. Aby wyeksportować ustawienia aplikacji do pliku, wprowadź ścieżkę do pliku.

Aby wykonać to polecenie, Ochrona hasłem musi być włączona. Użytkownik musi mieć uprawnienie **Eksportuj ustawienia**.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Nazwa profilu. *Profil* to komponent, zadanie lub funkcja Kaspersky Endpoint Security. Listę dostępnych profili można wyświetlić, wykonując polecenie `HELP EXPORT`.

Plik do wyeksportowania	
`<file name>`	Nazwa pliku, do którego będą eksportowane ustawienia aplikacji. Możesz także wprowadzić ścieżkę do pliku. Ustawienia Kaspersky Endpoint Security można wyeksportować do pliku konfiguracyjnego DAT lub CFG, pliku tekstowego TXT lub dokumentu XML.

Autoryzacja	
`/login=<user name> /password=<password>`	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem.

Na przykład

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Importowanie ustawień aplikacji

Importowanie ustawień Kaspersky Endpoint Security z pliku utworzonego przy użyciu polecenia `EXPORT`.

Aby wykonać to polecenie, Ochrona hasłem musi być włączona. Użytkownik musi mieć uprawnienie **Konfiguracja ustawień aplikacji**.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Plik do importu	
`<file name>`	Nazwa pliku, z którego będą importowane ustawienia aplikacji. Ustawienia Kaspersky Endpoint Security można zaimportować z pliku konfiguracyjnego DAT lub CFG, pliku tekstowego TXT lub dokumentu XML.

Autoryzacja	
`/login=<user name> /password=<password>`	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem.

Na przykład

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Zastosowanie pliku klucza

Aktywowanie Kaspersky Endpoint Security przy użyciu kodu aktywacyjnego. Jeśli aplikacja została już aktywowana, klucz zostanie dodany jako zapasowy.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Tego polecenia nie można uruchomić, jeśli aplikacja jest zainstalowana w trybie Light Agent.

Składnia polecenia

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Plik klucza	
`<file name>`	Nazwa pliku klucza.

Autoryzacja	
`/login=<user name> /password= <password>`	Dane uwierzytelniające konto użytkownika. Dane te należy wprowadzić tylko wtedy, gdy włączona jest Ochrona hasłem.

Na przykład

```
avp.com ADDKEY file.key
```

LICENSE. Licencjonowanie

Zarządzanie kluczami licencyjnymi Kaspersky Endpoint Security, EDR Optimum lub EDR Expert (Kaspersky Endpoint Detection and Response Add-on).

Aby wykonać to polecenie i usunąć klucz licencyjny, Ochrona hasłem musi być włączona. Użytkownik musi mieć uprawnienie **Usuwanie klucza**.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Tego polecenia nie można uruchomić, jeśli aplikacja jest zainstalowana w trybie Light Agent.

Składnia polecenia

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Działanie	
`/ADD <file name>`	Aktywowanie Kaspersky Endpoint Security przy użyciu kodu aktywacyjnego. Jeśli aplikacja została już aktywowana, klucz zostanie dodany jako zapasowy.
`/ADD <activation code>`	Aktywuje Kaspersky Endpoint Security przy użyciu kodu aktywacyjnego. Jeśli aplikacja została już aktywowana, klucz zostanie dodany jako zapasowy.
`/REFRESH`	Zaktualizuj stan licencji Kaspersky Endpoint Security. Dzięki temu aplikacja otrzymuje aktualne informacje o stanie licencji z serwerów aktywacyjnych Kaspersky.
`/REFRESH <license ID>`	Aktualizuj status licencji, używając numeru licencji. Za pomocą tego polecenia możesz zaktualizować status dodatku EDR, dodatku MDR, dodatku KUMA lub innych licencji. Numer licencji można uzyskać z certyfikatu licencyjnego. Dzięki temu aplikacja otrzymuje aktualne informacje o stanie licencji z serwerów aktywacyjnych Kaspersky.
`/CHECK`	Pobieranie informacji o licencji. Kaspersky Endpoint Security wyświetla informacje o wszystkich dodanych kluczach licencyjnych, w tym kluczach zapasowych, kluczach dodatku EDR, dodatku MDR, dodatku KUMA i innych kluczach. Kaspersky Endpoint Security wyświetla następujące informacje o licencji: • Nazwa licencji • Identyfikator licencji • Adres serwera ochrony (SVM), z którym połączona jest maszyna wirtualna, na której zainstalowana jest aplikacja w trybie Light Agent • Typ licencji: próbna, komercyjna, beta, subskrypcja • Data i godzina aktywacji aplikacji • Data i godzina wygaśnięcia licencji • Liczba dni pozostałych do wygaśnięcia licencji
`/CHECK <license ID>`	Uzyskaj informacje o licencji według identyfikatora. Za pomocą tego polecenia możesz uzyskać informacje o licencji. Numer licencji można uzyskać z certyfikatu licencyjnego.
`/DEL /login=<user name> /password=<password>`	Usuń klucz licencyjny aplikacji. Klucz zapasowy również zostanie usunięty.
`/DEL <license ID> /login=<user name> /password=<password>`	Usuń klucz używając numeru licencji. Za pomocą tego polecenia możesz usunąć klucz z dodatku EDR, dodatku MDR, dodatku KUMA lub innych licencji. Numer licencji można uzyskać z certyfikatu licencyjnego.

Autoryzacja	
`/login=<user name> /password=<password>`	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem.

Na przykład
```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Na przykład
```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. Kupowanie licencji

Otwieranie strony internetowej Kaspersky, na której można kupić lub odnowić licencję.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Tego polecenia nie można uruchomić, jeśli aplikacja jest zainstalowana w trybie Light Agent.

PBATESTRESET. Resetowanie wyników sprawdzania dysku przed zaszyfrowaniem dysku

Resetowanie wyników sprawdzania kompatybilności Szyfrowania całego dysku (FDE), w tym obu technologii Kaspersky Disk Encryption i Szyfrowanie dysków funkcją BitLocker.

Przed uruchomieniem Szyfrowania całego dysku aplikacja przeprowadza szereg kontroli w celu sprawdzenia, czy komputer może zostać zaszyfrowany. Jeśli komputer nie obsługuje Szyfrowania całego dysku, Kaspersky Endpoint Security rejestruje informacje o braku kompatybilności. Następnym razem, gdy spróbujesz zaszyfrować komputer, aplikacja nie wykona tego sprawdzenia i wyświetli ostrzeżenie informujące, że szyfrowanie nie jest możliwe. Jeśli konfiguracja sprzętowa komputera uległa zmianie, wyniki kontroli kompatybilności wcześniej zarejestrowane przez aplikację należy zresetować, aby ponownie sprawdzić systemowy dysk twardy pod kątem zgodności z technologiami Kaspersky Disk Encryption i Szyfrowanie dysków funkcją BitLocker.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

EXIT. Zakończenie działania aplikacji

Zakończenie działania Kaspersky Endpoint Security. Aplikacja zostanie wyładowana z pamięci RAM komputera.

Aby wykonać to polecenie, Ochrona hasłem musi być włączona. Użytkownik musi mieć uprawnienie **Zakończenie działania aplikacji**.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Wyłączanie profilu

Wyłączanie zasady Kaspersky Security Center na komputerze. Wszystkie ustawienia Kaspersky Endpoint Security są dostępne do konfiguracji, włącznie z ustawieniami, które mają zamkniętą kłódkę w profilu ( ).

Aby wykonać to polecenie, Ochrona hasłem musi być włączona. Użytkownik musi mieć uprawnienie **Wyłącz zasadę Kaspersky Security Center**.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Włączanie profilu

Włączanie zasady Kaspersky Security Center na komputerze. Ustawienia aplikacji zostaną skonfigurowane zgodnie z profilem.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

DISABLE. Wyłączanie ochrony

Wyłączanie Ochrony plików na komputerze z licencją dla Kaspersky Endpoint Security, która utraciła ważność. Nie można uruchomić tego polecenia na komputerze, na którym aplikacja nie została aktywowana lub posiada ważną licencję.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

SPYWARE. Wykrywanie oprogramowania szpiegującego

Zarządzanie wykrywaniem oprogramowania szpiegującego. Domyślnie wykrywanie programów szpiegujących jest włączone.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com SPYWARE on|off
```

KSN. Przełączanie między KSN / KPSN

Wybieranie rozwiązania Kaspersky do określania reputacji plików lub stron internetowych. Kaspersky Endpoint Security obsługuje następujące rozwiązania infrastrukturalne do pracy z bazami danych reputacji Kaspersky:

- *Kaspersky Security Network (KSN)* to rozwiązanie używane przez większość aplikacji Kaspersky. Uczestnicy KSN otrzymują informacje od firmy Kaspersky i wysyłają do Kaspersky informacje o obiektach wykrytych na komputerze użytkownika w celu dodatkowego przeanalizowania przez analityków Kaspersky i dołączenia ich do baz danych reputacji oraz statystycznych.

- *Kaspersky Private Security Network (KPSN)* to rozwiązanie, które umożliwia użytkownikom komputerów z zainstalowanym programem Kaspersky Endpoint Security lub innymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów. Sieć KPSN została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z dowolnego z następujących powodów:

  - Lokalne stacje robocze nie są połączone z internetem.

  - Przesyłanie wszelkich danych poza kraj lub poza korporacyjną sieć LAN są zabronione przez prawo lub ograniczone przez politykę bezpieczeństwa firmy.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Tego polecenia nie można uruchomić, jeśli aplikacja jest zainstalowana w trybie Light Agent.

Składnia polecenia

```
avp.com KSN /global | /private <file name>
```

Plik konfiguracyjny Kaspersky Security Network	
`<file name>`	Nazwa pliku konfiguracyjnego zawierającego ustawienia Kaspersky Private Security Network. Ten plik ma rozszerzenie PKCS7 lub PEM.

Na przykład

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Na przykład

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Wyłączanie ochrony połączenia z serwerem

Uruchamianie zadania *Ochrona połączenia z Serwerem administracyjnym*, które usuwa hasło połączenia komputera z Serwerem administracyjnym. W ten sposób zadanie wyłącza ochronę połączenia z Serwerem administracyjnym.

Aby wykonać to polecenie, Ochrona hasłem musi być włączona.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Hasło	
`/password=<password>`	Hasło konta użytkownika KL Admin lub hasło z zadania *Ochrona połączenia z Serwerem administracyjnym*. Jeśli nie określono parametru, Kaspersky Endpoint Security wyświetli monit o wprowadzenie hasła w następnym wierszu.

Polecenia KESCLI

Polecenia KESCLI umożliwiają odbieranie informacji o stanie ochrony komputera przy użyciu komponentu OPSWAT oraz umożliwiają wykonanie standardowych zadań, takich jak *Skanowanie w poszukiwaniu złośliwego oprogramowania* i *Aktualizacja baz danych i modułów aplikacji*.

Możesz przejrzeć listę poleceń KESCLI, korzystając z polecenia `kescli --help` lub używając skróconego polecenia `kescli -h`.

W celu zarządzania Kaspersky Endpoint Security z poziomu wiersza poleceń:

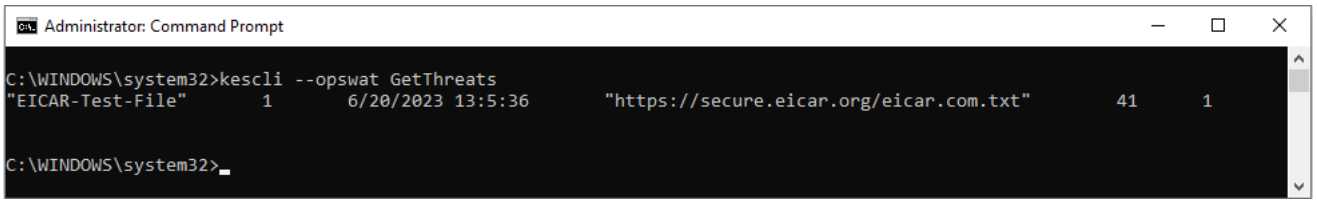
1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

   Możesz dodać ścieżkę do pliku wykonywalnego do zmiennej systemowej %PATH% podczas instalacja aplikacji.

3. Aby wykonać polecenie, użyj następującego szablonu:

```
kescli <polecenie> [options]
```

W rezultacie Kaspersky Endpoint Security wykona polecenie (patrz rysunek poniżej).



Zarządzanie aplikacją z poziomu wiersza poleceń

Scan. Skanowanie w poszukiwaniu złośliwego oprogramowania

Uruchamianie zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania* (Pełne skanowanie).

Aby uruchomić zadanie, administrator musi ustawić Zezwól na korzystanie z zadań lokalnych w zasadzie.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

Składnia polecenia

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

Możesz sprawdzić stan zakończenia zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*, korzystając z polecenia `GetScanState` i sprawdzając datę i godzinę zakończenia ostatniego skanowania przy użyciu polecenia `GetLastScanTime`.

Obszar skanowania	
`<scan scope>`	`;`-rozdzielona spacjami lista plików i folderów. Na przykład, `"C:\Program Files (x86)\Example Folder"`.

Działanie podejmowane w przypadku wykrycia zagrożenia	
`0`	**Poinformuj**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików.
`1`	**Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik. To ustawienie jest wybrane domyślnie.

Na przykład

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. Stan zakończenia skanowania

Wyświetlanie informacji o stanie zakończenia zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania* (*Pełne skanowanie*):

- `1` – skanowanie jest wykonywane.
- `0` – skanowanie nie zostało uruchomione.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

Składnia polecenia

```
kescli --opswat GetScanState
```

GetLastScanTime. Określanie czasu zakończenia skanowania

Wyświetlanie informacji o dacie i godzinie zakończenia ostatniego zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania* (*Pełne skanowanie*).

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

Składnia polecenia

```
kescli --opswat GetLastScanTime
```

GetThreats. Uzyskiwanie danych dotyczących wykrytych zagrożeń

Wyświetlanie listy wykrytych zagrożeń (*Raport o zagrożeniach*). Ten raport zawiera informacje o zagrożeniach i aktywności wirusów w ciągu ostatnich 30 dni przed utworzeniem raportu.

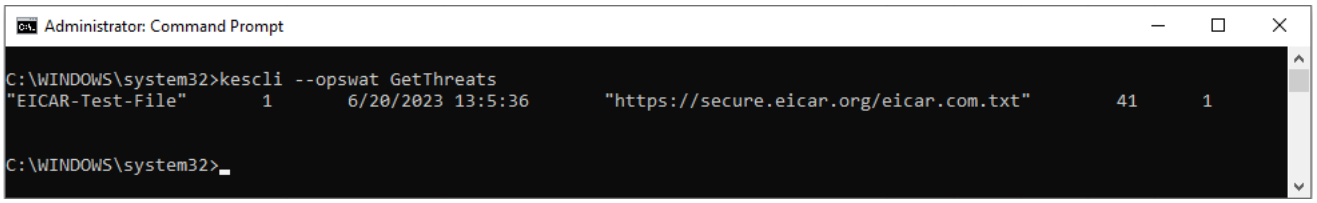
Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

Składnia polecenia

```
kescli --opswat GetThreats
```

Po wykonaniu tego polecenia, Kaspersky Endpoint Security wyśle odpowiedź w następującym formacie:

<name of detected object> <type of object> <detection date and time> <path to file> <action on threat detection> <threat danger level>



Zarządzanie aplikacją z poziomu wiersza poleceń

Typ obiektu	
0	Nieznany (Unknown).
1	Wirusy (Virware).
2	Programy typu trojan (Trojware).
3	Szkodliwe programy (Malware).
4	Programy reklamowe (Adware).
5	Auto-dialery (Pornware).
6	Aplikacje, które mogły zostać użyte przez cyberprzestępców do uszkodzenia komputera lub danych użytkownika (Riskware).
7	Obiekty spakowane, których metoda pakowania może być używana do ochrony szkodliwego kodu (Packed).
20	Nieznane obiekty (Xfiles).
21	Znane aplikacje (Software).
22	Ukryte pliki (Hidden).
23	Aplikacje wymagające uwagi (Pupware).
24	Nietypowe zachowanie (Anomaly).
30	Niezdefiniowany (Undetect).
40	Banery reklamowe (Banner).
50	Atak sieciowy (Attack).
51	Dostęp do rejestru (Registry).
52	Podejrzana aktywność (Suspicion).
60	Luki (Vulnerability).
70	Phishing (Phishing).
80	Niechciany załącznik poczty e-mail (Attachment).
90	Szkodliwe oprogramowanie wykryte przez Kaspersky Security Network (Urgent).
100	Nieznany odnośnik (Suspic URL).
110	Inne szkodliwe oprogramowanie (Behavioral).

Działanie podejmowane w przypadku wykrycia zagrożenia	
0	Nieznany (unknown).
1	Zagrożenie zostało skorygowane (ok).
2	Obiekt został zainfekowany i nie został wyleczony (infected).
5	Obiekt jest w archiwum i nie został wyleczony (archive).
9	Obiekt został wyleczony (disinfected).

10	Obiekt nie został wyleczony (`not disinfected`).
11	Obiekt został usunięty (`deleted`).
13	Utworzono kopię zapasową obiektu (`backupped`).
15	Obiekt został przeniesiony do Kopii zapasowej (`quarantined`).
23	Obiekt został usunięty po ponownym uruchomieniu komputera (`delete on reboot`).
25	Obiekt został wyleczony po ponownym uruchomieniu komputera (`disinfect on reboot`).
29	Obiekt został przeniesiony do Kopii zapasowej przez użytkownika (`added by user`).
30	Obiekt został dodany do wykluczeń (`added to exclude`).
31	Obiekt został przeniesiony do Kopii zapasowej po ponownym uruchomieniu komputera (`quarantine on reboot`).
36	Fałszywy alarm (`false alarm`).
38	Proces został przerwany (`terminated`).
40	Obiekt nie został wykryty (`not found`).
41	Nie można rozpoznać zagrożenia (`untreatable`).
42	Obiekt został przywrócony (`rolled back`).
43	Obiekt został utworzony w wyniku aktywności zagrożenia (`produced by threat`).
44	Obiekt został przywrócony po ponownym uruchomieniu komputera (`roll back on reboot`).
0xffffffff	Obiekt nie został przetworzony (`discarded`).

Poziom zagrożenia	
0	Nieznany
1	Wysoki
2	Średni
4	Niski
8	Informacja (mniej niż *Niski*)

UpdateDefinitions. Aktualizowanie baz danych i modułów aplikacji

Uruchamianie zadania *Aktualizacja baz danych i modułów aplikacji*. Kaspersky Endpoint Security korzysta z domyślnego źródła: serwery aktualizacji Kaspersky.

Aby uruchomić zadanie, administrator musi ustawić Zezwól na korzystanie z zadań lokalnych w zasadzie.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

Tego polecenia nie można uruchomić, jeśli aplikacja jest zainstalowana w trybie Light Agent.

Składnia polecenia

```
kescli --opswat UpdateDefinitions
```

Możesz przejrzeć datę i godzinę wydania bieżących baz danych antywirusów, korzystając z polecenia `GetDefinitionsetState`.

GetDefinitionState. Określenie daty i godziny ostatniej aktualizacji baz danych

Wyświetlanie informacji o dacie i godzinie ostatniej aktualizacji używanych antywirusowych baz danych.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

Składnia polecenia

```
kescli --opswat GetDefinitionState
```

EnableRTP. Włączanie ochrony

Włączanie składników ochrony Kaspersky Endpoint Security na komputerze: Ochrona plików, Ochrona WWW, Ochrona poczty, Ochrona sieci, Ochrona przed włamaniami.

> Aby włączyć składniki ochrony, administrator musi upewnić się, że odpowiednie ustawienia zasady mogą zostać zmodyfikowane (atrybuty są otwarte).

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

Składnia polecenia

```
kescli --opswat EnableRTP
```

W wyniku tego działania, składniki ochrony są włączone nawet wtedy, gdy zabroniłeś modyfikacji ustawień aplikacji z użyciem Ochrony hasłem.

Możesz sprawdzić stan działania Ochrony plików, korzystając z polecenia `GetRealTimeProtectionState`.

GetRealTimeProtectionState. Stan Ochrony plików

Wyświetlanie informacji o stanie działania komponentu Ochrona plików:

- `1` – komponent jest włączony.
- `0` – komponent jest wyłączony.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

Składnia polecenia

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Stan szyfrowania dysku

Wyświetlanie informacji o stanie zaszyfrowania dysku:

- `1` oznacza, że dysk jest chroniony przez Kaspersky lub technologię szyfrowania dysków BitLocker.
- `0` oznacza, że dysk nie jest szyfrowany.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

Składnia polecenia

```
kescli --opswat GetEncryptionState
```

Version. Identyfikowanie wersji aplikacji

Wyświetlanie wersji Kaspersky Endpoint Security for Windows.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

Składnia polecenia

```
kescli --Version
```

Możesz także użyć skróconego polecenia `-v`.

Polecenia zarządzania Detection and Response

Możesz użyć wiersza polecenia do zarządzania wbudowaną funkcjonalnością rozwiązań Detection and Response (na przykład, Kaspersky Sandbox lub Kaspersky Endpoint Detection and Response Optimum). Możesz zarządzać rozwiązaniami Detection and Response, jeśli zarządzanie przy użyciu konsoli Kaspersky Security Center nie jest możliwe. Możesz wyświetlić listę poleceń do zarządzania aplikacją, uruchamiając polecenie `HELP`. Aby zapoznać się z informacjami o składni konkretnego polecenia, wpisz `HELP <command>`.

W celu zarządzania wbudowanymi funkcjami rozwiązań Detection and Response przy użyciu wiersza poleceń:

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.
3. Aby wykonać polecenie, użyj następującego szablonu:

   ```
   avp.com <command> [options]
   ```

   W rezultacie Kaspersky Endpoint Security wykona polecenie.

SANDBOX. Zarządzanie Sandbox

Polecenia do zarządzania komponentem Sandbox:

- Włączanie lub wyłączanie komponentu Sandbox.

  Komponenty Sandbox umożliwiają interakcję z rozwiązaniem Kaspersky Sandbox i komponentem KATA Sandbox, który jest częścią Kaspersky Anti Targeted Attack Platform.

- Skonfigurowanie komponentu Kaspersky Sandbox:

  - Podłączanie komputera do serwerów Sandbox.

    Serwery używają wdrożonych obrazów wirtualnych systemów operacyjnych Microsoft Windows do uruchamiania obiektów, które muszą zostać przeskanowane. Możesz wprowadzić adres IP (IPv4 lub IPv6) lub w pełni kwalifikowaną nazwę domeny. Aby uzyskać szczegółowe informacje na temat wdrażania obrazów wirtualnych i konfigurowania serwerów Sandbox, zapoznaj się z informacjami zawartymi w Systemie pomocy dla Kaspersky Sandbox i Systemie pomocy dla Kaspersky Anti Targeted Attack Platform.

  - Konfigurowanie limitu czasu połączenia dla serwera.

    Przekroczono limit czasu połączenia dla serwera Sandbox (dla komponentu Kaspersky Sandbox) lub serwera Central Node (dla komponentu KATA). Po skonfigurowaniu upłynięcia określonej ilości czasu, Kaspersky Endpoint Security wyśle żądanie do następnego serwera. Możesz zwiększyć limit czasu połączenia dla serwera, jeśli prędkość Twojego połączenia spada lub jeśli połączenie jest niestabilne. Zalecany limit czasu żądania wynosi 0,5 sekundy lub mniej.

  - Konfigurowanie zaufanego połączenia między komputerem a serwerami.

    Aby skonfigurować zaufane połączenie z serwerem Sandbox (dla komponentu Kaspersky Sandbox) lub serwerem Central Node (dla komponentu KATA), należy przygotować certyfikat TLS. Następnie należy dodać certyfikat do komputera, stosując zasady. Należy również dodać certyfikat do serwera Sandbox (dla komponentu Kaspersky Sandbox) lub serwera Central Node (dla komponentu KATA).

  - Konfigurowanie trybu integracji.

    Należy wybrać rozwiązanie, którego częścią jest funkcja Sandbox, np. Kaspersky Sandbox lub KATA Sandbox. *Kaspersky Sandbox* jest samodzielnym rozwiązaniem typu Detection and Response firmy Kaspersky. *KATA Sandbox* jest komponentem rozwiązania Kaspersky Anti Targeted Attack Platform. Po zintegrowaniu z KATA Sandbox komponent może działać w następujących trybach:

    - **Ręcznie**. Użytkownik ręcznie przesyła plik do skanowania z menu kontekstowego (**Wyślij do Sandbox**).
    - **Automatycznie**. Aplikacja automatycznie wykrywa obiekty i przesyła je do Sandboxa w celu zeskanowania.
    - **Powiązany**.

- Wyświetlanie bieżących ustawień komponentu.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

Działanie	
`stop`	Wyłącza komponent Sandbox.
`start`	Włącza komponent Sandbox.
`set`	Konfiguruje komponent Sandbox. Możesz zmodyfikować następujące ustawienia: • Dodaj serwery Sandbox (`--servers`) • Dodaj certyfikat TLS (`--pinned-certificate`) • Dodaj kontener szyfrowania (`--client-certificate`) • Podaj hasło do kontenera kryptograficznego (`--client-certificate-password`); • Skonfiguruj limit czasu połączenia z serwerem (`--timeout`) • Wybierz tryb integracji (`--mode`): • `KSB` – integracja z Kaspersky Sandbox; • `KATAManual` – ręczna integracja z KATA Sandbox; • `KATAAuto` – automatyczna integracja z KATA Sandbox; • `KATAFull` – łączona integracja z KATA Sandbox.

`show`	Wyświetla bieżące ustawienia komponentu. Otrzymasz następującą odpowiedź:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Autoryzacja	
`/login=<user name> /password=<password>`	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem.

Na przykład

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB /login=login /password=password
```

PREVENTION. Zarządzanie zapobieganiem wykonaniu

Wyłączanie komponentu Zapobieganie wykonywaniu lub wyświetlanie bieżących ustawień komponentu, łącznie z listą reguł zapobiegania wykonywaniu.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com prevention disable
```

```
avp.com prevention /show
```

Po wykonaniu polecenia `prevention /show` uzyskasz następującą odpowiedź:

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

Wartości zwrotne polecenia:

- `-1` oznacza, że polecenie nie jest obsługiwane przez wersję aplikacji, która jest zainstalowana na komputerze.
- `0` oznacza, że polecenie zostało wykonane pomyślnie.
- `1` oznacza, że obowiązkowy argument nie został przekazany do polecenia.
- `2` oznacza, że wystąpił ogólny błąd.
- `4` oznacza, że wystąpił błąd składniowy.
- `9` – błędna operacja (na przykład, próba wyłączenia komponentu, gdy jest już wyłączony).

ISOLATION. Zarządzanie Izolacją sieci

Wyłączanie Izolacji od sieci komputera lub wyświetlanie bieżących ustawień komponentu. Ustawienia komponentu zawierają także listę połączeń sieciowych dodanych do wykluczeń.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

W wyniku uruchomienia polecenia `stat` otrzymujesz następującą odpowiedź: `Network isolation on|off`.

RESTORE. Przywracanie plików z Kwarantanny

Przywracanie pliku z kwarantanny do jego oryginalnego folderu. *Kwarantanna* to specjalny lokalny magazyn na komputerze. Użytkownik może poddać kwarantannie pliki, które użytkownik uznaje za niebezpieczne dla komputera. Pliki poddane kwarantannie są przechowywane w postaci zaszyfrowanej i nie zagrażają bezpieczeństwu urządzenia. Kaspersky Endpoint Security używa Kwarantanny tylko w przypadku integracji z rozwiązaniami Kaspersky Detection and Response. W innych przypadkach Kaspersky Endpoint Security umieszcza odpowiedni plik w Kopii zapasowej. Więcej informacji na temat zarządzania Kwarantanną jako częścią rozwiązań można znaleźć w pomocy dla Kaspersky Sandbox, pomocy dla Kaspersky Endpoint Detection and Response Optimum, pomocy dla Kaspersky Endpoint Detection and Response Expert, pomocy dla Kaspersky Anti Targeted Attack Platform i pomocy dla Kaspersky Endpoint Detection and Response Expert (on-premises).

Aby wykonać to polecenie, Ochrona hasłem musi być włączona. Użytkownik musi mieć uprawnienie **Przywróć z Kopii zapasowej**.

Obiekt jest poddawany kwarantannie z poziomu konta systemowego (SYSTEM).

Przywracanie plików z kwarantanny wiąże się z następującymi specjalnymi kwestiami:

- Jeżeli folder docelowy został usunięty lub użytkownik nie ma uprawnień dostępu do tego folderu, aplikacja umieszcza plik w folderze `%DataRoot%\QB\Restored`. Następnie ręcznie przenieś plik do folderu docelowego.
- Aplikacja traktuje nazwę przywracanego pliku z uwzględnieniem wielkości liter. Jeśli nie zauważysz przypadku podczas wpisywania nazwy pliku, aplikacja nie przywróci pliku.
- Jeśli w folderze docelowym znajduje się już plik o tej samej nazwie, aplikacja anuluje przywracanie pliku.
- Jeśli używasz rozwiązania KATA (EDR), po przywróceniu pliku aplikacja zapisuje jego kopię w Kwarantannie. Możesz ręcznie wyczyścić Kwarantannę. W przypadku rozwiązań EDR Optimum i EDR Expert aplikacja usuwa plik po przywróceniu.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Ustawienia zaawansowane	
`/REPLACE`	Nadpisuje istniejący plik.
`<file name>`	Nazwa pliku, który ma zostać przywrócony.

Autoryzacja	
`/login=<user name> /password=<password>`	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem.

Na przykład

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

Wartości zwrotne polecenia:

- `-1` oznacza, że polecenie nie jest obsługiwane przez wersję aplikacji, która jest zainstalowana na komputerze.
- `0` oznacza, że polecenie zostało wykonane pomyślnie.
- `1` oznacza, że obowiązkowy argument nie został przekazany do polecenia.
- `2` oznacza, że wystąpił ogólny błąd.
- `4` oznacza, że wystąpił błąd składniowy.

IOCSCAN. Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa (IOC)

Uruchamianie zadania *Skanowanie IOC*. *Wskaźnik naruszeń bezpieczeństwa (IOC)* to zestaw danych dotyczących obiektu lub aktywności, która wskazuje nieautoryzowany dostęp do komputera (naruszenie bezpieczeństwa danych). Na przykład, wiele niepomyślnych prób zalogowania do systemu może stanowić wskaźnik naruszeń bezpieczeństwa. Zadanie *Skanowanie IOC* umożliwia odszukanie wskaźników naruszeń bezpieczeństwa na komputerze i podejmują środki reakcji na zagrożenia.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Skanowanie IOC jest przerywane po znalezieniu 128 elementów ze wskaźnikami zagrożenia opisanymi w plikach IOC. Jest to konieczne, aby ograniczyć liczbę wpisów w raporcie zadania skanowania IOC i ułatwić jego analizę, a także zapobiec przepełnieniu raportu nieprecyzyjnie sformułowanymi wskaźnikami zagrożenia generującymi ogromną liczbę znalezionych elementów.

Składnia polecenia

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full
path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off]
[/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=
<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

Pliki IOC	
`<full path to the IOC file>`	Pełna ścieżka do pliku IOC, którego chcesz użyć do skanowania. Możesz określić kilka plików IOC oddzielonych spacjami. Pełna ścieżka do pliku IOC musi zostać wprowadzona bez argumentu `/path`. Na przykład: `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	Ścieżka do folderu z plikami IOC, których chcesz użyć do skanowania. *Pliki IOC* to pliki zawierające zestawy wskaźników, które aplikacja próbuje dopasować do licznika wykrywania. Pliki IOC muszą pasować do standardu OpenIOC. Na przykład: `C:\Users\Admin\Desktop\IOC`

Typ danych skanowania IOC	
`/process=on|off`	Analizuje dane procesu podczas wykonywania skanowania IOC (warunek ProcessItem). Jeśli wartość argumentu to `off`, Kaspersky Endpoint Security nie analizuje procesów uruchamianych na komputerze podczas wykonywania skanowania. Jeśli plik IOC zawiera warunki IOC dokumentu ProcessItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane procesu tylko wtedy, gdy dokument ProcessItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.
`/hint=<full path to the executable file of the process|full path to the file>`	Analizuje dane plików podczas wykonywania skanowania IOC (warunki ProcessItem i FileItem). Możesz wybrać plik na jeden z następujących sposobów: • `<full path to the executable file of the process>` — warunek ProcessItem; • `<full path to the file>` — warunek FileItem.
`/registry=on|off`	Analizuje dane rejestru systemu Windows podczas wykonywania skanowania IOC (warunek RegistryItem). Jeśli wartość argumentu to `off`, Kaspersky Endpoint Security nie skanuje rejestru systemu Windows. Jeśli plik IOC zawiera warunki dokumentu RegistryItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje rejestr systemu Windows tylko wtedy, gdy dokument RegistryItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania. Dla typów danych RegistryItem Kaspersky Endpoint Security skanuje zestaw kluczy rejestru.
`/dnsentry=on|off`	Analizuje dane dotyczące wpisów w lokalnej pamięci podręcznej DNS podczas wykonywania skanowania IOC (warunek DnsEntryItem). Jeśli wartość argumentu to `off`, Kaspersky Endpoint Security nie skanuje lokalnej pamięci podręcznej DNS. Jeśli plik IOC zawiera warunki dokumentu DnsEntryItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje lokalną pamięć podręczną DNS tylko wtedy, gdy dokument DnsEntryItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.
`/arpentry=on|off`	Analizuje dane dotyczące wpisów w tabeli ARP podczas wykonywania skanowania IOC (warunek ArpEntryItem). Jeśli wartość argumentu to `off`, Kaspersky Endpoint Security nie skanuje tabeli ARP. Jeśli plik IOC zawiera warunki dokumentu ArpEntryItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje tabelę ARP tylko wtedy, gdy dokument ArpEntryItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.
`/ports=on|off`	Analizuje dane dotyczące portów otwartych do nasłuchiwania podczas wykonywania skanowania IOC (warunek PortItem). Jeśli wartość argumentu to `off`, Kaspersky Endpoint Security nie skanuje tabeli aktywnych połączeń na urządzeniu. Jeśli plik IOC zawiera warunki dokumentu PortItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje tabelę aktywnych połączeń tylko wtedy, gdy dokument PortItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.
`/services=on|off`	Analizuje dane dotyczące usług zainstalowanych na urządzeniu podczas wykonywania skanowania IOC (warunek ServiceItem). Jeśli wartość argumentu to `off`, Kaspersky Endpoint Security nie skanuje danych dotyczących usług zainstalowanych na urządzeniu. Jeśli plik IOC zawiera warunki dokumentu ServiceItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane usługi tylko wtedy, gdy dokument ServiceItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.

`/system=on|off`	Analizuje dane środowiskowe podczas wykonywania skanowania IOC (warunek SystemInfoItem). Jeśli wartość argumentu to `off`, Kaspersky Endpoint Security nie analizuje danych środowiskowych. Jeśli plik IOC zawiera warunki dokumentu SystemInfoItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane środowiskowe tylko wtedy, gdy dokument SystemInfoItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.
`/users=on|off`	Analizuje dane dotyczące użytkowników podczas wykonywania skanowania IOC (warunek UserItem). Jeśli wartość argumentu to `off`, Kaspersky Endpoint Security nie analizuje danych dotyczących użytkowników utworzonych w systemie. Jeśli plik IOC zawiera warunki dokumentu UserItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane dotyczące użytkowników tworzonych w systemie tylko wtedy, gdy dokument UserItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.
`/volumes=on|off`	Analizuje dane dotyczące woluminów podczas wykonywania skanowania IOC (warunek VolumeItem). Jeśli wartość argumentu to `off`, Kaspersky Endpoint Security nie skanuje danych dotyczących woluminów na urządzeniu. Jeśli plik IOC zawiera warunki dokumentu VolumeItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane woluminów tylko wtedy, gdy dokument VolumeItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.
`/eventlog=on|off`	Analizuje dane dotyczące wpisów w Dzienniku zdarzeń systemu Windows podczas wykonywania skanowania IOC (warunek EventLogItem). Jeśli wartość argumentu to `off`, Kaspersky Endpoint Security nie skanuje wpisów w Dzienniku zdarzeń systemu Windows. Jeśli plik IOC zawiera warunki dokumentu EventLogItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje Dziennik zdarzeń systemu Windows tylko wtedy, gdy dokument EventLogItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.
`/datetime=<event publication date>`	Należy wziąć pod uwagę datę opublikowania zdarzenia w Dzienniku zdarzeń systemu Windows podczas określania obszaru skanowania IOC dla odpowiedniego dokumentu IOC. Podczas wykonywania skanowania IOC, Kaspersky Endpoint Security skanuje wpisy w Dzienniku zdarzeń systemu Windows opublikowane w trakcie czasu od określonej godziny i daty do momentu, gdy zadanie jest uruchomione. Kaspersky Endpoint Security umożliwia określenie daty publikacji zdarzenia jako wartości argumentu. Skanowanie jest wykonywane tylko dla zdarzeń opublikowanych w Dzienniku zdarzeń systemu Windows po określonej dacie, a przed uruchomieniem skanowania. Jeśli argument nie jest określony, Kaspersky Endpoint Security skanuje zdarzenia z dowolną datą publikacji. Ustawienia `TaskSettings::BaseSettings::EventLogItem::datetime` nie można edytować. Ustawienie jest używane tylko wtedy, gdy dokument EventLogItem IOC został opisany w pliku IOC dostarczonym do przeskanowania.
`/channel=<list of channels>`	Lista nazw kanałów (dziennik), dla których chcesz wykonać skanowanie IOC. Jeśli argument został określony, Kaspersky Endpoint Security skanuje wpisy opublikowane w określonych dziennikach. Dokument IOC musi zawierać opisany warunek EventLogItem. Nazwa dziennika jest określona jako ciąg znaków zgodnie z nazwą dziennika (kanału), określonego we właściwościach dziennika (parametr Full Name) lub we właściwościach zdarzenia (parametr `<Channel></Channel>` w schemacie xml zdarzenia). Możesz określić kilka kanałów oddzielonych spacjami. Jeśli argument nie został określony, Kaspersky Endpoint Security skanuje wpisy dla kanałów `Application`, `System`, `Security`.
`/files=on|off`	Analizuje dane plików podczas wykonywania skanowania IOC (warunek FileItem). Jeśli wartość argumentu to `off`, Kaspersky Endpoint Security nie analizuje danych plików. Jeśli plik IOC zawiera warunki dokumentu FileItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane plików tylko wtedy, gdy dokument FileItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.

`/drives=<all|system|critical|custom>`	Ustawia obszar skanowania IOC podczas analizowania danych dla dokumentu FileItem IOC. Możesz ustawić następujące wartości dla obszaru skanowania: • `<all>` dla wszystkich dostępnych obszarów plików. • `<system>` dla plików w folderach, w których zainstalowany jest system operacyjny. • `<critical>` dla plików tymczasowych w folderach użytkownika i systemowych. • `<custom>` dla plików w obszarach zdefiniowanych przez użytkownika (`/scope=<list of folders to scan>`). Jeśli argument nie został określony, wykonywanie jest skanowanie obszarów krytycznych.
`/excludes=<list of exclusions>`	Ustawia obszar wykluczeń podczas analizowania danych dla dokumentu FileItem IOC. Możesz określić kilka ścieżek oddzielonych spacjami.
`/scope=<list of folders to scan>`	Obszar skanowania IOC zdefiniowany przez użytkownika podczas analizowania danych dla dokumentu FileItem IOC (`/drives=custom`). Możesz określić kilka ścieżek oddzielonych spacjami.
`/retro /<number of days>`	*Retrospektywne skanowanie IOC* jest trybem zadania *Skanowanie IOC*, w ramach którego Kaspersky Endpoint Security skanuje dane w poszukiwaniu oznak naruszenia bezpieczeństwa przez określony czas. Tryb ten jest przeznaczony do wyszukiwania wskaźników zagrożenia na podstawie danych telemetrycznych chronionego komputera, takich jak aktywność sieciowa, procesy, pliki i inne dane telemetryczne. Można ustawić okres od 1 do 14 dni. Domyślnie aplikacja przez jeden dzień skanuje w poszukiwaniu wskaźników naruszeń bezpieczeństwa.
`/network=on|off`	Analiza danych sieciowych (warunek NetworkItem).
`/url=on|off`	Analiza danych w dziennikach przeglądarki (warunek UrlHistoryItem). Retrospektywne skanowanie IOC analizuje logi następujących przeglądarek: Google Chrome, Mozilla Firefox, Microsoft Edge (wersja 79 lub nowsza).
`/email`	Analiza obiektów pocztowych (warunek EmailItem).
`/route`	Analiza tablic routingu i przekazywania (warunek RouteEntryItem).

Wartości zwrotne polecenia:

- `-1` oznacza, że polecenie nie jest obsługiwane przez wersję aplikacji, która jest zainstalowana na komputerze.
- `0` oznacza, że polecenie zostało wykonane pomyślnie.
- `1` oznacza, że obowiązkowy argument nie został przekazany do polecenia.
- `2` oznacza, że wystąpił ogólny błąd.
- `4` oznacza, że wystąpił błąd składniowy.

Jeśli polecenie zostało wykonane pomyślnie (wartość zwrotna `0`) i wykryto wskaźniki naruszeń bezpieczeństwa, Kaspersky Endpoint Security zwróci do wiersza poleceń następujące informacje o wyniku wykonania zadania:

`Uuid`	ID pliku IOC z nagłówka struktury pliku IOC (znacznik `<ioc id="">`)
`Name`	Opis pliku IOC z nagłówka struktury pliku IOC (znacznik `<description></description>`)
`Matched Indicator Items`	Lista identyfikatorów wszystkich dopasowanych wskaźników.
`Matched objects`	Dana każdego dokumentu IOC, dla których było dopasowanie.

MDRLICENSE. Aktywacja MDR

Dodawanie pliku konfiguracyjnego BLOB, aby aktywować Managed Detection and Response. Plik BLOB zawiera ID klienta oraz informacje o licencji dla Kaspersky Managed Detection and Response. Plik BLOB znajduje się w archiwum ZIP pliku konfiguracyjnego MDR. Archiwum ZIP możesz uzyskać w Kaspersky Managed Detection and Response Console. Więcej informacji o pliku BLOB można znaleźć w pomocy dla Kaspersky Managed Detection and Response.

Uprawnienia administratora są wymagane do wykonania działań na pliku BLOB. Ustawienia Managed Detection and Response w zasadzie muszą być także dostępne do edycji ( ).

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Działanie	
`/ADD <file name>`	Zastosuj plik konfiguracyjny BLOB do integracji z Kaspersky Managed Detection and Response (format pliku P7). Możesz zastosować tylko jeden plik BLOB. Jeśli plik BLOB został już dodany do komputera, plik zostanie zastąpiony.
`/DEL`	Usuń plik konfiguracyjny BLOB.

Autoryzacja	
`/login=<user name> /password=<password>`	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem.

Na przykład

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

Na przykład

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. Integracja z EDR (KATA)

Polecenia do zarządzania komponentem Endpoint Detection and Response (KATA):

- Włączanie lub wyłączanie komponent EDR (KATA).

  Komponent EDR (KATA) zapewnia współdziałanie z rozwiązaniem Kaspersky Anti Targeted Attack Platform.

- Konfigurowanie połączenia z serwerami Kaspersky Anti Targeted Attack Platform.
- Wyświetlanie bieżących ustawień komponentu.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

Działanie	
`stop`	Wyłącz komponent EDR (KATA).
`start`	Włącz komponent EDR (KATA).
`set`	Skonfiguruj komponent EDR (KATA). Możesz zmodyfikować następujące ustawienia: • Dodaj serwery węzła centralnego (`servers=<server address>:<port>`) • Dodaj certyfikat TLS (`server-certificate=<path to the TLS certificate>`) • Ustaw limit czasu połączenia z serwerem Central Node (`/timeout=<Central Node server connection timeout (s)>`) • Ustaw okres synchronizacji z serwerem Central Node (`/sync-period=<Central Node server synchronization period (min)>`)
`show`	Wyświetla bieżące ustawienia komponentu.

KUMA. Integracja z KUMA

Polecenia zarządzania wbudowanym agentem KUMA:

- Włączanie lub wyłączanie integracji KUMA.

  Wbudowany agent KUMA zapewnia współpracę z rozwiązaniem Kaspersky Unified Monitoring and Analysis Platform.
- Konfigurowanie połączenia z serwerami Kaspersky Unified Monitoring and Analysis Platform.
- Wyświetlanie bieżących ustawień komponentu.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-
password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

Działanie	
`stop`	Wyłącz integrację KUMA.
`start`	Włącz integrację KUMA.
`set`	Skonfiguruj wbudowanego agenta KUMA. Możesz zmodyfikować następujące ustawienia: • Dodaj serwery KUMA (`/servers=<protocol>://<server address>:<port>`) Aplikacja obsługuje następujące protokoły połączeń serwerowych: `tcp`, `udp`, `http`, `https`. • Dodaj certyfikat TLS (`/server-certificate=<path to the TLS certificate>`) • Skonfiguruj limit czasu połączenia z serwerem (`/timeout=<KUMA server connection timeout (s)>`) • Dodaj kontener szyfrowania (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`) • Skonfiguruj opóźnienie transmisji zdarzeń (`/maximum-data-transfer-time=<maximum events transmission delay (sec)`)
`show`	Wyświetla bieżące ustawienia komponentu.

Autoryzacja	
`/login=<user name> /password=<password>`	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem.

Na przykład

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

YARA. Uruchamianie skanowania YARA

Uruchomienie zadania *Uruchom skanowanie YARA*. Aplikacja skanuje pliki i obiekty w poszukiwaniu wskaźników ukierunkowanych ataków na infrastrukturę informatyczną przedsiębiorstwa, wykorzystując do tego celu bazy reguł YARA. *Zasady YARA* są opisami sygnatur ukierunkowanych ataków i włamań do korporacyjnej infrastruktury IT, których Kaspersky Endpoint Security używa do skanowania obiektów.

Aby uruchomić skanowanie YARA, należy przygotować pliki YARA opisujące reguły. Tworząc pliki YARA, należy wziąć pod uwagę następujące wymagania:

- Kaspersky Endpoint Security obsługuje pliki YARA z rozszerzeniami .YARA lub .YAR, które są zgodne z otwartym standardem YARA 4.2.3 w zakresie opisu wskaźników naruszenia.
- Dla zadania można określać tylko pliki z regułami YARA. Zadanie *Uruchom skanowanie YARA* nie obsługuje innych typów reguł.
- Jeśli dodano pliki YARA, których Kaspersky Endpoint Security nie obsługuje, lub reguły zawierają błędy składniowe, zadanie zostanie przerwane i wyświetlony zostanie odpowiedni komunikat o błędzie.
- Identyfikatory wszystkich plików YARA używane w pojedynczym zadaniu muszą być unikatowe. Jeśli istnieją pliki YARA z takim samym identyfikatorem, mogą wpłynąć na wyniki wykonania zadania.
- Skanowanie YARA jest przerywane po znalezieniu 128 elementów pasujących do wskaźników opisanych w regułach YARA. Jest to konieczne, aby ograniczyć liczbę wpisów w raporcie zadania skanowania YARA i ułatwić jego analizę, a także zapobiec przepełnieniu raportu nieprecyzyjnie sformułowanymi wskaźnikami zagrożenia YARA generującymi ogromną liczbę znalezionych elementów.

Kaspersky zaleca utworzenie jednej reguły na każdy plik YARA. Dzięki temu wyniki skanowania będą bardziej czytelne.

Skanowanie YARA może zająć sporo czasu. W zależności od rozmiaru dysku, ustawień zadania i liczby obiektów na dysku, skanowanie YARA może trwać od kilku minut do kilku godzin. Aplikacja nie wyświetla wskaźnika postępu. Nie można zatrzymać ani anulować skanowania YARA. Zalecamy poczekać na wyniki skanowania YARA.

Składnia polecenia

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

Pliki YARA	
`<full path to the YARA file>`	Pełna ścieżka do pliku YARA, którego chcesz użyć do skanowania. Możesz określić kilka plików YARA oddzielonych spacjami. Wymagany argument, jeśli wartość `/path=<path to the folder with YARA files>` nie jest określona. Na przykład: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/path=<path to the folder with YARA files>`	Pełna ścieżka do folderu z plikami YARA, których chcesz użyć do skanowania. Wymagany argument, jeśli wartość `<full path to the YARA file>` nie jest określona. Na przykład: `/path=C:\Users\Admin\Desktop\YARA`

Ustawienia zaawansowane	
`/fastScan=<on|off>`	Szybkie skanowanie YARA. Dla każdego obiektu aplikacja rejestruje jedno wystąpienie wykrytego wskaźnika. Aplikacja ukrywa również duplikaty wykrytych wskaźników w dzienniku. Szybkie skanowanie YARA umożliwia szybsze skanowanie dużych plików. Jeżeli to ustawienie nie zostanie określone, aplikacja wykona standardowe skanowanie YARA. W tym trybie aplikacja rejestruje duplikaty wykrytych wskaźników.
`/maxRules=<maximum number of scan rules>`	Limit liczby unikalnych wyzwolonych reguł, po którego osiągnięciu aplikacja zatrzymuje skanowanie YARA. Jeżeli wartość tego ustawienia nie jest określona lub jeżeli `0` jest określony, aplikacja wykonuje skanowanie YARA bez ograniczeń.

`/timeOut=<stop scan after the specified time in seconds>`	Ile czasu może zająć skanowanie YARA (w sekundach). Po upływie tego czasu aplikacja zatrzyma skanowanie YARA. Jeżeli wartość tego ustawienia nie jest określona lub jeżeli `0` jest określony, aplikacja wykonuje skanowanie YARA bez ograniczeń.
`/recursive=<on|off>`	Ten argument rozpoczyna cykliczne skanowanie podfolderów w zakresie Skanowania obiektów `/scanFolders`.
`/scanFolders=<list of folders to be scanned>`	Ten argument rozpoczyna skanowanie YARA plików w folderach na określonej liście. Możesz podać kilka wartości oddzielonych spacjami. Kaspersky Endpoint Security obsługuje znaki `*` i `?` podczas wprowadzania maski ścieżki folderu. Jeśli to ustawienie nie zostanie określone, aplikacja przeprowadzi skanowanie YARA wszystkich dysków lokalnych z wyjątkiem udziałów sieciowych, dysków w chmurze i nośników wymiennych.
`/scanMemory=<on|off>`	Przeskanuj pamięć wszystkich uruchomionych procesów.
`/scanProcess=<process name>`	Skanuj pamięć tylko pod kątem określonych procesów. Podaj pełne ścieżki do plików wykonywalnych procesów oddzielone spacjami. Możesz również użyć znaków `*` i `?` do wprowadzenia maski.
`/maxSize=<file size in bytes>`	Ogranicz rozmiar pliku dla skanowania YARA. Aplikacja pomija większe pliki.
`/includes=<list of objects to be scanned>>`	Modyfikowanie obszaru skanowania. Możesz podać kilka wartości oddzielonych spacjami. Dostępne są następujące wartości: • Nazwa pliku • Rozszerzenie pliku Zakres skanowania musi być określony za pomocą parametru `/scanFolders`. Na przykład: `/scanFolders C:\*.* /includes=*.exe *.dll` – aplikacja skanuje wszystkie pliki z rozszerzeniami .EXE i .DLL na dysku C.
`/excludes=<list of objects to be scanned>`	Wykluczanie plików ze skanowania YARA. Możesz podać kilka wartości oddzielonych spacjami. Dostępne są następujące wartości: • Ścieżka pliku • Maska ścieżki pliku Wykluczenia muszą być określone za pomocą parametru `/scanFolders`. Na przykład: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – aplikacja pomija plik readme.txt, wszystkie pliki z folderu C:\trusted oraz wszystkie pliki z rozszerzeniem .XML w folderze głównym na dysku C.
`/scanAutoruns=<on|off>`	Skanowanie YARA punktowych obiektów automatycznego uruchamiania.
`/excludeAutoruns=<list of autorun point areas to skip>`	Wykluczanie automatycznie uruchamianych obiektów z zakresu skanowania. Podaj pełne ścieżki do plików wykonywalnych procesów oddzielone spacjami. Możesz również użyć znaków `*` i `?` do wprowadzenia maski.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Jeżeli podasz ścieżkę do folderu, aplikacja zapisze wyniki skanowania w podanej ścieżce w pliku o nazwie yara_<nazwa komputera>_<czas zakończenia skanowania>.txt. Jeśli podasz ścieżkę do konkretnego pliku TXT, aplikacja zapisze w nim wyniki skanowania. Na przykład: `/logFolder=C:\test` lub `/logFolder=C:\test\abc.txt`. Wyniki skanowania są wyświetlane w wierszu poleceń niezależnie od tego, czy określono opcję `/logFolder`.

Wartości zwrotne polecenia:

- `-1` oznacza, że polecenie nie jest obsługiwane przez wersję aplikacji, która jest zainstalowana na komputerze.
- `0` oznacza, że polecenie zostało wykonane pomyślnie.
- `1` oznacza, że obowiązkowy argument nie został przekazany do polecenia.
- `2` oznacza, że wystąpił ogólny błąd.
- `4` oznacza, że wystąpił błąd składniowy.
- `5` oznacza, że nie znaleziono jednego lub więcej plików z regułami YARA określonymi w parametrze.

Jeśli polecenie zostało wykonane pomyślnie (wartość zwrotna `0`) i wykryto wskaźniki naruszeń bezpieczeństwa, Kaspersky Endpoint Security zwróci do wiersza poleceń następujące informacje o wyniku wykonania zadania:

`Started at <time>` `Finished at <time>`	Czas rozpoczęcia i czas zakończenia skanowania.
`Host name: <computer name>`	Nazwa komputera, na którym wykryto obiekt.
`Result: <error>`	Kod błędu, który wystąpił podczas wykonywania zadania. Jeżeli nie ma błędów, aplikacja ustawia na wyjściu `0x00000000`.
`Comment: <comment text>`	Opis błędu, który wystąpił podczas wykonywania zadania. Na przykład, `Operation timeout`.
`Object Name:` lub `Process:` (podczas skanowania pamięci procesu)	Nazwa obiektu lub procesu, który wyzwolił regułę YARA.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Skróty obiektu, który wyzwolił regułę YARA.
`Rule Name`	Nazwa wyzwolonej reguły YARA.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Metadane określone w regule YARA.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	W obiekcie znaleziono elementy spełniające warunki reguły YARA:
	• Offset w pamięci procesu lub pliku, w którym wykryto pasujący element (`Offset`).
	• Nazwa pasującego ciągu w regule YARA (`String name`).
	• Pasujący ciąg w pamięci procesu lub pliku (`String data`).

TELEMETRYFILTERS. Filtrowanie zdarzeń, które mają zostać wysłane do KUMA

Wysyłanie zdarzeń na serwer KUMA jest domyślnie wyłączone. Aby zapewnić poprawne działanie serwera KUMA, należy włączyć wysyłanie danych telemetrycznych. Można wybrać źródło zdarzeń spośród standardowych dzienników: *Application*, *Security* lub *System*. Aby zwiększyć wydajność i zoptymalizować transmisję danych do serwera KUMA, możesz ręcznie dodawać poszczególne zdarzenia do danych telemetrycznych lub je z nich wykluczać. Można na przykład wykluczyć zdarzenia Sysmon.

Możesz wyeksportować listę wykluczeń do pliku JSON z poziomu wiersza poleceń.

Jeśli polecenie zawiera tylko nazwę pliku, do którego chcesz wyeksportować ustawienia, aplikacja umieści plik w następujący sposób:

- Jeśli ścieżka do avp.com zostanie dodana do zmiennej systemowej %PATH%, aplikacja umieści plik w folderze `C:\Windows\SysWOW64`.

- Jeśli uruchomisz polecenie z folderu instalacyjnego aplikacji, eksport nie powiedzie się, ponieważ autoochrona aplikacji blokuje utworzenie nowego pliku w folderze aplikacji. Aby wyeksportować ustawienia aplikacji do pliku, wprowadź ścieżkę do pliku.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Działanie	
`export`	Eksportowanie filtrów zdarzeń w celu wysłania do KUMA.
`import`	Importowanie filtrów zdarzeń w celu wysłania do KUMA. Jeśli na komputerze istnieją już reguły filtrowania zdarzeń, Kaspersky Endpoint Security zastąpi je podczas importowania.

Plik do eksportu lub importu	
`<file name>`	Nazwa pliku z filtrami zdarzeń, które mają zostać wysłane do KUMA. Możesz także wprowadzić ścieżkę do pliku. Można eksportować filtry do pliku JSON w celu wysłania do KUMA.

Polecenia do zarządzania klientem Light Agent

Aplikacją można zarządzać za pomocą wiersza poleceń w trybie Light Agent do ochrony środowisk wirtualnych. Możesz zarządzać aplikacją w trybie Light Agent, jeśli zarządzanie przy użyciu konsoli Kaspersky Security Center nie jest możliwe. Możesz wyświetlić listę poleceń do zarządzania aplikacją, uruchamiając polecenie `HELP`. Aby zapoznać się z informacjami o składni konkretnego polecenia, wpisz `HELP <command>`.

Aby zarządzać aplikacją w trybie Light Agent z poziomu wiersza poleceń:

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.
3. Aby wykonać polecenie, użyj następującego szablonu:

   ```
   avp.com <command> [options]
   ```

   W rezultacie Kaspersky Endpoint Security wykona polecenie.

Aplikacja zainstalowana w trybie Light Agent obsługuje niemal wszystkie polecenia AVP aplikacji zainstalowanej w trybie standardowym. W trybie Light Agent zadania aktualizacji antywirusowej bazy danych i zarządzania kluczami licencyjnymi są ograniczone.

KSVLAINFO. Określanie trybu klienta Light Agent

Określanie trybu klienta Light Agent.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com KSVLAINFO
```

Polecenie przesyła następujące informacje do konsoli:

- Tryb Light Agent do ochrony środowisk wirtualnych: włączony lub wyłączony.

  Jeśli tryb Light Agent jest włączony, aplikacja jest używana jako część rozwiązania Kaspersky Security for Virtualization Light Agent.

- Tryb ochrony VDI: włączony lub wyłączony.

  Tryb ochrony VDI pomaga zoptymalizować działanie Kaspersky Endpoint Security na nietrwałych maszynach wirtualnych. Jeśli tryb ochrony VDI jest włączony, aktualizacje wymagające ponownego uruchomienia chronionej maszyny wirtualnej nie są instalowane na nietrwałych maszynach wirtualnych. Po otrzymaniu aktualizacji wymagających ponownego uruchomienia Light Agent zainstalowany na nietrwałej maszynie wirtualnej wysyła wiadomość do Kaspersky Security Center z informacją o konieczności zaktualizowania szablonu chronionej maszyny wirtualnej.

- Typ chronionej maszyny wirtualnej: trwała lub nietrwała.

- Rola chronionej maszyny wirtualnej w infrastrukturze wirtualnej: serwer czy stacja robocza.

- Identyfikator: UUID.

VIISINFO. Stan połączeniu klienta Light Agent z serwerem integracyjnym

Wyświetlanie informacji o połączeniu klienta Light Agent z serwerem integracyjnym.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com VIISINFO
```

Polecenie przesyła następujące informacje do konsoli:

- Adres i port serwera integracyjnego, z którym połączony jest klientem Light Agent.

- Status połączenia z serwerem integracyjnym.

- Data i godzina ostatniego połączenia klienta Light Agent z serwerem integracyjnym.

SVMINFO. Stan połączeniu klienta Light Agent z serwerem ochrony

Wyświetlanie informacji o połączeniu klienta Light Agent z serwerem ochrony.

Aby uruchomić polecenie, przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security. Możesz także dodać ścieżkę pliku wykonywalnego do zmiennej systemowej %PATH% i uruchomić polecenie bez przechodzenia do folderu aplikacji.

Składnia polecenia

```
avp.com SVMINFO
```

Polecenie przesyła następujące informacje do konsoli:

- Adres maszyny SVM, z którą połączony jest klient Light Agent, oraz lokalizacja maszyny SVM w infrastrukturze wirtualnej względem klienta Light Agent: lokalna lub nielokalna.
- Metoda wykrywania SVM używana przez klienta Light Agent: korzystanie z serwera integracyjnego lub niestandardowej listy adresów SVM.
- Lista adresów SVM, jeśli jako metodę wykrywania SVM wybrano listę adresów SVM.
- Znacznik umożliwiający połączenie klienta Light Agent z maszyną SVM.
- Algorytm wyboru SVM: standardowy lub rozszerzony. Jeśli używany jest rozszerzony algorytm wyboru SVM, wyświetlany jest również typ ścieżki maszyny SVM w infrastrukturze wirtualnej.
- Status ochrony połączenia pomiędzy klientem Light Agent a serwerem ochrony.

Kody błędów

Podczas pracy z aplikacją za pośrednictwem wiersza poleceń mogą wystąpić błędy. Jeśli wystąpią błędy, Kaspersky Endpoint Security wyświetla komunikat o błędzie, na przykład, `Error: Cannot start task 'EntAppControl'`. Kaspersky Endpoint Security może również wyświetlać dodatkowe informacje w postaci kodu, na przykład, `error=8947906D` (patrz tabela poniżej).

Kody błędów

Kod błędu	Opis
09479001	Ten klucz jest już w użyciu
0947901D	Licencja utraciła ważność. Aktualizacja baz danych jest niedostępna
89479002	Nie odnaleziono klucza
89479003	Nie odnaleziono podpisu cyfrowego lub jest on uszkodzony
89479004	Dane są uszkodzone
89479005	Plik klucza jest uszkodzony
89479006	Licencja utraciła ważność
89479007	Nie wybrano pliku klucza

Kod błędu	Opis
89479008	Nieprawidłowy plik klucza
89479009	Zapisanie danych nie powiodło się
8947900A	Odczytanie danych nie powiodło się
8947900B	Błąd wejścia/wyjścia
8947900C	Nie odnaleziono baz danych
8947900E	Biblioteka licencjonowania nie została załadowana
8947900F	Bazy danych są uszkodzone lub zostały uaktualnione ręcznie
89479010	Bazy danych są uszkodzone
89479011	Nie można użyć nieprawidłowego pliku klucza jako klucza zapasowego
89479012	Błąd systemowy
89479013	Lista zablokowanych kluczy jest uszkodzona
89479014	Podpis pliku nie jest zgodny z podpisem cyfrowym Kaspersky
89479015	Nie można użyć klucza licencji testowej jako klucza licencji komercyjnej
89479016	Aby skorzystać z wersji beta aplikacji, wymagana jest licencja do testów beta
89479017	Plik klucza nie jest kompatybilny z tą aplikacją. Nie jest możliwe aktywowanie Kaspersky Endpoint Security for Windows przy użyciu pliku klucza dla innej aplikacji. Proszę sprawdź zainstalowaną aplikację
89479018	Klucz licencyjny został zablokowany przez Kaspersky
89479019	Obecnie zainstalowana jest wersja testowa aplikacji. Ponowne dodanie testowego klucza licencyjnego nie jest możliwe
8947901A	Plik klucza jest uszkodzony
8947901B	Nie odnaleziono podpisu cyfrowego, jest on uszkodzony lub nie jest podpisem cyfrowym firmy Kaspersky
8947901C	Nie można dodać klucza, jeśli odpowiadająca mu licencja niekomercyjna utraciła ważność
8947901E	Data utworzenia lub aktywacji pliku klucza jest nieprawidłowa. Proszę sprawdzić ustawienia daty systemowej
8947901F	Nie można dodać klucza licencji testowe: inny klucz licencji testowej jest już aktywny
89479020	Brak listy zablokowanych kluczy lub jest ona uszkodzona
89479021	Brak opisu aktualizacji lub jest on uszkodzony
89479022	Klucz nie jest przeznaczony dla tej aplikacji
89479023	Nie można użyć nieprawidłowego pliku klucza jako klucza zapasowego
89479025	Wystąpił błąd podczas wysyłania żądania do serwera aktywacji. Możliwe przyczyny: błąd połączenia z internetem lub tymczasowe problemy na serwerze aktywacji. Spróbuj aktywować aplikację przy użyciu kodu aktywacyjnego później (w ciągu 1-2 godzin). Jeżeli problem będzie wciąż występował, skontaktuj się ze swoim dostawcą internetu
89479026	Żądanie zawiera nieprawidłowy kod aktywacyjny
89479027	Nie można uzyskać stanu odpowiedzi
89479028	Wystąpił błąd podczas zapisu pliku tymczasowego
89479029	Wprowadzono nieprawidłowy kod aktywacyjny lub na komputerze ustawiona jest nieprawidłowa data systemowa. Proszę sprawdzić ustawienia daty systemowej na komputerze
8947902A	Klucz nie jest przeznaczony dla tej aplikacji lub licencja utraciła ważność
8947902B	Nie powiodło się uzyskanie pliku klucza. Wprowadzono nieprawidłowy kod aktywacyjny
8947902C	Serwer aktywacyjny zwrócił błąd 400
8947902D	Serwer aktywacyjny zwrócił błąd 401
8947902E	Serwer aktywacyjny zwrócił błąd 403
8947902F	Wymagany zasób nie jest dostępny na serwerze aktywacji. Serwer aktywacji zwrócił błąd 404. Proszę sprawdzić ustawienia połączenia internetowego

Kod błędu	Opis
89479030	Serwer aktywacyjny zwrócił błąd 405
89479031	Serwer aktywacyjny zwrócił błąd 406
89479032	Wymagana jest autoryzacja proxy. Proszę sprawdzić ustawienia sieci
89479033	Przekroczono limit czasu żądania
89479034	Serwer aktywacyjny zwrócił błąd 409
89479035	Wymagany zasób nie jest dostępny na serwerze aktywacji. Serwer aktywacji zwrócił błąd 410. Proszę sprawdzić ustawienia połączenia internetowego
89479036	Serwer aktywacyjny zwrócił błąd 411
89479037	Serwer aktywacyjny zwrócił błąd 412
89479038	Serwer aktywacyjny zwrócił błąd 413
89479039	Serwer aktywacyjny zwrócił błąd 414
8947903A	Serwer aktywacyjny zwrócił błąd 415
8947903C	Błąd wewnętrzny serwera
8947903D	Funkcja nie jest obsługiwana
8947903E	Niepoprawna odpowiedź bramy. Sprawdź ustawienia sieci
8947903F	Zasób tymczasowo niedostępny
89479040	Przekroczono czas odpowiedzi bramy. Sprawdź ustawienia sieci
89479041	Ten protokół nie jest obsługiwany przez serwer
89479043	Nieznany błąd HTTP
89479044	Nieprawidłowy identyfikator zasobu
89479046	Nieprawidłowy adres internetowy
89479047	Nieprawidłowy folder docelowy
89479048	Błąd alokacji pamięci
89479049	Wystąpił błąd podczas konwersji parametrów na ciąg znaków ANSI (adres internetowy, folder, agent)
8947904A	Wystąpił błąd podczas tworzenia wątku roboczego
8947904B	Wątek roboczy jest już uruchomiony
8947904C	Wątek roboczy nie jest uruchomiony
8947904D	Plik klucza nie został znaleziony na serwerze aktywacji
8947904E	Klucz został zablokowany
8947904F	Błąd wewnętrzny serwera aktywacji
89479050	Niewystarczająca ilość informacji w żądaniu aktywacji
89479053	Licencja odpowiadająca dodanemu kluczowi utraciła już ważność
89479054	Na komputerze ustawiona jest nieprawidłowa data systemowa. Proszę sprawdzić ustawienia daty systemowej
89479055	Licencja testowa utraciła ważność
89479056	Wygasł okres aktywacji aplikacji
89479057	Limit aktywacji określonego kodu aktywacyjnego został przekroczony
89479058	Aktywacja nie powiodła się. Błąd systemowy
89479059	Nie można użyć klucza licencji testowej jako klucza licencji komercyjnej
8947905C	Wymagany jest kod aktywacyjny
89479062	Nie można nawiązać połączenia z serwerem aktywacji

Kod błędu	Opis
89479064	Serwer aktywacji jest niedostępny. Proszę sprawdzić połączenie z internetem i ponowić aktywację
89479065	Licencja utraciła ważność
89479066	Aktywny klucz nie może zostać zastąpiony kluczem, który utracił swą ważność
89479067	Nie można dodać zapasowego klucza, jeśli odpowiadająca mu licencja utraci ważność wcześniej niż bieżąca licencja
89479068	Brak uaktualnionego klucza subskrypcyjnego
8947906A	Nieprawidłowy kod aktywacyjny
8947906B	Klucz jest już aktywny
8947906C	Rodzaje licencji odpowiadające kluczowi aktywnemu oraz zapasowemu nie są zgodne
8947906D	Składnik nie jest obsługiwany przez licencję
8947906E	Nie można dodać klucza subskrypcyjnego jako klucza zapasowego
89479213	Ogólny błąd warstwy transportowej
89479214	Nie można nawiązać połączenia z serwerem aktywacji
89479215	Nieprawidłowy format adresu internetowego
89479216	Rozwiązanie adresu serwera proxy nie powiodło się
89479217	Rozwiązanie adresu serwera nie powiodło się. Proszę sprawdzić ustawienia połączenia z internetem
89479218	Próba nawiązania połączenia z serwerem nie powiodła się
89479219	Zdalny dostęp jest zabroniony
8947921A	Przekroczono czas na zakończenie operacji
8947921B	Błąd podczas przesyłania żądania HTTP
8947921C	Błąd połączenia SSL
8947921D	Operacja przerwana przez wywołanie zwrotne
8947921E	Zbyt wiele przekierowań
8947921F	Sprawdzenie odbiorcy nie powiodło się
89479220	Pusta odpowiedź z serwera
89479221	Błąd podczas przesyłania danych
89479222	Błąd podczas odbierania danych
89479223	Problem dotyczący certyfikatu SSL
89479224	Problem dotyczący szyfrowania SSL
89479225	Problem dotyczący centrum certyfikacji SSL
89479226	Nieprawidłowa zawartość pakietu sieciowego
89479227	Dostęp konta zabroniony
89479228	Nieprawidłowy plik certyfikatu SSL
89479229	Nie można zakończyć połączenia SSL
8947922A	Powracający błąd
8947922B	Nieprawidłowy plik zawierający unieważnione certyfikaty
8947922C	Błąd żądania certyfikatu SSL
89479401	Nieznany błąd serwera
89479402	Błąd wewnętrzny serwera
89479403	Brak dostępnego klucza dla wprowadzonego kodu aktywacyjnego
89479404	Aktywny klucz został zablokowany

Kod błędu	Opis
89479405	Brak wymaganych parametrów żądania aktywacji
89479406	Nieprawidłowy numer klienta lub hasło
89479407	Nieprawidłowy kod aktywacyjny
89479408	Kod aktywacyjny nie jest kompatybilny z tą aplikacją. Nie jest możliwe aktywowanie Kaspersky Endpoint Security for Windows przy użyciu kodu aktywacyjnego dla innej aplikacji. Proszę sprawdzić zainstalowaną aplikację
89479409	Wymagany jest kod aktywacyjny
8947940B	Wygasł okres aktywacji
8947940C	Liczba aktywacji dla tego kodu aktywacyjnego została przekroczona
8947940D	Nieprawidłowy format żądania ID
8947940E	Kod aktywacyjny jest już w użyciu
8947940F	Odnowienie kodu aktywacyjnego nie powiodło się
89479410	Kod aktywacyjny nie jest przeznaczony dla tego regionu
89479411	Ten kod aktywacyjny nie może zostać użyty w tej wersji językowej aplikacji
89479412	Kod aktywacyjny przeznaczony jest do nowszej wersji tej aplikacji. Uzyskaj inny kod aktywacyjny w celu aktywacji zainstalowanej wersji aplikacji
89479413	Serwer aktywacji zwrócił błąd 643
89479414	Serwer aktywacji zwrócił błąd 644
89479415	Serwer aktywacji zwrócił błąd 645
89479416	Serwer aktywacji zwrócił błąd 646
89479417	Wymagany jest serwer aktywacji w wersji 1.0
89479418	Nieprawidłowy format kodu aktywacyjnego
89479419	Czas na komputerze nie jest zsynchronizowany z czasem serwera aktywacji
8947941A	Nieprawidłowa wersja aplikacji
8947941B	Subskrypcja utraciła ważność
8947941C	Przekroczono liczbę dopuszczalnych aktywacji
8947941D	Nieprawidłowy podpis zgłoszenia
8947941E	Wymagane są dodatkowe dane
8947941F	Weryfikacja danych nie powiodła się
89479420	Subskrypcja nieaktywna
89479421	Trwają prace konserwacyjne serwera aktywacji
89479501	Nieoczekiwany błąd
89479502	Przesłano nieprawidłowy parametr. Przykładowo, pustą listę adresów serwerów aktywacji
89479503	Niepoprawny kod aktywacyjny (niepoprawna suma kontrolna)
89479504	Nieprawidłowy identyfikator użytkownika
89479505	Nieprawidłowe hasło użytkownika
89479506	Nieprawidłowa odpowiedź z serwera aktywacji
89479507	Żądanie aktywacji zostało przerwane
89479509	Serwer aktywacji zwrócił pustą listę przekierowań

Dodatek. Profile aplikacji

Profil to komponent, zadanie lub funkcja Kaspersky Endpoint Security. Profile służą do zarządzania aplikacją z poziomu wiersza poleceń. Za pomocą profili można wykonywać polecenia `START`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT`. Korzystając z profili, możesz skonfigurować ustawienia aplikacji (na przykład `STOP DeviceControl`) lub uruchomić zadania (na przykład `START Scan_My_Computer`).

Dostępne są następujące profile:

- `AdaptiveAnomaliesControl` – Adaptacyjna kontrola anomalii
- `AMSI` – Ochrona AMSI
- `AntiCryptor`
- `BehaviorDetection` – Wykrywanie zachowań
- `DeviceControl` – Kontrola urządzeń
- `EntAppControl` – Kontrola aplikacji
- `File_Monitoring` lub `FM` — Ochrona plików
- `Firewall` lub `FW` – Zapora sieciowa
- `HIPS` – Ochrona przed włamaniami
- `IDS` – Ochrona sieci
- `IntegrityCheck` – Sprawdzanie integralności
- `LogInspector` – Kontrola dziennika
- `Mail_Monitoring` lub `EM` – Ochrona poczty
- `Rollback` – Wycofanie aktualizacji (profil nie może zostać zastosowany, jeśli aplikacja jest zainstalowana w trybie Light Agent)
- `Scan_ContextScan` – Skanowanie z menu kontekstowego
- `Scan_IdleScan` – Skanowanie w tle
- `Scan_Memory` – Skanowanie pamięci jądra
- `Scan_My_Computer` – Pełne skanowanie
- `Scan_Objects` – Skanowanie obiektów
- `Scan_Qscan` – Skanowanie obiektów ładowanych podczas uruchamiania systemu operacyjnego
- `Scan_Removable_Drive` – Skanowanie dysków wymiennych

- `Scan_Startup` lub `STARTUP` – Skanowanie obszarów krytycznych
- `Updater` – Aktualizacja (profil nie może zostać zastosowany, jeśli aplikacja jest zainstalowana w trybie Light Agent)
- `Web_Monitoring` lub `WM` – Ochrona WWW
- `WebControl` – Kontrola sieci

Kaspersky Endpoint Security obsługuje również profile usług. Profile usług mogą być wymagane podczas kontaktu z pomocą techniczną Kaspersky.

Zarządzanie aplikacją za pośrednictwem interfejsu API REST

Kaspersky Endpoint Security umożliwia skonfigurowanie ustawień aplikacji, uruchamianie skanowania, aktualizowanie antywirusowych baz danych i wykonywanie innych zadań przy użyciu rozwiązań innych firm. Kaspersky Endpoint Security oferuje w tym celu interfejs API. Interfejs API REST Kaspersky Endpoint Security działa przez HTTP i składa się z zestawu metod żądania / odpowiedzi. Innymi słowy, możesz zarządzać Kaspersky Endpoint Security za pomocą rozwiązania innej firmy, a nie lokalnego interfejsu aplikacji lub Konsoli administracyjnej Kaspersky Security Center.

Aby rozpocząć korzystanie z interfejsu API REST, musisz zainstalować Kaspersky Endpoint Security z obsługą interfejsu API REST. Klient REST i Kaspersky Endpoint Security muszą być zainstalowani na tym samym komputerze.

W celu zapewnienia bezpiecznej interakcji między Kaspersky Endpoint Security a klientem REST:

- Skonfiguruj ochronę klienta REST przed nieautoryzowanym dostępem zgodnie z zaleceniami dewelopera klienta REST. Skonfiguruj ochronę folder klienta REST przed pracą z pomocą Discretionary Access Control List – DACL.
- Aby uruchomić klienta REST, użyj oddzielnego konta z uprawnieniami administratora. Zablokuj interaktywne logowanie do systemu dla tego konta.

Aplikacja jest zarządzana za pomocą interfejsu API REST pod adresem http://127.0.0.1 lub http://localhost. Zdalne zarządzanie Kaspersky Endpoint Security za pośrednictwem interfejsu API REST nie jest możliwe.

OTWÓRZ DOKUMENTACJĘ API REST

Instalowanie aplikacji za pośrednictwem interfejsu API REST

Aby zarządzać aplikacją poprzez interfejs API REST, musisz zainstalować Kaspersky Endpoint Security z obsługą interfejsu API REST. Jeśli zarządzasz Kaspersky Endpoint Security za pośrednictwem interfejsu API REST, nie możesz zarządzać aplikacją za pomocą Kaspersky Security Center.

Przygotowywanie do zainstalowania aplikacji z obsługą API REST

Bezpieczna interakcja Kaspersky Endpoint Security z klientem REST wymaga skonfigurowania identyfikacji żądania. W tym celu należy zainstalować certyfikat i podpisać ładunek każdego żądania.

Aby utworzyć certyfikat, możesz użyć, na przykład, OpenSSL.

Na przykład:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Użyj algorytmu szyfrowania RSA z kluczem o efektywnej długości wynoszącej 2048 bitów lub więcej.

W rezultacie otrzymasz certyfikat `cert.pem` i klucz prywatny `key.pem`.

Instalowanie aplikacji z obsługą API REST

W celu zainstalowania Kaspersky Endpoint Security z obsługą API REST:

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu zawierającego pakiet dystrybucyjny dla Kaspersky Endpoint Security w wersji 11.2.0 lub nowszej.
3. Zainstaluj Kaspersky Endpoint Security z następującymi ustawieniami:
   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     Nazwa użytkownika do zarządzania aplikacją za pośrednictwem interfejsu API REST. Wpisz nazwę użytkownika w formacie `<DOMAIN>\<UserName>` (na przykład: `RESTAPI_User=COMPANY\Administrator`). Aplikacją można zarządzać za pośrednictwem interfejsu API REST tylko na tym koncie. Możesz wybrać tylko jednego użytkownika do pracy z interfejsem API REST.
   - `RESTAPI_Port=<port>`

     Port używany do zarządzania aplikacją za pośrednictwem interfejsu API REST. Domyślnie używany jest port 6782. Upewnij się, że port jest wolny. Jest to parametr opcjonalny.
   - `RESTAPI_Certificate=<path to certificate>`

     Certyfikat do identyfikowania żądań (na przykład, `RESTAPI_Certificate=C:\cert.pem`).

     Możesz zainstalować certyfikat po zainstalowaniu aplikacji lub aktualizacji certyfikatu po wygaśnięciu certyfikatu.

     Jak zainstalować certyfikat dla identyfikacji żądania API REST?

     1. Wyłącz Autoochronę Kaspersky Endpoint Security

        Mechanizm autoochrony uniemożliwia modyfikowanie i usuwanie plików aplikacji, procesów w pamięci i wpisów w rejestrze systemu.
     2. Przejdź do klucza rejestru, który zawiera ustawienia API REST:
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. Wprowadź ścieżkę do certyfikatu, na przykład, `Certificate = C:\Folder\cert.pem`.
     4. Włącz Autoochronę Kaspersky Endpoint Security.
     5. Uruchom aplikację ponownie.
   - `AdminKitConnector=1`

     Zarządzanie aplikacjami za pomocą systemów administracyjnych. Domyślnie zarządzanie jest dozwolone.

Możesz także użyć pliku setup.ini, aby zdefiniować ustawienia do pracy z interfejsem API REST.

Na przykład:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
/pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
```

Dzięki temu będziesz mógł zarządzać aplikacją za pośrednictwem interfejsu API REST. Aby zweryfikować jego działanie, otwórz dokumentację interfejsu API REST za pomocą żądania GET.

Na przykład:

```
GET http://localhost:6782/kes/v1/api-docs
```

Jeśli zainstalowałeś aplikację z obsługą API REST, Kaspersky Endpoint Security automatycznie tworzy regułę zezwalającą w ustawieniach Kontroli sieci do uzyskania dostępu do zasobów sieciowych (*reguła usługowa dla REST API*). Ta reguła jest potrzebna, aby zezwolić klientowi REST na dostęp do Kaspersky Endpoint Security przez cały czas. Na przykład, jeśli ograniczyłeś dostęp użytkownika do zasobów sieciowych, to nie będzie wpływało na zarządzanie aplikacją poprzez API REST. Zalecane jest, żebyś nie usuwał reguły lub nie zmieniał ustawień *reguły usługowej dla API REST*. Jeśli usunąłeś regułę, Kaspersky Endpoint Security przywróci ją po ponownym uruchomieniu aplikacji.

Praca z interfejsem API

Nie można ograniczyć dostępu do aplikacji za pośrednictwem interfejsu API REST za pomocą Ochrony hasłem. Na przykład nie można zablokować użytkownikowi możliwości wyłączenia ochrony za pośrednictwem interfejsu API REST. Możesz skonfigurować Ochronę hasłem za pośrednictwem interfejsu API REST i ograniczyć dostęp użytkownika do aplikacji za pośrednictwem interfejsu lokalnego.

Aby zarządzać aplikacją za pośrednictwem interfejsu API REST, musisz uruchomić klienta REST na koncie określonym podczas instalowania aplikacji z obsługą interfejsu API REST. Możesz wybrać tylko jednego użytkownika do pracy z interfejsem API REST.

OTWÓRZ DOKUMENTACJĘ API REST

Zarządzanie aplikacją za pośrednictwem interfejsu API REST obejmuje następujące kroki:

1. Uzyskanie aktualnych wartości ustawień aplikacji. Aby to zrobić, wyślij żądanie GET.

   Na przykład:

   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. Aplikacja wyśle odpowiedź ze strukturą i wartościami ustawień. Kaspersky Endpoint Security obsługuje formaty XML i JSON.

   Na przykład:

   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. Zmodyfikuj ustawienia aplikacji. Użyj struktury ustawień otrzymanej w odpowiedzi na żądanie GET.

Na przykład:

```
{
"action": 0,
"enableSystemProcessesMemoryProtection": false,
"enabled": true
}
```

4. Zapisz ustawienia aplikacji (ładunek) w JSON (payload.json).

5. Zapisz JSON w formacie PKCS7.

   Na przykład:

   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out
   signed_payload.pem
   ```

   W rezultacie uzyskasz podpisany plik z ładunkiem żądania (`signed_payload.pem`).

6. Zmodyfikuj ustawienia aplikacji. Aby to zrobić, wyślij żądanie POST i załącz podpisany plik z ładunkiem żądania (`signed_payload.pem`).

Aplikacja stosuje nowe ustawienia i wysyła odpowiedź zawierającą wyniki konfiguracji aplikacji (odpowiedź może być pusta). Możesz sprawdzić, czy ustawienia są aktualizowane przy użyciu żądania GET.

Źródła informacji o aplikacji

Ta sekcja zawiera opis źródeł informacji na temat aplikacji.

Możesz wybrać najdogodniejsze źródło informacji w zależności od wagi i pilności problemu.

Strona Kaspersky Endpoint Security w witrynie Kaspersky

Na stronie Kaspersky Endpoint Security możesz przeglądać ogólne informacje o aplikacji i jej funkcjach.

Strona Kaspersky Endpoint Security zawiera łącze do sklepu internetowego. Tam możesz kupić lub odnowić aplikację.

Strona Kaspersky Endpoint Security w Bazie wiedzy

Baza wiedzy to sekcja na stronie pomocy technicznej.

Na stronie Kaspersky Endpoint Security w Bazie wiedzy, możesz przeczytać artykuły zawierające przydatne informacje, zalecenia i odpowiedzi na najczęściej zadawane pytania dotyczące zakupu, instalacji i korzystania z aplikacji.

Artykuły Bazy wiedzy mogą zawierać odpowiedzi na pytania dotyczące nie tylko Kaspersky Endpoint Security, ale także innych aplikacji firmy Kaspersky. Artykuły w Bazie wiedzy mogą również zawierać wiadomości od pomocy technicznej.

Dyskusja na temat aplikacji firmy Kaspersky na forum

Jeśli Twoje pytanie nie wymaga pilnej odpowiedzi, możesz omówić je z ekspertami firmy Kaspersky i innymi użytkownikami na naszym Forum.

Na Forum możesz przeglądać istniejące tematy, zamieszczać własne komentarze i tworzyć nowe tematy dyskusji.

Kontakt z działem pomocy technicznej

Jeśli nie znajdziesz rozwiązania swojego problemu w dokumentacji lub w innych źródłach informacji o Kaspersky Endpoint Security, zalecamy skontaktować się z działem pomocy technicznej. Eksperci z działu pomocy technicznej odpowiedzą na Twoje pytania związane z instalacją i użytkowaniem Kaspersky Endpoint Security.

Kaspersky oferuje wsparcie dla Kaspersky Endpoint Security podczas cyklu życia aplikacji (zapoznaj się ze stroną cyklu życia 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 stronę pomocy technicznej
- Wysyłając zgłoszenie do pomocy technicznej poprzez portal Kaspersky CompanyAccount

Po poinformowaniu o swoim problemie specjalistów z działu pomocy technicznej Kaspersky, mogą oni poprosić o utworzenie *pliku śledzenia*. Plik śledzenia umożliwia śledzenie procesu wykonywania poleceń aplikacji krok po kroku, a także określenie etapu działania aplikacji, w którym pojawił się błąd.

Specjaliści z pomocy technicznej mogą również potrzebować dodatkowych informacji o systemie operacyjnym, uruchomionych na komputerze procesach, szczegółowego raportu z działania modułów aplikacji.

Podczas wykonywania diagnostyki specjaliści z działu pomocy technicznej mogą poprosić o zmianę ustawień aplikacji poprzez:

- Aktywowanie funkcji gromadzenia rozszerzonych informacji diagnostycznych.
- Skonfiguruj pojedyncze moduły aplikacji, zmieniając specjalne ustawienia, które nie są dostępne poprzez standardowy interfejs użytkownika.
- Zmianę ustawień przechowywania informacji diagnostycznych.
- Konfigurację przechwytywania i rejestrowania ruchu sieciowego.

Eksperci z pomocy technicznej dostarczą wszystkie informacje potrzebne do wykonania tych działań (opis sekwencji kroków, ustawienia, które mają zostać zmodyfikowane, pliki konfiguracyjne, skrypty, dodatkowe funkcje wiersza polecenia, moduły diagnostyczne, narzędzia do zadań specjalnych itd.) oraz poinformują o zakresie danych używanych w celach diagnostycznych. Rozszerzone informacje diagnostyczne są zapisywane na komputerze użytkownika. Dane nie są automatycznie przesyłane do Kaspersky.

Powyższe działania powinny być wykonywane tylko pod nadzorem specjalistów z pomocy technicznej i zgodnie z ich poleceniami. Samodzielna zmiana ustawień aplikacji w sposób, który nie został opisany w pomocy online lub przez specjalistów z pomocy technicznej może powodować spowolnienia i awarie systemu operacyjnego, zmniejsza poziom ochrony komputera i niszczy dostępność i integrację przetwarzanych informacji.

Zawartość i przechowywanie plików śledzenia

Jesteś osobiście odpowiedzialny za bezpieczeństwo danych przechowywanych na swoim komputerze, w szczególności za monitorowanie i ograniczanie dostępu do danych, aż do momentu wysłania ich do Kaspersky.

Pliki śledzenia są przechowywane na komputerze tak długo, jak aplikacja jest używana i są trwale usuwane, gdy aplikacja jest usuwana.

Pliki śledzenia, z wyjątkiem plików śledzenia Agenta autoryzacji, są przechowywane w folderze `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`.

Pliki śledzenia są nazywane w następującym formacie: `KES<14.1_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

Możesz przejrzeć dane zapisane w plikach śledzenia.

Wszystkie pliki śledzenia zawierają następujące dane:

- Czas zdarzenia
- Liczbę procesów wykonania

  Plik śledzenia Agenta autoryzacji nie zawiera tej informacji.

- Komponent aplikacji, który wywołał zdarzenie
- Poziom priorytetu zdarzenia (zdarzenie informacyjne, ostrzeżenie, zdarzenie krytyczne, błąd)
- Opis zdarzenia dotyczący wykonania polecenia przez moduł aplikacji oraz wynik wykonania tego polecenia.

Zawartość plików śledzenia SRV.log, GUI.log oraz ALL.log

Oprócz ogólnych danych, pliki śledzenia `SRV.log`, `GUI.log` i `ALL.log` mogą przechowywać następujące informacje:

- Dane osobowe, łącznie z nazwiskiem, imieniem oraz drugim imieniem, jeśli takie dane są uwzględnione w ścieżce dostępu do plików na komputerze lokalnym.
- Dane dotyczące sprzętu zainstalowanego na komputerze (takie jak dane oprogramowania układowego BIOS/UEFI). Te dane są zapisywane w celu zapisu do plików śledzenia podczas przeprowadzania Kaspersky Disk Encryption.
- Nazwa użytkownika i hasło, jeśli były otwarcie przesyłane. Dane te mogą być zapisywane w plikach śledzenia podczas skanowania ruchu internetowego.
- Nazwa użytkownika i hasło, jeśli znajdują się w nagłówkach HTTP.

- Nazwa konta Microsoft Windows, jeśli nazwa konta jest uwzględniona w nazwie pliku.
- Twój adres e-mail lub adres sieciowy zawierający nazwę Twojego konta i hasło, jeśli znajdują się w nazwie wykrytego obiektu.
- Odwiedzane strony internetowe oraz przekierowania z tych stron. Dane te są zapisywane w plikach śledzenia, gdy aplikacja skanuje strony internetowe.
- Adres serwera proxy, nazwa komputera, port, adres IP i login używany przy dostępie do serwera proxy. Dane te są zapisywane w plikach śledzenia, jeśli aplikacja używa serwera proxy.
- Zdalne adresy IP, z którymi Twój komputer nawiązał połączenie.
- Temat wiadomości, numer ID, adres i nazwisko nadawcy wiadomości, strona internetowa nadawcy w sieci społecznościowej. Dane te są zapisywane w plikach śledzenia, jeśli Kontrola sieci jest włączona.
- Dane dotyczące ruchu sieciowego. Dane są zapisywane w plikach śledzenia, jeśli włączone są komponenty monitorowania ruchu (takie jak Kontrola sieci).
- Dane otrzymane z serwerów Kaspersky (takie jak wersja antywirusowych baz danych).
- Stany składników Kaspersky Endpoint Security i dane dotyczące ich działania.
- Dane dotyczące aktywności użytkownika w aplikacji.
- Zdarzenia systemu operacyjnego.

Zawartość plików śledzenia HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Poza ogólnymi danymi, plik śledzenia `HST.log` zawiera informacje o wykonaniu zadania aktualizacji bazy danych i modułów aplikacji.

Oprócz ogólnych danych, plik śledzenia `BL.log` zawiera informacje o zdarzeniach występujących podczas działania aplikacji, a także o danych wymaganych do rozwiązania błędów aplikacji. Ten plik jest tworzony, jeśli aplikacja jest uruchamiana w parametrem avp.exe –bl.

Plik śledzenia `Dumpwriter.log` zawiera nie tylko ogólne dane, ale także informacje o usłudze niezbędne do rozwiązania problemów występujących podczas zapisywania plików zrzutu pamięci aplikacji.

Poza ogólnymi danymi, plik śledzenia `WD.log` zawiera informacje o zdarzeniach występujących podczas działania usługi avpsus, w tym o zdarzeniach aktualizacji modułów aplikacji.

Plik śledzenia `AVPCon.dll.log` zawiera nie tylko ogólne dane, ale także informacje o zdarzeniach występujących podczas działania modułu połączeniowego Kaspersky Security Center.

Zawartość plików śledzenia wydajności

Pliki śledzenia wydajności są nazywane w następującym formacie:
`KES<14.1_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Oprócz ogólnych danych, pliki śledzenia wydajności zawierają informacje o obciążeniu procesora, informacje o czasie ładowania systemu operacyjnego i aplikacji, a także informacje o uruchomionych procesach.

Zawartość plików śledzenia modułu Ochrona AMSI

Oprócz ogólnych danych, plik śledzenia `AMSI.log` zawiera informacje o wynikach skanowania wykonanego na żądanie ze strony aplikacji firm trzecich.

Zawartości plików śledzenia komponentu Ochrona poczty

Oprócz ogólnych danych, plik śledzenia `mcou.OUTLOOK.EXE.log` może zawierać części wiadomości e-mail, w tym adresy e-mail.

Zawartości plików śledzenia komponentu Skanowanie z menu kontekstowego

Oprócz ogólnych informacji, plik śledzenia `shellex.dll.log` zawiera informacje o zakończeniu zadania skanowania i danych wymaganych do debugowania aplikacji.

Zawartość plików śledzenia wtyczki webowej aplikacji

Pliki śledzenia wtyczki webowej aplikacji są przechowywane na komputerze, na którym wdrożono Kaspersky Security Center Web Console, w folderze `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs`.

Pliki śledzenia wtyczki webowej aplikacji mają następujące nazwy: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`. Konsola Web Console rozpoczyna zapisywanie danych po instalacji, a usuwanie plików śledzenia po usunięciu Web Console.

Pliki śledzenia wtyczki webowej aplikacji zawierają nie tylko ogólne dane, ale także następujące informacje:

- Hasło użytkownika KLAdmin do odblokowania interfejsu Kaspersky Endpoint Security (Ochrona hasłem).
- Tymczasowe hasło do odblokowania interfejsu Kaspersky Endpoint Security (Ochrona hasłem).
- Nazwa użytkownika i hasło dla serwera pocztowego SMTP (Powiadomienia e-mail).
- Nazwa użytkownika i hasło dla internetowego serwera proxy (Serwer proxy).
- Nazwa użytkownika i hasło dla zadania *Zmiana składników aplikacji*.
- Dane uwierzytelniające i ścieżki określone w zadaniach i właściwościach profilu Kaspersky Endpoint Security.

Zawartość pliku śledzenia Agenta autoryzacji

Plik śledzenia Agenta autoryzacji jest przechowywany w folderze System Volume Information i posiada następującą nazwę: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Oprócz ogólnych danych, plik śledzenia Agenta autoryzacji zawiera informacje o działaniu Agenta autoryzacji oraz o działaniach wykonywanych przez użytkownika na Agencie autoryzacji.

Śledzenie działania aplikacji

Śledzenie aplikacji to szczegółowy zapis akcji wykonanych przez aplikację oraz wiadomości o zdarzeniach, które występują w trakcie działania aplikacji. Podczas procesu śledzenia aplikacja tworzy zestaw plików z danymi dotyczącymi działania różnych komponentów aplikacji (na przykład SRV.log, WD.log i innych).

Śledzenie aplikacji powinno odbywać się pod nadzorem pomocy technicznej Kaspersky.

W celu utworzenia pliku śledzenia aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W otwartym oknie kliknij przycisk **Narzędzia pomocy technicznej**.
3. Użyj przełącznika **Włącz śledzenie aplikacji**, aby włączyć lub wyłączyć śledzenie działania aplikacji.
4. Z listy rozwijalnej **Śledzenie** wybierz tryb śledzenia aplikacji:
   - **Z ograniczeniem rozmiaru**. Zapisuje ślady do ograniczonej liczby zestawów plików o ograniczonym rozmiarze i nadpisuje starsze pliki po osiągnięciu maksymalnego rozmiaru. Jeśli ten tryb jest zaznaczony, możesz zdefiniować maksymalną liczbę zestawów plików do rotacji oraz maksymalny rozmiar dla każdego zestawu plików.

     Domyślnie aplikacja zapisuje pięć zestawów plików śledzenia. Rozmiar każdego zestawu plików to 3072 MB. Dzięki temu do zapisania plików śledzenia potrzebne będzie 15 GB wolnego miejsca na dysku.
   - **Bez ograniczeń**. Zapisuje jeden plik śledzenia (bez ograniczenia rozmiaru).
5. Z listy rozwijalnej **Poziom** wybierz poziom śledzenia:
   - **Normalny** oznacza, że plik śledzenia zapisuje komunikaty o wszystkich błędach, ostrzeżenia, a także informacje o normalnym działaniu aplikacji (domyślnie).
   - **Szczegółowy** oznacza, że plik śledzenia zapisuje wszystkie informacje o działaniu aplikacji.

   Dodatkowe poziomy śledzenia są dostępne, jeśli zarządzasz ustawieniami śledzenia aplikacji w wierszu poleceń. Zaleca się uzgodnić wymagany poziom śledzenia ze specjalistami z pomocy technicznej. Jeżeli z pomocy technicznej nie zostały przekazane żadne zalecenia, należy ustawić poziom śledzenia na **Normalny**.

Jeśli śledzenie aplikacji zostało włączone w wierszu poleceń i ustawiono inny poziom śledzenia niż **Normalny** lub **Szczegółowy**, lista rozwijana **Poziom** jest ustawiana na **Normalny**.

6. Aby zatrzymać proces śledzenia, wróć do okna **Narzędzia pomocy technicznej** i wyłącz śledzenie.

Pliki śledzenia możesz także utworzyć podczas instalowania aplikacji z poziomu wiersza poleceń, w tym przy użyciu pliku setup.ini.

W rezultacie pliki śledzenia działania aplikacji zostaną utworzone w folderze `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. Po utworzeniu plików śledzenia, wyślij pliki do pomocy technicznej Kaspersky.

Kaspersky Endpoint Security automatycznie usuwa pliki śledzenia podczas usuwania aplikacji. Możliwe jest również ręczne usunięcie tych plików. W tym celu należy włączyć śledzenie i zatrzymać działanie aplikacji.

Śledzenie wydajności aplikacji

Kaspersky Endpoint Security umożliwia otrzymywanie informacji o problemach z działaniem komputera podczas korzystania z aplikacji. Na przykład, możesz otrzymywać informacje o opóźnieniach w ładowaniu systemu operacyjnego po zainstalowaniu aplikacji. Aby to zrobić, Kaspersky Endpoint Security tworzy pliki śledzenia wydajności. *Śledzenie wydajności* odnosi się do rejestrowania działań wykonanych przez aplikację w celu zdiagnozowania problemów z działaniem Kaspersky Endpoint Security. Aby otrzymywać informacje, Kaspersky Endpoint Security używa usługi Śledzenie zdarzeń systemu Windows (ETW). Pomoc techniczna Kaspersky jest odpowiedzialna za diagnozowanie problemów z Kaspersky Endpoint Security i znalezienie powodów tych problemów.

Śledzenie aplikacji powinno odbywać się pod nadzorem pomocy technicznej Kaspersky.

W celu utworzenia pliku śledzenia wydajności:

1. W oknie głównym aplikacji kliknij przycisk .
2. W otwartym oknie kliknij przycisk **Narzędzia pomocy technicznej**.
3. Użyj przełącznika **Włącz śledzenie wydajności**, aby włączyć lub wyłączyć śledzenie wydajności aplikacji.
4. Z listy rozwijalnej **Śledzenie** wybierz tryb śledzenia aplikacji:
   - **Z ograniczeniem rozmiaru**. Zapisuje ślady do ograniczonej liczby plików o ograniczonym rozmiarze i nadpisuje starsze pliki po osiągnięciu maksymalnego rozmiaru. Jeśli ten tryb jest wybrany, możesz zdefiniować maksymalny rozmiar każdego pliku.
   - **Bez ograniczeń**. Zapisuje jeden plik śledzenia (bez ograniczenia rozmiaru).

5. Z listy rozwijalnej **Poziom** wybierz poziom śledzenia:

   - **Lekki**. Kaspersky Endpoint Security analizuje najważniejsze procesy systemu operacyjnego związane z działaniem.
   - **Szczegółowy**. Kaspersky Endpoint Security analizuje wszystkie procesy systemu operacyjnego związane z działaniem.

6. Z listy rozwijalnej **Typ śledzenia** wybierz typ śledzenia:

   - **Informacje podstawowe**. Kaspersky Endpoint Security analizuje procesy podczas działania systemu operacyjnego. Użyj tego typu śledzenia, jeśli problem występuje po załadowaniu systemu operacyjnego, takich jak problem z uzyskaniem dostępu do internetu w przeglądarce.
   - **Po ponownym uruchomieniu**. Kaspersky Endpoint Security analizuje procesy tylko podczas ładowania systemu operacyjnego. Po załadowaniu systemu operacyjnego, Kaspersky Endpoint Security zatrzymuje śledzenie. Użyj tego typu śledzenia, jeśli problem jest związany z opóźnieniem ładowania systemu operacyjnego.

7. Uruchom komputer ponownie i spróbuj odtworzyć problem.

8. Aby zatrzymać proces śledzenia, wróć do okna Narzędzia pomocy technicznej i wyłącz śledzenie.

   W rezultacie plik śledzenia zostanie utworzony w folderze `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. Po utworzeniu pliku śledzenia, wyślij plik do pomocy technicznej Kaspersky.

Zapisywanie zrzutu pamięci

Plik zrzutu pamięci zawiera wszystkie informacje o pamięci roboczej procesów Kaspersky Endpoint Security w momencie utworzenia pliku zrzutu.

> Zapisane pliki zrzutów mogą zawierać poufne dane. Aby kontrolować dostęp do danych, musisz niezależnie zapewnić bezpieczeństwo plików zrzutów pamięci.

Pliki zrzutów pamięci są przechowywane na komputerze tak długo, jak aplikacja jest używana i są trwale usuwane, gdy aplikacja jest usuwana. Pliki zrzutów pamięci są przechowywane w folderze `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`.

Jak w Konsoli administracyjnej (MMC) włączyć zapisywanie zrzutów pamięci?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.
4. W sekcji **Informacje debugowania** kliknij przycisk **Ustawienia**.
5. W sekcji użyj pola wyboru **Włącz zapisywanie zrzutów pamięci**, aby włączyć lub wyłączyć zapisywanie zrzutów pamięci aplikacji.
6. Zapisz swoje zmiany.

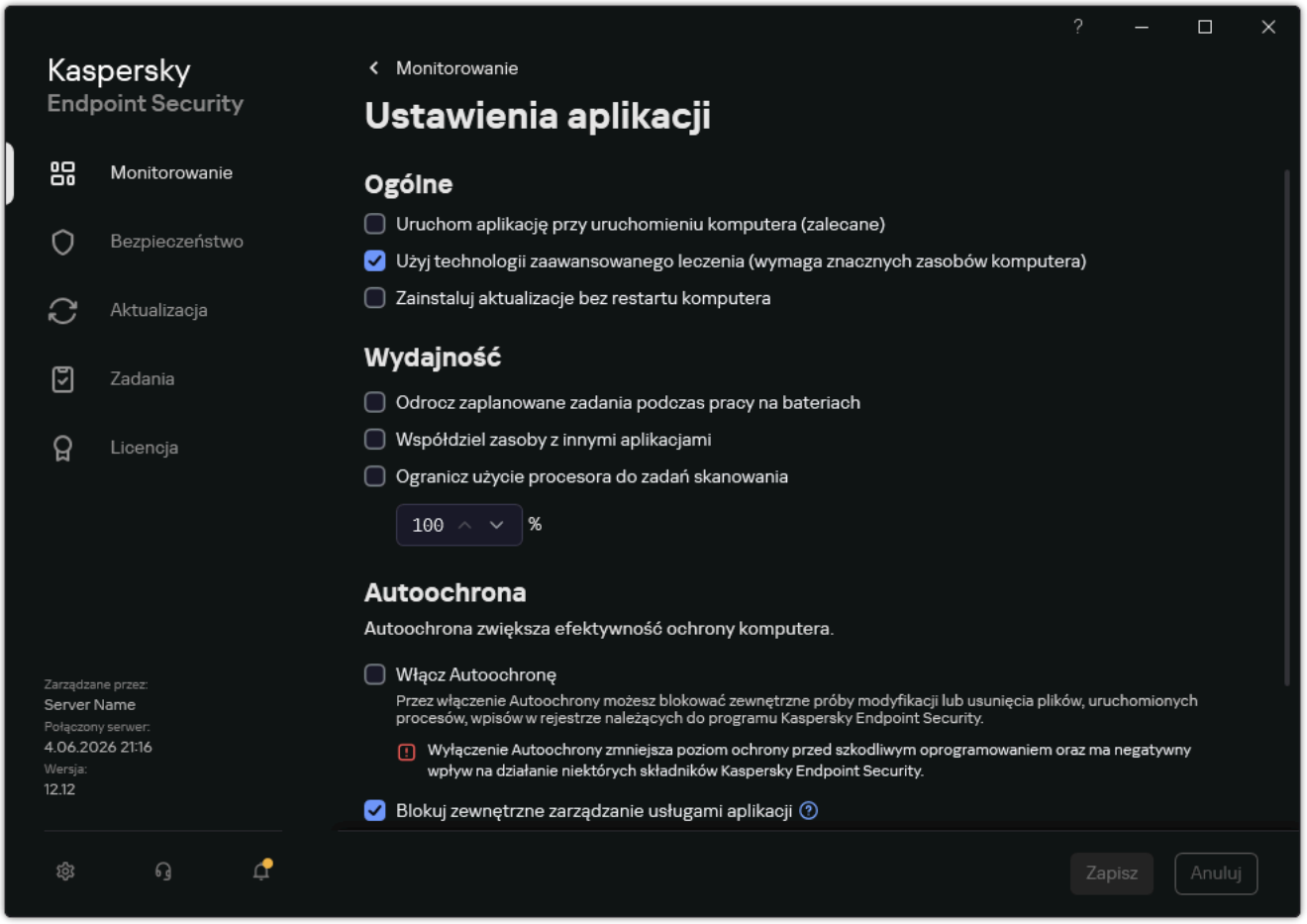
Jak w konsoli Web Console i Cloud Console włączyć zapisywanie zrzutów pamięci?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Pomoc techniczna**.
5. W sekcji **Informacje debugowania** użyj pola **Zapisywanie zrzutów pamięci WŁĄCZONE**, aby włączyć lub wyłączyć zapisywanie zrzutów pamięci aplikacji.
6. Zapisz swoje zmiany.

Jak w interfejsie aplikacji włączyć zapisywanie zrzutów pamięci?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.



Ustawienia Kaspersky Endpoint Security for Windows

3. W sekcji **Informacje debugowania** użyj pola **Włącz zapisywanie zrzutów pamięci**, aby włączyć lub wyłączyć zapisywanie zrzutów pamięci aplikacji.
4. Zapisz swoje zmiany.

Ochrona plików zrzutu i plików śledzenia

Pliki zrzutów pamięci oraz pliki śledzenia zawierają informacje o systemie operacyjnym i mogą także zawierać dane użytkownika. Aby zablokować dostęp do tych danych, możesz włączyć ochronę plików zrzutu i plików śledzenia.

Jeśli ochrona plików zrzutu i plików śledzenia jest włączona, dostęp do plików mogą uzyskać następujący użytkownicy:

- Dostęp do plików zrzutu może uzyskać administrator systemowy i administrator lokalny, a także użytkownik, który włączył zapisywanie plików zrzutu pamięci i plików śledzenia.
- Dostęp do plików śledzenia może uzyskać tylko administrator systemowy i administrator lokalny.

Jak włączyć ochronę plików zrzutów i plików śledzenia w Konsoli administracyjnej (MMC)?

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz **Zasady**.
2. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
3. W oknie zasady wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.
4. W sekcji **Informacje debugowania** kliknij przycisk **Ustawienia**.
5. W sekcji, która zostanie otwarta, użyj pola wyboru **Włącz ochronę zrzutów pamięci i plików śledzenia**, aby włączyć lub wyłączyć ochronę plików.
6. Zapisz swoje zmiany.

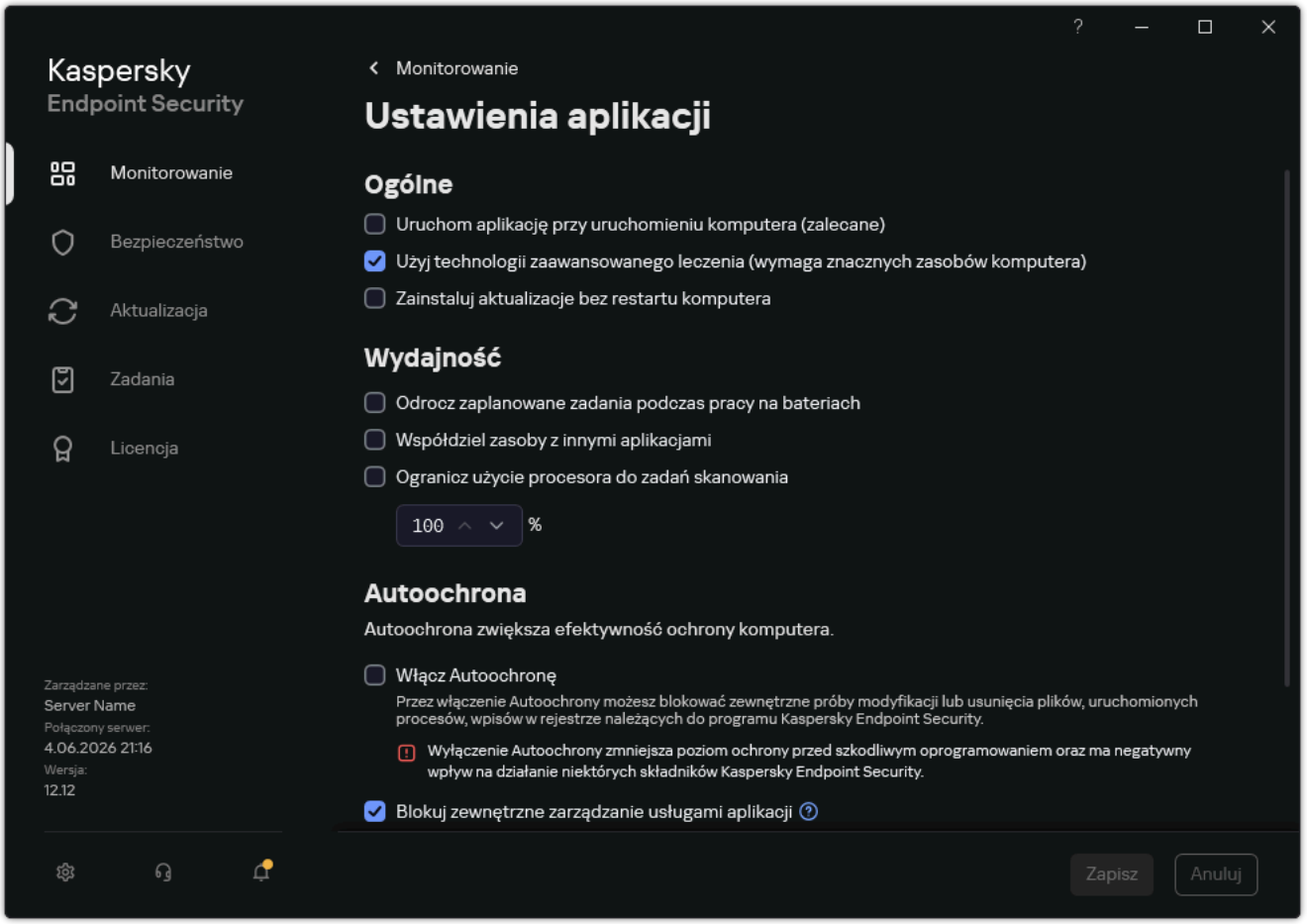
Jak włączyć ochronę plików zrzutów i plików śledzenia w Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Zarządzanie zasobami** → **Zasady**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.

   Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Pomoc techniczna**.
5. W sekcji **Informacje debugowania** użyj pola **Ochrona zrzutów pamięci i plików śledzenia WŁĄCZONA**, aby włączyć lub wyłączyć ochronę plików.
6. Zapisz swoje zmiany.

Jak włączyć ochronę plików zrzutów i plików śledzenia w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk ⚙.
2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Ustawienia aplikacji**.



Ustawienia Kaspersky Endpoint Security for Windows

3. W sekcji **Informacje debugowania** użyj pola **Włącz ochronę zrzutów pamięci i plików śledzenia**, aby włączyć lub wyłączyć ochronę plików.
4. Zapisz swoje zmiany.

Pliki zrzutu i pliki śledzenia, które zostały zapisane, gdy ochrona była aktywna, pozostaną chronione nawet po wyłączeniu tej funkcji.

Uzyskiwanie danych systemu operacyjnego (Kaspersky Get System Info)

Po zainstalowaniu aplikacji Kaspersky Endpoint Security system operacyjny lub aplikacja mogą nie działać prawidłowo. Występuje konflikt pomiędzy aplikacją i oprogramowaniem lub sterownikami podzespołów komputera.

Aby zidentyfikować przyczynę problemu, Pomoc techniczna Kaspersky potrzebuje raportu z narzędzia Kaspersky Get System Info (zwanego dalej GSI). Szczegółowe informacje na temat korzystania z tego narzędzia znajdziesz w Bazie wiedzy Kaspersky.

Ograniczenia i uwagi

Kaspersky Endpoint Security posiada kilka ograniczeń, które nie są krytyczne dla działania aplikacji.

Instalowanie aplikacji

- Więcej informacji na temat obsługi systemów operacyjnych Microsoft Windows 10, Microsoft Windows Server 2016 i Microsoft Windows Server 2019 można znaleźć w Bazie wiedzy na stronie działu pomocy technicznej.
- Więcej informacji na temat obsługi systemów operacyjnych Microsoft Windows Server 11 i Microsoft Windows Server 2022 można znaleźć w Bazie wiedzy na stronie działu pomocy technicznej.
- Po zainstalowaniu aplikacji na zainfekowanym komputerze, nie informuje ona użytkownika o konieczności przeprowadzenia skanowania. Mogą wystąpić problemy z aktywacją aplikacji. Aby rozwiązać te problemy, uruchom Skanowanie obszarów krytycznych.
- Jeśli w plikach setup.ini i setup.reg używane są znaki inne niż ASCII (na przykład znaki cyrylicy), zalecamy edycję pliku w Notepad.exe i zapisanie go w kodowaniu UTF-16LE. Inne opcje kodowania nie są obsługiwane.
- Aplikacja nie obsługuje znaków innych niż ASCII podczas określania ścieżki instalacji aplikacji w ustawieniach pakietu instalacyjnego.
- Jeśli ustawienia aplikacji są importowane z pliku CFG, wartość ustawienia, które definiuje uczestnictwo w Kaspersky Security Network, nie jest stosowana. Po zaimportowaniu ustawień przeczytaj treść Oświadczenia Kaspersky Security Network i potwierdź zgodę na uczestnictwo w Kaspersky Security Network. Treść Oświadczenia możesz przeczytać w interfejsie aplikacji lub w pliku ksn_*.txt, znajdującym się w folderze zawierającym pakiet dystrybucyjny aplikacji.
- Jeśli chcesz usunąć, a następnie ponownie zainstalować szyfrowanie (FLE lub FDE) lub komponent Kontrola urządzeń, musisz uruchomić system ponownie przed ponowną instalacją.
- Jeśli używasz systemu operacyjnego Microsoft Windows 10, po usunięciu komponentu Szyfrowanie plików (FLE) musisz uruchomić system ponownie.
- Podczas usuwania poszczególnych komponentów aplikacji (na przykład przy pomocy zadania *Zmiana składników aplikacji*), konieczne może być ponowne uruchomienie komputera.
- We właściwościach zadania *Zmiana składników aplikacji*, podczas przełączania trybu instalacji (**Tryb oddzielny** / **Tryb powiązany**), synchronizacja zestawu komponentów między trybami nie jest obsługiwana. Aplikacja synchronizuje zestaw komponentów pomiędzy trybami po ponownym otwarciu właściwości zadania.
- Instalacja aplikacji może zakończyć się błędem stwierdzającym, że *na komputerze została zainstalowana aplikacja bez nazwy lub z nazwą, która jest nieczytelna*. To oznacza, że na komputerze pozostają niekompatybilne aplikacje lub ich fragmenty. Aby usunąć artefakty lub niekompatybilne aplikacje, wyślij zgłoszenie ze szczegółowym opisem sytuacji do pomocy technicznej Kaspersky za pośrednictwem Kaspersky CompanyAccount.
- Jeśli usunięcie Kaspersky Endpoint Security zostało anulowane, rozpocznij odzyskiwanie aplikacji po ponownym uruchomieniu komputera.
- Aplikacja wymaga Microsoft .NET Framework 4.0 lub nowsza. Microsoft .NET Framework Wersja 4.6.1 ma luki w zabezpieczeniach. Jeśli używasz Microsoft .NET Framework 4.6.1, musisz zainstalować aktualizacje zabezpieczeń. Więcej informacji o aktualizacjach zabezpieczeń Microsoft .NET Framework możesz znaleźć na stronie internetowej pomocy technicznej firmy Microsoft.

- Jeśli aplikacja została niepomyślnie zainstalowana z komponentem Kaspersky Endpoint Agent wybranym w serwerowym systemie operacyjny i zostało wyświetlone okno *Błąd Koordynatora Instalatora Windows*, zapoznaj się z instrukcjami na stronie internetowej pomocy technicznej firmy Microsoft.

- Jeśli aplikacja została zainstalowana lokalnie w trybie nieinteraktywnym, użyj udostępnionego pliku setup.ini, aby zastąpić zainstalowane komponenty.

- Po zainstalowaniu programu Kaspersky Endpoint Security for Windows w niektórych konfiguracjach Windows 7, Windows Defender będzie dalej działać. Aby zapobiec obniżeniu wydajności systemu, zalecane jest ręczne wyłączenie Windows Defender.

- Podczas instalacji programu Kaspersky Endpoint Security for Windows na serwerze z zainstalowanymi aplikacjami Kaspersky Security for Windows Server (KSWS) oraz Windows Defender należy ponownie uruchomić komputer. Ponowne uruchomienie systemu jest konieczne, nawet jeśli włączyłeś instalację aplikacji bez ponownego uruchamiania systemu. Program Windows Defender for Windows Server znajduje się na liście programów niekompatybilnych z Kaspersky Endpoint Security for Windows. Przed instalacją aplikacji instalator usuwa program Windows Defender for Windows Server. Usunięcie niekompatybilnego oprogramowania powoduje konieczność ponownego uruchomienia systemu.

- Przed zainstalowaniem Kaspersky Endpoint Security for Windows (KES) na serwerze z zainstalowaną aplikacją Kaspersky Security for Windows Server (KSWS), należy wyłączyć Ochronę hasłem KSWS. Po migracji z KSWS do KES, włącz Ochronę hasłem w ustawieniach aplikacji.

- Aby zainstalować aplikację na komputerach z Windows 7 lub Windows Server 2008. R2 z wdrożonym oprogramowaniem Veeam Backup & Replication, może być niezbędne ponowne uruchomienie komputera i instalacji.

- Migracja z Kaspersky Small Office Security (KSOS) do Kaspersky Endpoint Security (KES) z włączoną ochroną hasłem jest możliwa tylko w przypadku KSOS w wersji co najmniej 21.16.*.*. Aby zmigrować starsze wersje KSOS, musisz wyłączyć ochronę hasłem lub ręcznie usunąć KSOS. Migracja z KSOS do KES z wyłączoną ochroną hasłem jest wykonywana poprawnie.

- Nie można zainstalować Kaspersky Endpoint Security na rozruchowym dysku wymiennym. Podczas instalacji Kaspersky Endpoint Security wyświetla komunikat o błędzie: *Wybrałeś niewłaściwy folder lub dysk. Aplikacja musi zostać zainstalowana na lokalnym dysku twardym*. Jeśli uda Ci się zainstalować aplikację na dysku wymiennym, korzystając z narzędzi innych firm, może to spowodować awarię systemu operacyjnego (BSOD) podczas procesu rozruchu. Oznacza to, że Kaspersky Endpoint Security nie obsługuje funkcji Windows To Go i podobnych rozwiązań. Aby przeskanować komputer z dysku wymiennego, możesz skorzystać z bezpłatnej aplikacji Kaspersky Rescue Disk.

- Instalacja Kaspersky Endpoint Security ze składnikami sieciowymi na serwerze terminali z sesjami RDP dla wielu użytkowników wymaga uwzględnienia pewnych szczególnych kwestii. System operacyjny wymusza zakończenie wszystkich sesji użytkowników po zakończeniu sesji administratora. Aby połączyć się z serwerem terminali, musisz ponownie uruchomić serwer lub zalogować się do systemu lokalnie. Takie zachowanie jest podyktowane specyfiką systemu operacyjnego.

- Jeżeli wtyczki webowe Kaspersky Endpoint Security for Windows (kompilacja 12.11.0.2004) i Kaspersky Endpoint Security for Linux (kompilacja 12.4.0.1354) są zainstalowane w Kaspersky Security Center 16.0 lub Kaspersky Security Center 16.1, aktualizacja wtyczki webowej Kaspersky Endpoint Security for Windows do wersji 12.11.0.6004 może prowadzić do nieprawidłowego działania zasad Kaspersky Endpoint Security for Linux.

  Możliwe rozwiązanie: przejdź do **Ustawienia** → okno **Wtyczki webowa**, i usuń z listy wtyczkę webową Kaspersky Endpoint Security for Windows, wtyczkę webową Kaspersky Endpoint Security for Linux oraz Unified Protection and Management Plug-in. Następnie najpierw zainstaluj wtyczkę webową Kaspersky Endpoint Security for Linux a później wtyczkę webową Kaspersky Endpoint Security for Windows.

- Lista komponentów w Web Console jest nieprawidłowo wyświetlana we właściwościach pakietu instalacyjnego Kaspersky Endpoint Security 12.11 for Windows. Osobny komponent Anti-Cryptor nie jest dostępny w tej wersji aplikacji. Komponent Wykrywanie zachowań obejmuje ochronę folderów współdzielonych przed funkcjami szyfrowania zewnętrznego. Ta funkcja jest osobnym komponentem w Kaspersky Endpoint Security 12.12 for Windows. Lista komponentów wyświetla się jednak poprawnie w Konsoli administracyjnej (MMC).

Aktualizowanie aplikacji

- Począwszy od wersji 11.0.0, możesz zainstalować wtyczkę MMC Kaspersky Endpoint Security for Windows na poprzedniej wersji wtyczki. Aby wrócić do poprzedniej wersji wtyczki, usuń bieżącą wersję wtyczki i zainstaluj poprzednią wersję wtyczki.

- Podczas aktualizowania Kaspersky Endpoint Security 11.0.0 lub 11.0.1 for Windows, ustawienia lokalnego terminarza dla zadań *Aktualizacja baz danych i modułów aplikacji*, *Skanowanie obszarów krytycznych*, *Skanowanie niestandardowe* i *Sprawdzanie integralności aplikacji* nie są zapisywane.

- Na komputerach działających pod kontrolą systemu Windows 10 w wersji 1903 i 1909, aktualizacje z Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (wersja 10.3.3.275), Service Pack 2 Maintenance Release 4 (wersja 10.3.3.304), 11.0.0 i 11.0.1 z zainstalowanym komponentem Szyfrowanie plików (FLE) może zakończyć się błędem. Jest to spowodowane tym, że w systemie Windows 10 w wersji 1903 i 1909 szyfrowanie plików nie jest obsługiwane dla tych wersji Kaspersky Endpoint Security for Windows. Przed zainstalowaniem tej aktualizacji zalecane jest usunięcie komponentu szyfrowania plików.

- Aplikacja wymaga programu Microsoft .NET Framework 4.0 lub nowszego. Microsoft .NET Framework 4.6.1 posiada luki. Jeśli używasz Microsoft .NET Framework 4.6.1, musisz zainstalować aktualizacje zabezpieczeń. Więcej informacji o aktualizacjach zabezpieczeń Microsoft .NET Framework możesz znaleźć na stronie internetowej pomocy technicznej firmy Microsoft.

- Jeśli aktualizujesz Kaspersky Endpoint Security, aplikacja wyłącza korzystanie z KSN, dopóki nie zaakceptujesz Oświadczenia Kaspersky Security Network. Dodatkowo, stan komputera może zostać zmieniony na *Krytyczny* w Kaspersky Security Center; zostanie odebrane zdarzenie *Serwery KSN są niedostępne*. Jeśli używasz Kaspersky Managed Detection and Response, otrzymasz zdarzenia dotyczące naruszeń związanych z działaniem rozwiązania. Użycie KSN jest wymagane do działania Kaspersky Managed Detection and Response. Kaspersky Endpoint Security włącza użycie KSN po zastosowaniu zasady, w której administrator akceptuje warunki korzystania z KSN. Po zaakceptowaniu Oświadczenia Kaspersky Security Network, Kaspersky Endpoint Security wznawia jego działanie.

- Po aktualizacji Kaspersky Endpoint Security do wersji 11.10.0 lub nowszej bez ponownego uruchomienia, na komputerze będą zainstalowane dwie aplikacje Kaspersky Endpoint Security. Nie usuwaj ręcznie poprzedniej wersji aplikacji. Poprzednia wersja zostanie usunięta automatycznie po ponownym uruchomieniu komputera.

- Po aktualizacji aplikacji Kaspersky Endpoint Security na komputerze z systemem Microsoft Windows 11, menu kontekstowe pliku może wyświetlać elementy zarówno dla poprzednich, jak i nowych wersji aplikacji. Uruchom ponownie komputer dwukrotnie, aby zapewnić prawidłowe działanie menu kontekstowego pliku.

- Jeśli autoochrona aplikacji jest wyłączona, a wszystkie karty sieciowe zatrzymane, komponenty sieciowe aplikacji nie będą działać pomiędzy zakończeniem aktualizacji aplikacji a ponownym uruchomieniem komputera. Składniki sieciowe aplikacji obejmują ochronę WWW, ochronę poczty, ochronę sieci, zaporę sieciową, ochronę przed włamaniami i kontrolę sieci. Aby aplikacja działała poprawnie, uruchom ponownie komputer.

- Ochrona przed atakami BadUSB nie działa pomiędzy zakończeniem aktualizacji aplikacji a ponownym uruchomieniem komputera. Aby aplikacja działała poprawnie, uruchom ponownie komputer.

- Aplikacji nie można uaktualnić, jeśli poprzedni proces uaktualniania nie został ukończony. Aby aplikacja działała poprawnie, uruchom ponownie komputer.

- Po zaktualizowaniu aplikacji z wersji wcześniejszych niż Kaspersky Endpoint Security 11 for Windows, komputer musi być uruchomiony ponownie.

- Jeśli zarządzasz aplikacją Kaspersky Endpoint Security przy użyciu Kaspersky Security Center Cloud Console, lokalna aktualizacja aplikacji nie jest dozwolona. Podczas lokalnej aktualizacji aplikacji nie można zaakceptować Umowy o przetwarzaniu danych dla Kaspersky Security Center Cloud Console.

Obsługa architektury Arm

- Instalacja Kaspersky Endpoint Security w trybie Light Agent na maszynach wirtualnych opartych na architekturze ARM nie jest obsługiwana.

- Rozwiązanie Kaspersky Disk Encryption nie jest obsługiwane na komputerach opartych na architekturze ARM.

- Szyfrowanie plików nie jest obsługiwane na komputerach opartych na architekturze ARM.

- Szyfrowanie dysków wymiennych nie jest obsługiwane na komputerach opartych na architekturze ARM.

- Na komputerach z systemem Windows 11 dla architektury Arm64 agent EDR Agent nie jest zgodny z Bitdefender Endpoint Security Tools.

- Funkcje ochrony sygnału audio i ochrony dostępu do kamery internetowej nie są obsługiwane na komputerach opartych na architekturze ARM.

- Na komputerach opartych na architekturze Arm rozszerzenie Ochrony poczty obsługuje 32- i 64-bitowe wersje programów Outlook 2016, Outlook 2021, Outlook 2024 i Outlook 365 dla architektury Arm64.

- Kaspersky Endpoint Security nie wysyła obiektów przeznaczonych dla architektury Arm do Kaspersky Sandbox.

- Kontrola drukowania nie jest obsługiwana na komputerach opartych na architekturze Arm.

- Integracja z Kaspersky Endpoint Detection and Response Expert (cloud) nie jest obsługiwana na komputerach opartych na architekturze Arm.

- Na komputerach opartych na architekturze Arm zadanie *Skanowanie IOC* obsługuje pliki e-mail tylko z następujących klientów poczty: 32-bitowe i 64-bitowe wersje programu Outlook 2016 oraz Outlook 2021, 2024 i 365 dla architektury Arm64.

Obsługa platform serwerowych

- Na serwerach z włączoną *deduplikacją danych* trzeba dodać plik fsdmhost.exe do listy zaufanych aplikacji. Pomaga to zoptymalizować wydajność aplikacji i zapobiegać nadmiernemu obciążeniu procesora.

- System plików ReFS jest obsługiwany z ograniczeniami:

  - Kaspersky Endpoint Security może niepoprawnie przetwarzać zdarzenia dotyczące leczenia zagrożeń. Na przykład, jeśli aplikacja usunęła szkodliwy plik, raport może zawierać wpis Obiekt nie został przetworzony. W tym samym czasie Kaspersky Endpoint Security wyleczy zagrożenia zgodnie z ustawieniami aplikacji. Kaspersky Endpoint Security może także zduplikować zdarzenie *Obiekt zostanie wyleczony po restarcie* dla tego samego obiektu.

  - Ochrona plików może pominąć niektóre zagrożenia. W tym samym czasie Skanowanie w poszukiwaniu złośliwego oprogramowania działa poprawnie.

  - Po uruchomieniu zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*, wykluczenia ze skanowania, dodane do iChecker, są resetowane po ponownym uruchomieniu serwera.

  - Technologia iSwift nie jest obsługiwana. Kaspersky Endpoint Security nie uwzględnia wykluczeń ze skanowania dodanych przy użyciu technologii iSwift.

  - Kaspersky Endpoint Security nie wykrywa plików eicar.com i susp-eicar.com, jeśli plik meicar.exe istniał na komputerze przed zainstalowaniem Kaspersky Endpoint Security.

  - Kaspersky Endpoint Security może niepoprawnie wyświetlać powiadomienia dotyczące leczenia zagrożeń. Na przykład, aplikacja może wyświetlić powiadomienie dotyczące zagrożenia dla wcześniej wyleczonego zagrożenia.

- Technologie Szyfrowanie plików (FLE) i Kaspersky Disk Encryption (FDE) nie są obsługiwane na platformach serwerowych. Jednocześnie Kaspersky Endpoint Security może niepoprawnie przetwarzać zdarzenia dotyczące szyfrowania danych.

- W serwerowych systemach operacyjnych nie jest wyświetlane żadne ostrzeżenie dotyczące konieczności przeprowadzenia zaawansowanego leczenia.

- System Microsoft Windows Server 2008 został wykluczony ze wsparcia. Instalowanie aplikacji na komputerze działającym pod kontrolą systemu operacyjnego Microsoft Windows Server 2008 nie jest obsługiwane.

- Kaspersky Endpoint Security zainstalowany na serwerze z wdrożonym Microsoft Data Protection Manager (DPM) może spowodować nieprawidłowe działanie DPM. Ma to związek z ograniczeniami w działaniu DPM. Aby wyeliminować nieprawidłowe działanie, dodaj dyski lokalne serwera do wykluczeń dla komponentu Ochrona plików i zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Tryb Server Core jest obsługiwany z ograniczeniami:

  - Lokalny interfejs graficzny nie jest dostępny, w tym powiadomienia, wiadomości wyskakujące i inne kontrolki interfejsu. Aplikacja nie może wyświetlić okien z pytaniem, w tym następujących okien:

    - Okno z pytaniem o potwierdzenie aktualizacji modułu i wersji aplikacji;

    - Pytanie o ponowne uruchomienie komputera;

    - Pytanie o dane uwierzytelniające serwera proxy;

    - Pytaj o uzyskanie dostępu do urządzenia (Kontrola urządzeń).

- Brak następujących komponentów: Ochrona WWW, Ochrona poczty, Kontrola sieci, Ochrona przed atakami BadUSB.
- Moduł Anti-Bridging nie jest dostępny.
- Możesz tylko zaakceptować Oświadczenie Kaspersky Security Network w zasadzie aplikacji, w konsoli Kaspersky Security Center.
- Szyfrowanie dysków funkcją BitLocker jest dostępne tylko z Trusted Platform Module (TPM). Kod PIN / hasło nie może zostać użyte do zaszyfrowania, ponieważ aplikacja nie może wyświetlić okna z pytaniem o hasło do autoryzacji przed rozruchem. Jeśli w systemie operacyjnym jest włączony tryb kompatybilności z metodą szyfrowania weryfikowanych standardem FIPS (Federal Information Processing Standard), podłącz dysk przenośny do zapisania klucza szyfrowania przed rozpoczęciem szyfrowania dysku.

Obsługa platform wirtualnych

- Szyfrowanie całego dysku (FDE) na maszynach wirtualnych Hyper-V nie jest obsługiwane.
- Szyfrowanie całego dysku (FDE) na platformach wirtualnych Citrix nie jest obsługiwane.
- Wielosesyjny Windows 10 Enterprise jest obsługiwany z ograniczeniami:
  - Kaspersky Endpoint Security leczy aktywne zagrożenia bez powiadamiania użytkownika, tak jak podczas leczenia aktywnych zagrożeń na serwerach. Ponieważ system operacyjny dalej działa w trybie wielosesyjnym, inni aktywni użytkownicy mogą utracić swoje dane, jeśli zagrożenie nie zostanie zneutralizowane od razu.
  - Szyfrowanie całego dysku (FDE) nie jest obsługiwane.
  - Zarządzanie funkcją BitLocker nie jest obsługiwane.
  - Używanie Kaspersky Endpoint Security z dyskami wymiennymi nie jest obsługiwane. Infrastruktura Microsoft Azure definiuje dyski wymienne jako dyski sieciowe.
- Instalacja i używanie funkcji szyfrowania na poziomie plików (FLE) na platformach wirtualnych Citrix nie są obsługiwane.
- Aby włączyć kompatybilność Kaspersky Endpoint Security for Windows z Citrix PVS, wykonaj instalację z włączoną opcją **Zapewnij zgodność z Citrix PVS**. Ta opcja może być włączona w Kreatorze instalacji lub przy użyciu parametru wiersza poleceń `/pCITRIXCOMPATIBILITY=1`. W przypadku zdalnej instalacji należy zmodyfikować plik KUD, dodając do niego następujący parametr: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. Przed rozpoczęciem klonowania należy wyłączyć autoochronę, aby klonować maszyny wirtualne, które korzystają z vDisk.
- Przygotowując urządzenie szablonowe do głównego obrazu Citrix XenDesktop z zainstalowanym programem Kaspersky Endpoint Security for Windows i Agentem sieciowym Kaspersky Security Center, dodaj do pliku konfiguracyjnego następujące typy wykluczeń:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Więcej informacji o Citrix XenDesktop można znaleźć na stronie internetowej pomocy technicznej Citrix.

- W niektórych przypadkach próba bezpiecznego odłączenia nośnika wymiennego może zakończyć się niepowodzeniem na maszynie wirtualnej, która jest wdrażana na hipernadzorcy VMware ESXi. Spróbuj ponownie bezpiecznie odłączyć urządzenie.

- Rozwiązanie Kaspersky Endpoint Security jest zgodne z hipernadzorcą VMware ESXi, ale ma następujące ograniczenia:

  - Rozwiązanie Kaspersky Endpoint Security może być niezgodne ze sterownikami Guest Introspection (vnetWFP.sys, vnetFLT.sys i innymi). Aby rozwiązać problem niezgodności, należy zaktualizować sterowniki do najnowszej wersji lub je odinstalować.

  - W niektórych przypadkach próba bezpiecznego usunięcia dysku wymiennego na maszynie wirtualnej może się nie powieść. Spróbuj ponownie bezpiecznie odłączyć urządzenie.

- Instalacja Kaspersky Endpoint Security na maszynach wirtualnych za pomocą agenta Citrix VDA może zakończyć się błędem zgodności. Dzieje się tak, ponieważ Citrix Provisioning Services ma ograniczoną zgodność z rozwiązaniami antywirusowymi. Aby zapoznać się z najlepszymi praktykami korzystania z rozwiązań antywirusowych w ramach usług Citrix Provisioning Services, zapoznaj się ze Stroną pomocy technicznej Citrix.

- Kaspersky Endpoint Security pomija skanowanie dysku wymiennego, jeśli dysk jest podłączony do maszyny wirtualnej na hipernadzorcy Citrix (zadanie *Skanowanie dysków wymiennych*). W przypadku takich urządzeń system operacyjny wykrywa podłączony dysk wymienny jako dysk sieciowy. W takich przypadkach można użyć zadania *Skanowanie niestandardowe*. Zachowanie aplikacji w trybie standardowym i w trybie Light Agent jest takie samo.

- Jeśli program Kaspersky Endpoint Security jest zainstalowany na maszynie wirtualnej w infrastrukturze wykorzystującej technologię Citrix App Layering, pliki wykryte przez aplikację jako zainfekowane ze statusem *Obiekt zostanie usunięty po restarcie* nie zostaną automatycznie usunięte po ponownym uruchomieniu maszyny wirtualnej.

  Aby usunąć takie pliki, należy zamontować plik VHDX zawierający warstwę użytkownika na komputerze administratora Citrix App Layering i uruchomić skanowanie zamontowanego dysku w poszukiwaniu złośliwego oprogramowania.

Kompatybilność z Kaspersky Security Center

- W Kaspersky Security Center Web Console w wersji 14.1 i wcześniejszych, nazwy obszarów funkcjonalnych dla komponentów Kontrola dziennika i Monitor integralności plików nie są poprawnie wyświetlane w sekcji ustawień uprawnień dostępu użytkownika we właściwościach Serwera administracyjnego.

- Po naprawie aplikacji ochrona połączenia komputera z Serwerem administracyjnym jest wyłączona. Po naprawie aplikacji uruchom ponownie zadanie *Ochrona połączenia z Serwerem administracyjnym*.

- Okno **Wybierz użytkownika lub grupę użytkowników** w konsoli administracyjnej Kaspersky Security Center wyświetla tylko pierwszych 50 000 użytkowników z listy Kaspersky Security Center. Szczegółowe informacje można znaleźć w Pomocy Kaspersky Security Center.

- Podczas wyszukiwania zarządzanych urządzeń w Konsoli administracyjnej Kaspersky Security Center zakładka **Składniki aplikacji** może jednocześnie wyświetlać wiele wariantów nazwy tego samego komponentu aplikacji, w tym nazwy odpowiadające starszym wersjom Kaspersky Endpoint Security. Nazwy niektórych komponentów mogą się również powtarzać.

  Aby wyszukiwać według komponentu, wystarczy wybrać jeden z wyświetlonych wariantów. Bardziej szczegółowe informacje na temat wykrywania urządzeń można znaleźć w pomocy do Kaspersky Security Center.

Licencjonowanie

- Jeśli zostanie wyświetlona wiadomość systemowa *Błąd podczas pobierania danych*, sprawdź, czy komputer, na którym przeprowadzasz aktywację, posiada dostęp do sieci, bądź też skonfiguruj ustawienia aktywacji poprzez Kaspersky Security Center Activation Proxy.

- W interfejsie aplikacji data wygaśnięcia licencji jest wyświetlana w czasie lokalnym komputera.

- Instalacja aplikacji z osadzonym plikiem klucza na komputerze, który posiada niestabilny dostęp do internetu, może powodować tymczasowe wyświetlanie zdarzeń informujących, że aplikacja nie została aktywowana lub licencja nie pozwala na działanie komponentu. Dzieje się tak, ponieważ podczas instalacji aplikacja najpierw aktywuje osadzoną licencję testową. Wymaga to dostępu do Internetu.

- W trakcie obowiązywania okresu testowego instalacja dowolnej aktualizacji lub łaty aplikacji na komputerze, na którym jest niestabilne połączenie z internetem, może wpływać na tymczasowe wyświetlanie zdarzeń informujących, że aplikacja nie została aktywowana. Dzieje się tak, ponieważ podczas instalacji aktualizacji aplikacja najpierw aktywuje osadzoną licencję testową. Wymaga to dostępu do Internetu.

- Jeśli licencja testowa została automatycznie aktywowana podczas instalacji aplikacji, a następnie aplikacja została usunięta bez zapisywania informacji o licencji, aplikacja nie zostanie automatycznie aktywowana z licencją testową po ponownej instalacji. W tym przypadku przeprowadź ręczną aktywację aplikacji.

- Jeśli korzystasz z Kaspersky Security Center w wersji 11 oraz w Kaspersky Endpoint Security w wersji 14.1, raporty z działania komponentu mogą nie działać poprawnie. Jeśli zainstalowałeś komponenty Kaspersky Endpoint Security, które nie znajdują się w Twojej licencji, Agent sieciowy może wysłać błędy o stanie komponentów do dziennika zdarzeń systemu Windows. Aby uniknąć błędów, usuń komponenty, które nie znajdują się w Twojej licencji.

Ochrona poczty

- Podczas skanowania poczty z użyciem rozszerzenia modułu Ochrona poczty dla Microsoft Outlook zalecane jest korzystanie z trybu buforowanego programu Exchange (opcja Użyj trybu buforowanej wymiany).

- Kaspersky Endpoint Security nie obsługuje 64-bitowych wersji klienta poczty Microsoft Outlook. Oznacza to, że Kaspersky Endpoint Security nie skanuje plików Microsoft Outlook (plików PST i OST), jeśli na komputerze jest zainstalowana 64-bitowa wersja Microsoft Outlook, nawet jeśli poczta jest objęta zakresem skanowania.

- Kaspersky Endpoint Security nie obsługuje nowego klienta poczty Microsoft Outlook.

Silnik korygujący

- Aplikacja przywraca pliki tylko na urządzeniach, które posiadają system plików NTFS lub FAT32.

- Aplikacja przywraca pliki o rozmiarze do 100 MB.

- Aplikacja przywraca pliki z następującymi rozszerzeniami: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.

- Nie jest możliwe przywrócenie plików przechowywanych na dyskach sieciowych lub na dyskach CD/DVD wielokrotnego zapisu.

- Nie jest możliwe przywrócenie plików, które zostały zaszyfrowane za pomocą systemu szyfrowania plików (EFS). Więcej informacji na temat działania EFS znajdziesz na stronie internetowej firmy Microsoft.

- Aplikacja nie monitoruje modyfikacji na plikach, wykonywanych przez procesy na poziomie jądra systemu operacyjnego.

Zapora sieciowa

- Jeśli reguła pakietu sieciowego lub reguła sieciowa aplikacji określa nazwy DNS, Kaspersky Endpoint Security może wysyłać żądania do serwera DNS w celu ustalenia adresów IP tych zasobów. Zapora sieciowa wykorzystuje adresy IP do monitorowania aktywności sieciowej. Dlatego aplikacja rozkłada nazwy DNS na adresy IP. Zaleca się używanie nazw DNS w regułach tylko w przypadku komputerów w sieci LAN lub usług wewnętrznych.

- Aby określić regułę dla wszystkich adresów IPv6, należy dodać zakres adresów ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Zapora nie obsługuje maski ::/0.

- Filtrowanie pakietów lub połączeń według adresu lokalnego, interfejsu fizycznego i czasu życia pakietu (TTL) jest obsługiwane w następujących przypadkach:

  - Według adresu lokalnego dla pakietów lub połączeń wychodzących w regułach dla aplikacji (dla portu TCP i UDP) i regułach dla pakietów.

  - Według adresu lokalnego dla pakietów lub połączeń przychodzących (za wyjątkiem portu UDP) w regułach blokowania aplikacji i regułach dla pakietów.

  - Według czasu życia pakietu (TTL) w regułach blokowania dla pakietów przychodzących lub wychodzących.

  - Według interfejsu sieciowego dla pakietów lub połączeń przychodzących i wychodzących w regułach dla pakietów.

- Jeśli skonfigurowałeś kartę sieciową lub czas wygaśnięcia pakietu (TTL) dla zezwalającej reguł dla pakietu, priorytet tej reguły jest mniejszy niż blokująca reguła dla aplikacji. Innymi słowy, jeśli aktywność sieciowa aplikacji jest zablokowana (na przykład, aplikacja jest w grupie zaufania *Wysokie ograniczenia*), nie można na nią zezwolić przy użyciu reguły dla pakietu z tymi ustawieniami. We wszystkich pozostałych przypadkach priorytet reguły dla pakietu jest wyższy niż reguła sieciowa dla aplikacji.

- Podczas importowania reguł dla pakietów Zapory sieciowej program Kaspersky Endpoint Security może modyfikować nazwy reguł. Aplikacja określa reguły z identycznymi zestawami parametrów ogólnych: protokół, kierunek, porty zdalne i lokalne, czas wygaśnięcia pakietu (TTL). Jeśli ten zestaw parametrów ogólnych jest identyczny dla kilku reguł, aplikacja przypisze tę samą nazwę do tych reguł lub doda znacznik parametru do nazwy. W ten sposób Kaspersky Endpoint Security importuje wszystkie reguły dla pakietów, ale nazwa reguł, które posiadają identyczne ustawienia ogólne, może zostać zmodyfikowana.

- Jeśli w regule sieciowej włączyłeś raportowanie o zdarzeniach aplikacji, podczas przenoszenia aplikacji do innej grupy zaufania ograniczenia tejże grupy nie będą stosowane. Dlatego, jeśli aplikacja znajduje się w grupie Zaufane, nie będzie posiadała żadnych ograniczeń sieciowych. Następnie włączono raportowanie o zdarzeniach dla tej aplikacji i przeniesiono ją do grupy *Niezaufane*. Zapora sieciowa nie wymusi ograniczeń sieciowych dla tej aplikacji. Zalecane jest, abyś w pierwszej kolejności przeniósł aplikację do odpowiedniej grupy zaufania, a następnie włączył raportowanie o zdarzeniach. Jeśli ta metoda nie jest odpowiednia, możesz ręcznie skonfigurować ograniczenia dla aplikacji w ustawieniach reguły sieciowej. Ograniczenie jest stosowane tylko do lokalnego interfejsu aplikacji. Przenoszenie aplikacji między grupami zaufania w zasadzie działa poprawnie.

- Komponenty Zapora sieciowa i Ochrona przed włamaniami posiadają wspólne ustawienia: uprawnienia aplikacji i chronione zasoby. Jeśli zmienisz te ustawienia dla Zapory sieciowej, Kaspersky Endpoint Security automatycznie zastosuje nowe ustawienia do Ochrony przed włamaniami. Jeśli, na przykład, zezwoliłeś na zmiany w ustawieniach głównych zasady Zapory sieciowej (kłódka jest otwarta), ustawienia Ochrony przed włamaniami także staną się dostępne do edycji.

- Jeśli reguła dla pakietu sieciowego została wyzwolona w Kaspersky Endpoint Security 11.6.0 lub wcześniejszej wersji, kolumna **Nazwa aplikacji** w raporcie Zapory sieciowej będzie zawsze wyświetlała wartość *Kaspersky Endpoint Security*. Dodatkowo, Zapora sieciowa zablokuje połączenie na poziomie pakietów dla wszystkich aplikacji. To zachowanie zostało zmodyfikowane dla Kaspersky Endpoint Security 11.7.0 lub nowszej wersji. Kolumna **Typ reguły** została dodana do raportu Zapory sieciowej. Jeśli reguła dla pakietu sieciowego zostanie wyzwolona, wartość w kolumnie **Nazwa aplikacji** pozostanie pusta.

- Jeśli zablokujesz wszelką aktywność sieciową przy użyciu Zapory sieciowej, moduł Ochrona sieci może wykryć atak typu skanowanie portów. Może się tak zdarzyć, ponieważ aplikacja uruchamia Ochronę sieci przed Zaporą sieciową w celu wykrycia podejrzanej aktywności w sieci.

Ochrona przed atakami BadUSB

- Kaspersky Endpoint Security resetuje limit czasu blokady urządzenia USB, gdy komputer jest zablokowany (na przykład, minął limit czasu blokady ekranu). Oznacza to, że jeśli kilka razy wprowadzono zły kod autoryzacyjny dla urządzenia USB i aplikacja zablokuje urządzenie USB, Kaspersky Endpoint Security zezwoli na powtórzenie próby autoryzacji po odblokowaniu komputera. W tym przypadku Kaspersky Endpoint Security nie zablokuje urządzenia USB na czas określony w ustawieniach komponentu Ochrona przed atakami BadUSB.

- Kaspersky Endpoint Security resetuje limit czasu blokady urządzenia USB, gdy ochrona komputera jest wstrzymana. Oznacza to, że jeśli kilka razy wprowadzono zły kod autoryzacyjny dla urządzenia USB i aplikacja zablokuje urządzenie USB, Kaspersky Endpoint Security zezwoli na powtórzenie próby autoryzacji po wznowieniu ochrony komputera. W tym przypadku Kaspersky Endpoint Security nie zablokuje urządzenia USB na czas określony w ustawieniach komponentu Ochrona przed atakami BadUSB.

Kaspersky Security Network

- Kaspersky Endpoint Security nie obsługuje protokołu HTTPS podczas łączenia się z KSN Proxy (pole wyboru **Użyj HTTPS** zaznaczone w ustawieniach połączenia KSN Proxy), jeśli adres serwera zawiera litery inne niż łacińskie (symbole inne niż ASCII).

- W Kaspersky Security Center, podczas przełączania z korzystania z globalnej sieci Kaspersky Security Network na korzystanie z prywatnej sieci Kaspersky Security Network (KPSN) lub vice versa, opcja uczestniczenia w Kaspersky Security Network jest wyłączona w zasadzie określonego produktu. Po przełączeniu uważnie przeczytaj treść Oświadczenia Kaspersky Security Network i potwierdź chęć uczestnictwa w KSN. Możesz przeczytać treść Oświadczenia w interfejsie aplikacji lub podczas edytowania zasady produktu.

- Począwszy od wersji Kaspersky Endpoint Security 12.9 for Windows, przy przełączaniu się z KPSN na globalną sieć KSN konieczne jest ponowne potwierdzenie akceptacji Oświadczenia Kaspersky Security Network. W tym celu należy włączyć korzystanie z usługi Kaspersky Security Network we właściwościach zasady lub w interfejsie aplikacji, a także potwierdzić akceptację Oświadczenia Kaspersky Security Network. Jeśli wcześniej korzystano z globalnego protokołu KSN, musisz najpierw wyłączyć korzystanie z protokołu KSN, a następnie włączyć go ponownie i potwierdzić akceptację Oświadczenia Kaspersky Security Network. Jeśli nie zaakceptujesz Oświadczenia Kaspersky Security Network, aplikacja nie będzie mogła uzyskać dostępu do danych Kaspersky Security Network.

- Kaspersky Endpoint Security nie wysyła plików tekstowych (takich jak pliki TXT, CSV, LOG i DOCX bez makr) do Kaspersky Security Network w celu skanowania. Aplikacja wysyła pliki, które mogą stanowić zagrożenie dla komponentu KSN, w celu ich zeskanowania. Do takich plików należą pliki wykonywalne lub pliki, które mogą zawierać kod wykonywalny (np. makra w plikach DOCX). Pozostałe komponenty aplikacji odpowiadają za skanowanie plików tekstowych. Można również ręcznie sprawdzić reputację pliku tekstowego z menu kontekstowego pliku. Jeśli plik tekstowy ma reputację *Niezaufana (Kaspersky Security Network)*, aplikacja ignoruje działania zdefiniowane dla wykrytych zagrożeń.

Kontrola aplikacji

- Podczas pracy z regułami kontroli aplikacji nie zaleca się dodawania więcej niż 100 000 warunków włączenia i wykluczenia dla aplikacji w różnych kategoriach, pod warunkiem że program Kaspersky Endpoint Security jest uruchomiony na komputerze spełniającym minimalne wymagania sprzętowe i działa w systemie Microsoft Windows 10.

- Podczas pracy z regułami Kontroli aplikacji w Kaspersky Security Center Web Console obsługiwane są tylko archiwa w formacie ZIP. Archiwa w innych formatach, takich jak RAR lub 7z, nie są obsługiwane. Nie ma takiego ograniczenia, jeśli pracujesz z regułami Kontroli aplikacji w Konsoli administracyjnej (MMC).

- Podczas pracy z regułami Kontroli aplikacji w konsoli Kaspersky Security Center Web Console maksymalny obsługiwany rozmiar przesyłanego pliku wynosi 104 MB. Nie ma takiego ograniczenia, jeśli pracujesz z regułami Kontroli aplikacji w Konsoli administracyjnej (MMC).

- Podczas pracy w systemie Microsoft Windows 10 trybie listy zablokowanych aplikacji, blokowanie reguł może być niepoprawnie zastosowane, co może spowodować blokowanie aplikacji, które nie zostały określone w regułach.

- Jeśli podczas aktualizacji Kaspersky Endpoint Security dodano nowe *wstępnie zdefiniowane reguły kontroli aplikacji*, nie można ich zastosować do poprzednich wersji aplikacji.

- Jeśli progresywne aplikacje internetowe (PWA) są blokowane przez komponent Kontrola aplikacji, plik appManifest.xml został wskazany jako zablokowana aplikacja w raporcie.

- Podczas dodawania standardowej aplikacji Notatnik do reguły Kontroli aplikacji dla systemu Windows 11, nie jest zalecane określenie ścieżki do aplikacji. Na komputerach z systemem Windows 11 system operacyjny korzysta z Notatnika Metro, który znajduje się w folderze `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe`. W poprzednich wersjach systemu operacyjnego, Notatnik znajduje się w następujących folderach:

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  Podczas dodawania Notatnika do reguły Kontroli aplikacji, możesz określić nazwę aplikacji i sumę kontrolną pliku z właściwości uruchomionej aplikacji.

- Gdy migracja polityki KSWS do profilu zasad KES, kreator wsadowej konwersji zasad i zadań (kreator migracji) zmienia nazwy kategorii aplikacji, jeśli nazwy kategorii zawierają zabronione znaki: `'` `*` `<` `>` `?` `\` `:` `|`. Kreator migracji zastępuje te znaki znakiem `_`. Na przykład nazwa kategorii aplikacji `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` zostaje zmieniona na `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Kontrola urządzeń

- Kaspersky Endpoint Security może rejestrować zdarzenia podłączania i rozłączania urządzeń zewnętrznych. Usługi systemu Windows wykorzystują konto użytkownika systemowego do łączenia i rozłączania urządzeń. Utrudnia to stwierdzenie, który użytkownik podłącza lub rozłącza urządzenie. Kaspersky Endpoint Security określa w zdarzeniu konto użytkownika SYSTEMU.

- Dostęp do Drukarek dodanych do listy zaufanych urządzeń jest blokowany przez reguły blokowania magistral i urządzeń.

- Dla urządzeń MTP kontrola działań Odczyt, Zapis i Podłącz jest obsługiwana, jeśli korzystasz wbudowane sterowniki Microsoft systemu operacyjnego. Jeśli użytkownik instaluje niestandardowy sterownik do pracy z urządzeniem (na przykład, jako część iTunes lub Android Debug Bridge), kontrola działań Odczyt i Zapis może nie działać.

- Podczas pracy z urządzeniami MTP, reguły dostępu zostaną zmienione po ponownym podłączeniu urządzenia.

- Komponent Kontrola urządzeń rejestruje zdarzenia dotyczące monitorowanych urządzeń, takie jak podłączanie i odłączanie urządzenia, odczyt pliku z urządzenia, zapis pliku na urządzeniu oraz inne zdarzenia. Kaspersky Endpoint Security rejestruje zdarzenia rozłączenia tylko dla następujących typów urządzeń: Urządzenia przenośne (MTP), Dyski wymienne, Napędy dyskietek, Płyty CD/DVD. W przypadku pozostałych typów urządzeń aplikacja nie rejestruje zdarzeń rozłączenia. Aplikacja rejestruje operację podłączenia urządzenia do komputera dla wszystkich typów urządzeń.

- Jeśli dodajesz rządzenie do listy zaufanych w oparciu o maskę modelu i używane znaki, które znajdują się w identyfikatorze, a nie w nazwie modelu, te urządzenia nie zostaną dodane. Na stacji roboczej te urządzenia zostaną dodane do listy zaufanych w oparciu o maskę identyfikatora.

- W przypadku aktualizacji aplikacji bez ponownego uruchomienia komputera Kontrola urządzeń nie stosuje reguł dostępu do ponownie podłączanych urządzeń. Jeśli jednak urządzenie zostało podłączone przed aktualizacją, Kontrola urządzeń prawidłowo zastosuje reguły. Uruchom ponownie komputer, aby aplikacja działała poprawnie z ponownie podłączonymi urządzeniami.

- Na komputerach z zainstalowanym programem Kaspersky Endpoint Security w wersji 12.0, tryb dostępu do drukarki **Zezwól i nie zapisuj w dzienniku** dla typu urządzenia **Drukarki sieciowe** nazywa się **W zależności od magistrali połączenia**, jeżeli na komputerze zastosowana jest polityka Kaspersky Endpoint Security w wersji 12.1. W tych trybach aplikacja wykonuje te same czynności. W Kaspersky Endpoint Security w wersji 12.1 tryb dostępu dla drukarek sieciowych ma poprawną nazwę **Zezwól i nie zapisuj w dzienniku**.

- Począwszy od Kaspersky Endpoint Security for Windows w wersji 12.0, aplikacja umożliwia konfigurowanie reguł drukowania dla drukarek (kontrola drukowania). Po zainstalowaniu aplikacji z kontrolą drukowania lub uaktualnieniu aplikacji do wersji z kontrolą drukowania należy ponownie uruchomić komputer. Dopóki komputer nie zostanie ponownie uruchomiony, Kaspersky Endpoint Security nie stosuje reguł drukowania i może jedynie kontrolować dostęp do drukarek. Jeśli ponowne uruchomienie komputera niekorzystnie wpływa na przepływy pracy w Twojej organizacji, możesz ponownie uruchomić tylko usługę spoolsv (bufor wydruku). Kontrola drukowania nie jest obsługiwana na komputerach opartych na architekturze Arm.

- Począwszy od Kaspersky Endpoint Security 12.0 for Windows, aplikacja obsługuje protokół WPA3 urządzeń typu **Wi-Fi**. Jeśli na komputerze zastosowano zasadę Kaspersky Endpoint Security w wersji 12.2, na komputerach z Kaspersky Endpoint Security w wersji 11.11.0 i wcześniejszych zostanie wybrany protokół WPA2; WPA2 / WPA3 jest wybrany dla wersji od 12.0 do 12.1; WPA3 jest wybrany dla wersji 12.2 i nowszych.

- Urządzenia Apple są sklasyfikowane jako urządzenia przenośne (MTP) i urządzenia iTunes. System operacyjny noże nieprawidłowo rozpoznać podłączone urządzenie Apple i nie określić go jako urządzenie przenośne (MTP). Dlatego urządzenie Apple będzie niedostępne w menedżerze plików, ale dostępne w aplikacji iTunes. W rezultacie Kaspersky Endpoint Security będzie kontrolował dostęp urządzenia Apple tylko w aplikacji iTunes. Aby uzyskać dostęp do urządzenia Apple jako urządzenia przenośnego (MTP), należy przejść do Menedżera urządzeń i usunąć sterownik Apple Mobile Device USB Driver z listy kontrolerów USB. Po ponownym uruchomieniu komputera system rozpozna urządzenie Apple jako urządzenie przenośne (MTP) i iTunes. Kaspersky Endpoint Security będzie kontrolował dostęp urządzenia w aplikacji iTunes oraz w menedżerze plików.

- W Kaspersky Endpoint Security 12.3 for Windows ustawienia dostępu są inne niż urządzenia typu **Bluetooth**. Jeśli wpisałeś wartość **W zależności od magistrali połączenia** w poprzedniej wersji aplikacji, to po aktualizacji aplikacji do wersji 12.3 skonfigurowana wartość zmienia się na **Zezwól i nie zapisuj w dzienniku**. Nie zmienia to funkcjonowania urządzenia.

- Sterowanie urządzeniami obsługuje urządzenia Bluetooth tylko poprzez stos Bluetooth systemu Microsoft Windows. Sterowanie urządzeniami może działać nieprawidłowo w przypadku stosów Bluetooth innych firm.
- Jeśli urządzenie Bluetooth ukrywa się lub podszywa się pod inną klasę urządzenia (COD), Sterowanie urządzeniami może działać nieprawidłowo.
- Na komputerach z systemem Windows 7 lub Windows 8 i niektórymi sterownikami klucza sprzętowego Bluetooth firmy Realtek zezwolenie na podłączanie urządzeń Bluetooth wyłącznie jako urządzeń wejściowych (klasa HID) może nie być możliwe. Oznacza to, że jeśli zabronisz dostępu do urządzeń Bluetooth w ustawieniach aplikacji i dodasz urządzenia wejściowe do wyjątków, Sterowanie urządzeniami może zamiast tego uniemożliwić dostęp do wszystkich urządzeń Bluetooth.

Kontrola sieci

- Formaty OGV i WEBM nie są obsługiwane.
- Protokół RTMP nie jest obsługiwany.
- Kontrola sieci obsługuje tylko protokół WSL1. Aplikacja nie kontroluje ruchu przez protokół WSL2.

Adaptacyjna kontrola anomalii

- Zalecane jest automatyczne utworzenie wykluczeń w oparciu o zdarzenie. Jeśli ręcznie dodajesz wykluczenie, podczas obiektu docelowego, do początku ścieżki dodaj znak `*`.
- Raport reguły Adaptacyjnej kontroli anomalii nie może zostać wygenerowany, jeśli próbka zawiera chociaż jedno zdarzenie, którego nazwa zawiera ponad 260 znaków.
- Dodawanie wykluczeń z repozytorium Wywoływanie reguł Adaptacyjnej kontroli anomalii nie jest obsługiwane, jeśli właściwości obiektu lub procesu posiadają wartość zawierającą ponad 256 znaków (na przykład, ścieżka do obiektu docelowego). Możesz ręcznie dodać wykluczenie w ustawieniach zasady. Możesz także dodać wykluczenie w Raporcie dotyczącym wyzwolonych reguł Adaptacyjnej kontroli anomalii.
- Kaspersky Security Center 15.1 nie może wygenerować szczegółowego raportu **Raport o stanie reguł Adaptacyjnej kontroli anomalii** dla wybranej reguły.

Szyfrowanie dysku (FDE)

- Rozwiązanie Kaspersky Disk Encryption nie jest obsługiwane na komputerach opartych na architekturze ARM.
- Szyfrowanie dysków funkcją BitLocker nie jest obsługiwane na komputerach z systemem Windows Home.
- Po zainstalowaniu aplikacji, w celu zapewnienia poprawnego działania należy ponownie uruchomić system operacyjny dla szyfrowania dysku twardego.
- Agent autoryzacji nie obsługuje hieroglifów i znaków specjalnych `|` i `\`.
- W celu zapewnienia optymalnego działania komputera po szyfrowaniu, wymagane jest, aby procesor obsługiwał zestaw instrukcji AES-NI (Intel Advanced Encryption Standard New Instructions). Jeśli procesor nie obsługuje AES-NI, wydajność komputera może spadać.
- Jeśli istnieją procesy próbujące uzyskać dostęp do zaszyfrowanych urządzeń zanim aplikacja udzieliła dostępu do tych urządzeń, aplikacja wyświetli ostrzeżenie dotyczące zakończenia działania tych procesów. Jeśli procesy nie mogą zostać zakończone, ponownie podłącz zaszyfrowane urządzenia.
- Unikatowy numer ID dysków twardych jest wyświetlany w statystykach szyfrowania urządzeń, w formacie odwróconym.

- Podczas szyfrowania urządzeń nie jest zalecane ich formatowanie.

- Jeśli kilka nośników wymiennych jest podłączonych do komputera w tym samym czasie, zasada szyfrowania może zostać zastosowana tylko do jednego nośnika wymiennego. Jeśli nośniki wymienne zostaną podłączone ponownie, zasada szyfrowania została zastosowana poprawnie.

- Proces szyfrowania może nie rozpocząć się na mocno pofragmentowanym dysku twardym. Zdefragmentuj dysk twardy.

- Podczas szyfrowania dysków twardych, hibernacja jest blokowana od momentu rozpoczęcia zadania szyfrowania, aż do pierwszego ponownego uruchomienia komputera z systemem operacyjnym Microsoft Windows 7/8/8.1/10, a w przypadku zainstalowania szyfrowania dysku twardego, aż do pierwszego ponownego uruchomienia systemu operacyjnego Microsoft Windows 8/8.1/10. W przypadku deszyfrowania dysku twardego hibernacja jest blokowana od momentu całkowitego odszyfrowania sektorów startowych dysku twardego, aż do pierwszego ponownego uruchomienia systemu operacyjnego. Jeśli w systemie operacyjnym Microsoft Windows 8/8.1/10 włączona jest opcja Szybki start, zablokowanie hibernacji uniemożliwia zamknięcie systemu operacyjnego.

- Komputery z systemem Windows 7 nie pozwalają na zmianę hasła podczas wykrywania szyfrowania dysku przy użyciu technologii BitLocker. Po wprowadzeniu klucza odzyskiwania i załadowaniu systemu operacyjnego, program Kaspersky Endpoint Security nie wyświetli monitu o zmianę hasła lub kodu PIN. Dlatego też niemożliwe jest ustawienie nowego hasła lub kodu PIN. Ten problem jest spowodowany przez szczególne właściwości systemu operacyjnego. Aby kontynuować, należy ponownie zaszyfrować dysk twardy.

- Nie jest zalecane użycie narzędzia xbootmgr.exe z włączonymi dodatkowymi opcjami. Na przykład: Dispatcher, Network lub Drivers.

- Formatowanie zaszyfrowanego nośnika wymiennego nie jest obsługiwane na komputerze z zainstalowanym programem Kaspersky Endpoint Security for Windows.

- Formatowanie zaszyfrowanego nośnika wymiennego z systemem plików FAT32 nie jest obsługiwane (dysk jest wyświetlany jako zaszyfrowany). W celu sformatowania dysku, ponownie sformatuj go do system plików NTFS.

- Na jednym zaszyfrowanym komputerze nie może istnieć kilku agentów pobierania.

- Próba przywrócenia obrazu dysku startowego GPT w stanie niezaszyfrowanym może spowodować, że system operacyjny stanie się niezdatny do użytku. Aby tego uniknąć, postępuj zgodnie z poniższymi zaleceniami:

  - Przed przywróceniem obrazu z kopii zapasowej całkowicie odszyfruj dysk.

  - Podczas tworzenia obrazu stosuj kopiowanie sektor po sektorze.

  - Przed przywróceniem obrazu usuń dane z pierwszych sektorów zaszyfrowanego dysku i ponownie zainicjuj dysk.

- Nie można uzyskać dostępu do nośnika wymiennego, który wcześniej został zaszyfrowany na innym komputerze, jeśli jednocześnie spełnione są wszystkie z następujących warunków:

  - Brak połączenia z serwerem Kaspersky Security Center.

  - Użytkownik podejmuje próbę uwierzytelnienia przy użyciu nowego tokena lub hasła.

  Jeśli wystąpi podobna sytuacja, uruchom komputer ponownie. Po ponownym uruchomieniu komputera, dostęp do zaszyfrowanego nośnika wymiennego zostanie udzielony.

- Wykrycie urządzeń USB przez Agenta autoryzacji może nie być obsługiwane, jeśli w ustawieniach BIOS-u, dla USB włączony jest tryb xHCI.
- Kaspersky Disk Encryption (FDE) dla dysku SSD, który jest używany do buforowania najczęściej używanych danych, nie jest obsługiwane dla urządzeń SSHD.
- Szyfrowanie dysków twardych w 32-bitowych systemów operacyjnych Microsoft Windows 8/8.1/10, działających w trybie UEFI, nie jest obsługiwane.
- Uruchom komputer ponownie przed ponownym zaszyfrowaniem odszyfrowanego dysku twardego.
- Szyfrowanie dysku twardego nie jest kompatybilne z Kaspersky Anti-Virus dla UEFI. Nie jest zalecane używanie funkcji szyfrowania dysku twardego na komputerach, na których jest zainstalowany Kaspersky Anti-Virus dla UEFI.
- Tworzenie kont Agenta autoryzacji w oparciu o konta Microsoft jest obsługiwane z następującymi ograniczeniami:
  - Nie jest obsługiwana technologia logowania jednokrotnego.
  - Automatyczne tworzenie kont Agenta autoryzacji nie jest obsługiwane, jeśli została wybrana opcja tworzenia kont dla użytkowników, którzy logowali się do systemu w ciągu ostatnich N dni.
- Jeśli nazwa konta Agenta autoryzacji posiada format `<domain>/<Windows account name>`, po zmianie nazwy komputera, musisz także zmienić nazwy kont, które zostały utworzone dla lokalnych użytkowników tego komputera. Na przykład, wyobraź sobie, że na komputerze `Ivanov` istnieje lokalny użytkownik `Ivanov`, a dla tego użytkownika utworzono konto Agenta autoryzacji o nazwie `Ivanov/Ivanov`. Jeśli nazwa komputera `Ivanov` została zmieniona na `Ivanov-PC`, musisz zmienić nazwę konta Agenta autoryzacji dla użytkownika `Ivanov` z `Ivanov/Ivanov` na `Ivanov-PC/Ivanov`. Możesz zmienić nazwę konta przy użyciu zadania zarządzania kontem lokalnym Agenta autoryzacji. Przed zmianą nazwy konta, uwierzytelnianie w środowisku wykonawczym przed uruchomieniem systemu jest możliwe przy użyciu starej nazwy (na przykład: `Ivanov/Ivanov`).
- Jeśli użytkownik może uzyskać dostęp do komputera, który został zaszyfrowany z użyciem technologii Kaspersky Disk Encryption tylko przy użyciu tokena, a ten użytkownik musi zakończyć procedurę odzyskiwania dostępu, upewnij się, że po przywróceniu dostępu do zaszyfrowanego komputera temu użytkownikowi można udzielić dostępu z użyciem hasła do tego komputera. Hasło, które użytkownik ustawił podczas przywracania dostępu, może nie zostać zapisane. W tym przypadku użytkownik będzie musiał ponownie zakończyć procedurę przywracania dostępu do zaszyfrowanego komputera przy jego kolejnym ponownym uruchomieniu.
- Podczas odszyfrowywania dysku twardego przy użyciu narzędzia FDE Recovery Tool, proces deszyfracji może zakończyć się błędem, jeśli dane na urządzeniu źródłowym zostaną nadpisane odszyfrowanymi danymi. Część danych na dysku twardym pozostanie zaszyfrowana. Zalecane jest wybranie opcji zapisu odszyfrowanych danych do pliku w ustawieniach odszyfrowywania urządzenia podczas korzystania z FDE Recovery Tool.
- Jeśli hasło do Agenta autoryzacji zostało zmienione, zostanie wyświetlona wiadomość *Twoje hasło zostało pomyślnie zmienione.Kliknij OK*, a użytkownik uruchomi komputer ponownie, nowe hasło nie zostanie zapisane. Stare hasło musi być używane do kolejnego uwierzytelniania w środowisku wykonawczym przed uruchomieniem systemu.
- Szyfrowanie dysku jest niekompatybilne z technologią Intel Rapid Start.
- Szyfrowanie dysku jest niekompatybilne z technologią ExpressCache.

- W niektórych przypadkach, podczas próby odszyfrowania zaszyfrowanego dysku przy użyciu FDE Recovery Tool, po zakończeniu procedury „Żądanie-Odpowiedź" narzędzie błędnie wykrywa stan urządzenia jako „niezaszyfrowane". Raport narzędzia wyświetla zdarzenie informujące, że urządzenie zostało pomyślnie odszyfrowane. W tym przypadku należy ponownie uruchomić procedurę odzyskiwania danych, aby odszyfrować urządzenie.

- Po zaktualizowaniu wtyczki Kaspersky Endpoint Security for Windows w konsoli Web Console, właściwości komputera klienckiego nie wyświetlają klucza odzyskiwania BitLocker, aż usługa Web Console nie zostanie ponownie uruchomiona.

- Aby zobaczyć inne ograniczenia obsługi szyfrowania całego dysku oraz listę urządzeń, dla których szyfrowanie dysków twardych jest obsługiwane z ograniczeniami, zapoznaj się z Bazą wiedzy, dostępną na stronie pomocy technicznej.

Szyfrowanie plików (FLE)

- Szyfrowanie plików nie jest obsługiwane na komputerach opartych na architekturze ARM.

- Szyfrowanie plików i folderów nie jest obsługiwane w systemach operacyjnych Microsoft Windows Embedded.

- Po zainstalowaniu aplikacji, musisz ponownie uruchomić system operacyjny, aby szyfrowanie plików i folderów działało poprawnie.

- Aplikacja obsługuje szyfrowanie plików tylko na urządzeniach z systemami plików NTFS i FAT32. Jeśli zaszyfrowany plik zostanie przesłany na urządzenie z nieobsługiwanym systemem plików (na przykład exFAT), plik nie zostanie zaszyfrowany na tym urządzeniu i będzie go można modyfikować.

- Jeśli zaszyfrowany plik jest przechowywany na komputerze, który posiada dostępną funkcję szyfrowania, a użytkownik uzyskuje dostęp do pliku z komputera, na którym szyfrowanie nie jest dostępne, bezpośredni dostęp do tego pliku zostanie udzielony. Zaszyfrowany plik przechowywany w folderze sieciowym na komputerze, na którym jest dostępna funkcjonalność szyfrowania, zostanie skopiowany w postaci odszyfrowanej na komputer, na którym nie ma dostępnej funkcjonalności szyfrowania.

- Przed zaszyfrowaniem plików przy użyciu Kaspersky Endpoint Security for Windows zalecane jest odszyfrowanie plików, które zostały zaszyfrowane za pomocą Encrypting File System.

- Po zaszyfrowaniu pliku, jego rozmiar zwiększy się o 4 kB.

- Po zaszyfrowaniu pliku, w jego właściwościach zostanie ustawiony atrybut *Archiwum*.

- Podczas kopiowania odszyfrowanego pliku, na przykład na nośnik wymienny, plik może pozostać zaszyfrowany. Może się tak zdarzyć, ponieważ gdy menedżer plików (na przykład explorer.exe) próbuje uzyskać dostęp do zaszyfrowanego pliku, zapisuje skrót pliku na specjalnej liście procesów. Po odszyfrowaniu pliku, gdy menedżer plików próbuje uzyskać do niego dostęp, proces przeszukuje listę pod kątem skrótu pliku. Jeśli skrót zostanie znaleziony, Kaspersky Endpoint Security pozostawi plik w postaci zaszyfrowanej. Aby tego uniknąć, należy wyczyścić listę procesów. System operacyjny automatycznie czyści listę procesów w miarę jej zapełniania. Możesz również wyczyścić listę ręcznie. Aby to zrobić, możesz ponownie uruchomić komputer, ponownie uruchomić proces, którego używasz do uzyskania dostępu do pliku (na przykład explorer.exe), lub skorzystać z innego menedżera plików, który nie był używany do uzyskania dostępu do zaszyfrowanego pliku.

- Jeśli nierozpakowany plik z zaszyfrowanego archiwum posiada taką samą nazwę co już istniejący plik na komputerze, ten istniejący zostanie nadpisany przez nowy plik, który został wypakowany z zaszyfrowanego archiwum. Użytkownik nie zostaje poinformowany o działaniu nadpisania.

- Przed wyodrębnieniem zaszyfrowanego archiwum należy upewnić się, że jest wystarczająco dużo wolnego miejsca na dysku, aby pomieścić wyodrębnione pliki. Jeśli nie ma wystarczającej ilości miejsca na dysku, wyodrębnianie archiwum może zostać ukończone, ale pliki mogą być uszkodzone. W takim przypadku możliwe jest, że Kaspersky Endpoint Security nie wyświetli żadnych komunikatów o błędach.

- Interfejs Przenośnego Menedżera plików nie wyświetla wiadomości o błędach, które występują podczas jego działania.

- Kaspersky Endpoint Security for Windows nie uruchamia Przenośnego Menedżera plików na komputerze, na którym jest zainstalowany komponent Szyfrowanie plików.

- Nie możesz użyć Przenośnego menedżera plików do uzyskania dostępu do dysku wymiennego, jeśli następujące warunki są spełnione jednocześnie:

  - Brak połączenia z Kaspersky Security Center;

  - Kaspersky Endpoint Security for Windows jest zainstalowany na komputerze;

  - Szyfrowanie danych (FDE lub FLE) nie zostało wykonane na komputerze.

  Dostęp nie jest możliwy nawet wtedy, gdy znasz hasło do Przenośnego menedżera plików.

- Jeśli używana jest funkcja szyfrowania plików, aplikacja jest niekompatybilna z klientem pocztowym Sylpheed.

- Kaspersky Endpoint Security for Windows nie obsługuje reguł ograniczeń dostępu do zaszyfrowanych plików dla niektórych aplikacji. Wynika to z faktu, że niektóre operacje na plikach są wykonywane przez inne aplikacje. Na przykład, kopiowanie plików jest wykonywane przez menedżera plików, a nie przez samą aplikację. W ten sposób, jeżeli klientowi poczty Outlook odmówiono dostępu do zaszyfrowanych plików, Kaspersky Endpoint Security pozwoli klientowi poczty na dostęp do zaszyfrowanego pliku, jeżeli użytkownik skopiował pliki do wiadomości e-mail za pomocą schowka lub używając funkcji „przeciągnij i upuść". Czynność kopiowania została wykonana przez menedżera plików, dla którego nie zostały określone zasady ograniczania dostępu do zaszyfrowanych plików, tzn. dostęp jest dozwolony.

- Jeśli nośniki wymienne są zaszyfrowane z obsługą trybu przenośnego, kontrola ważności hasła nie może zostać wyłączona.

- Zmiana ustawień plików stronicowania nie jest obsługiwana. System operacyjny używa domyślnych wartości zamiast określonych wartości parametrów.

- Podczas pracy z zaszyfrowanymi nośnikami wymiennymi należy użyć bezpiecznego usuwania. Nie można zagwarantować integralności danych, jeśli nośnik wymienny nie został bezpiecznie usunięty.

- Po zaszyfrowaniu plików ich oryginalne niezaszyfrowane kopie są bezpiecznie usuwane.

- Synchronizacja plików offline przy użyciu usługi Client-Side Caching (CSC) nie jest obsługiwana. Szyfrowanie plików offline lub technologia Branch Caching przez SMB dla serwerów również nie jest obsługiwana. Zalecane jest zablokowanie zarządzania offline współdzielonymi zasobami na poziomie zasady grupy. Pliki, które są w trybie offline, mogą być edytowane. Po synchronizacji, zmiany wprowadzone w pliku offline mogą zostać utracone.

- Tworzenie zaszyfrowanego archiwum na głównym dysku twardym nie jest obsługiwane.

- Podczas uzyskiwania dostępu do zaszyfrowanych plików poprzez sieć mogą pojawić się problemy. Zalecane jest przeniesienie plików do innego źródła lub upewnienie się, że komputer używany jako serwer plików jest zarządzany przez ten sam Serwer administracyjny Kaspersky Security Center.

- Zmiana układu klawiatury powoduje brak odpowiedzi okna do wprowadzenia hasła do zaszyfrowanego samorozpakowującego się archiwum. Aby rozwiązać ten problem, zamknij okno do wprowadzenia hasła, przełącz układ klawiatury w swoim systemie operacyjnym, a następnie ponownie wprowadź hasło do zaszyfrowanego archiwum.

- Jeśli szyfrowanie plików jest używane na systemach, które posiadają kilka partycji na jednym dysku, zalecane jest użycie opcji, która automatycznie określa rozmiar pliku pagefile.sys. Po ponownym uruchomieniu komputera plik pagefile.sys może zostać przenoszony między partycjami dysku.

- Po zastosowaniu reguł szyfrowania plików, w tym plików w folderze *Moje dokumenty*, upewnij się, że użytkownicy, dla których szyfrowanie zostało zastosowane, mogą pomyślnie uzyskać dostęp do zaszyfrowanych plików. Aby to zrobić, każdy użytkownik loguje się do systemu, w którym dostępne jest połączenie z Kaspersky Security Center. Jeśli użytkownik spróbuje uzyskać dostęp do zaszyfrowanych plików bez połączenia z Kaspersky Security Center, system może się zawieszać.

- Jeśli pliki systemowe są w jakiś sposób uwzględnione w obszarze szyfrowania plików, w raportach mogą pojawić się zdarzenia dotyczące błędów, które wystąpiły podczas szyfrowania tych plików. Pliki określone w tych zdarzeniach nie są tak naprawdę szyfrowane.

- Procesy Pico nie są obsługiwane.

- Ścieżki uwzględniające wielkość liter nie są obsługiwane. Jeśli reguły szyfrowania lub reguły deszyfrowania zostaną zastosowane, ścieżki w zdarzeniach produktu są napisane małymi literami.

- Nie jest zalecane szyfrowanie plików, które są używane przez system podczas uruchamiania. Jeśli te pliki są zaszyfrowane, próba dostępu do zaszyfrowanych plików bez połączenia z Kaspersky Security Center może powodować zawieszanie się systemu lub doprowadzić do wyświetlenia monitów o dostęp do odszyfrowanych plików.

- Jeśli użytkownicy wspólnie pracują z plikiem poprzez sieć zgodnie z regułami FLE za pośrednictwem aplikacji, które wykorzystują metodę mapowania wczytywania pliku do pamięci (np. WordPad lub FAR) oraz aplikacje zaprojektowane do pracy z dużymi plikami (np. Notepad ++), plik w postaci zaszyfrowanej może zostać zablokowany niezależnie bez możliwości uzyskania dostępu do niego z poziomu komputera, na którym się znajduje.

- Kaspersky Endpoint Security nie szyfruje plików, które znajdują się z magazynie w chmurze OneDrive lub w innych folderach, które w nazwie posiadają OneDrive. Kaspersky Endpoint Security blokuje także kopiowanie zaszyfrowanych plików do folderów OneDrive, jeśli te pliki nie są dodawane do reguły odszyfrowywania.

- Jeśli zainstalowano komponent szyfrowania plików, zarządzanie użytkownikami i grupami nie działa w trybie WSL (Windows Subsystem for Linux).

- Po zainstalowaniu komponentu szyfrowania plików, tryb POSIX (Portable Operating System Interface) do zmiany nazwy i usuwania plików nie jest obsługiwany.

- Nie zaleca się szyfrowania plików tymczasowych, ponieważ może to spowodować utratę danych. Na przykład Microsoft Word tworzy pliki tymczasowe podczas przetwarzania dokumentu. Jeśli pliki tymczasowe zostaną zaszyfrowane, ale oryginalny plik nie, podczas próby zapisania dokumentu może wystąpić błąd *Odmowa dostępu*. Dodatkowo Microsoft Word może zapisać plik, ale nie będzie można otworzyć dokumentu następnym razem, czyli dane zostaną utracone. Aby zapobiec utracie danych, należy wykluczyć folder plików tymczasowych z reguł szyfrowania.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- Nie możesz przeskanować obiektu poddanego kwarantannie w wyniku działania zadania *Przenieś plik do Kwarantanny*.

- Nie można poddać kwarantannie Alternate Data Stream (ADS), który jest większy niż 4 MB. Kaspersky Endpoint Security pomija tak duże ADS bez powiadamiania użytkownika.

- Kaspersky Endpoint Security nie uruchamia zadań *Skanowanie IOC* na dyskach sieciowych, jeśli ścieżka do folderu we właściwościach zadania rozpoczyna się od litery dysku. Kaspersky Endpoint Security obsługuje tylko format ścieżki UNC dla zadań *Skanowanie IOC* na dyskach sieciowych. Na przykład, `\\server\shared_folder`.

- Aby zadanie *Skanowanie IOC* wykorzystujące elementy EmailItem działało prawidłowo, należy zaktualizować wtyczkę internetową Kaspersky Endpoint Security do najnowszej wersji.

- Na komputerach opartych na architekturze Arm zadanie *Skanowanie IOC* obsługuje pliki e-mail tylko z następujących klientów poczty: 32-bitowe i 64-bitowe wersje programu Outlook 2016 oraz Outlook 2021, 2024 i 365 dla architektury Arm64.

- Importowanie pliku konfiguracyjnego aplikacji zakończy się błędem, jeśli ustawienie integracji z Kaspersky Sandbox zostanie włączone w pliku konfiguracyjnym. Przed wyeksportowaniem ustawień aplikacji wyłącz Kaspersky Sandbox. Następnie wykonaj procedurę eksportu/importu. Po zaimportowaniu pliku konfiguracyjnego włącz Kaspersky Sandbox.

- Podczas importowania zasady z pliku KLP wartość parametru określająca akceptację warunków umowy Kaspersky Detection and Response Expert Agreement nie jest stosowana. W rezultacie po zaimportowaniu zasady Kaspersky Endpoint Security nie wykonuje funkcji EDR Agent. Aby EDR Agent działał, otwórz zasadę, zmień dowolny parametr i zapisz ustawienia zasady.

- Jeśli wskaźnik naruszeń bezpieczeństwa został wykryty podczas wykonywania zadania *Skanowanie IOC*, aplikacja podda kwarantannie plik tylko dla warunku FileItem. Poddawanie pliku kwarantannie dla innych warunków nie jest obsługiwane.

- Do zarządzania szczegółami alertów wymagana jest wtyczka internetowa Kaspersky Endpoint Security for Windows w wersji 11.7.0 lub nowszej. Szczegóły alertów są niezbędne podczas pracy z rozwiązaniami Endpoint Detection and Response (EDR Optimum i EDR Expert). Szczegóły dotyczące detekcji są dostępne jedynie w Kaspersky Security Center Web Console i Kaspersky Security Center Cloud Console.

- Migrowanie konfiguracji [KES+KEA] do konfiguracji [KES+wbudowany agent] może zakończyć się błędem usunięcia aplikacji Kaspersky Endpoint Agent. Błąd usunięcia aplikacji został naprawiony w najnowszej wersji Kaspersky Endpoint Agent. Aby usunąć Kaspersky Endpoint Agent, uruchom komputer ponownie i utwórz zadanie dezinstalacji aplikacji.

- Konfiguracja [KES + KEA + wbudowany agent] nie jest obsługiwana. Taka konfiguracja zakłóca interakcję między aplikacjami a rozwiązaniem Detection and Response wdrożonym w Twojej organizacji. Ponadto używanie Kaspersky Endpoint Agent i wbudowanego agenta na tym samym komputerze może prowadzić do zduplikowania danych telemetrycznych i zwiększonego obciążenia komputera oraz sieci. Po migracji do konfiguracji [KES + wbudowany agent] upewnij się, że usunięto Kaspersky Endpoint Agent z komputera. Jeśli Kaspersky Endpoint Agent nadal działa po migracji, odinstaluj aplikację ręcznie (na przykład przy użyciu zadania *Zdalna dezinstalacja aplikacji*).

  Instalator umożliwia zainstalowanie Kaspersky Endpoint Agent na komputerze z zainstalowanym Kaspersky Endpoint Security i wbudowanym agentem. Kaspersky Endpoint Agent i wbudowany agent mogą również zostać zainstalowane na jednym komputerze w wyniku użycia zadania *Zmiana składników aplikacji*. Zachowanie zależy od wersji Kaspersky Endpoint Security i Kaspersky Endpoint Agent.

- Podczas generowania szczegółów alertu aplikacja dostarcza informacje o wykrytym zagrożeniu, w tym skróty zmodyfikowanych plików. Kaspersky Endpoint Security oblicza skrót pliku podczas generowania szczegółów alertu. Należy pamiętać, że oryginalny skrót pliku w momencie wygenerowania zdarzenia modyfikacji pliku może nie być taki sam, jak skrót obliczony w momencie wygenerowania szczegółów alertu.

- Wbudowany agent, EDR (KATA), wznawia izolację komputera od sieci po ponownym uruchomieniu komputera, nawet jeśli okres izolacji wygasł. Aby zapobiec powtarzającej się izolacji komputera, należy wyłączyć izolację od sieci w konsoli Kaspersky Anti Targeted Attack Platform.

- Zalecamy aktualizację aplikacji po zakończeniu izolacji od sieci. Po zaktualizowaniu Kaspersky Endpoint Security izolacja od sieci może zostać wstrzymana.

- Wbudowane agenty dla EDR (KATA), EDR Optimum i EDR Expert nie są ze sobą zgodne. Aktywacja wbudowanego agenta EDR z autonomiczną licencją na dodatek Kaspersky Endpoint Detection and Response może więc zostać pominięta, jeśli aktywowano Kaspersky Endpoint Security z inną funkcjonalnością EDR. Na przykład, aktywacja wbudowanego agenta EDR (KATA) z autonomiczną licencją jest pomijana, jeśli aktywowano Kaspersky Endpoint Security z licencją [KES+EDR Optimum].

- W Kaspersky Endpoint Security w wersji 12.1, wbudowany agent EDR (KATA) nie obsługuje następujących metaplików dla zadania *Pobierz metapliki NTFS*: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. Obsługa tych metaplików została dodana do Kaspersky Endpoint Security w wersji 12.2.

- Podczas migracji z programu Kaspersky Endpoint Agent do Kaspersky Endpoint Security dla rozwiązania Kaspersky Anti Targeted Attack Platform (EDR) mogą wystąpić błędy z połączeniem komputera do serwerów Central Node. Dzieje się tak, ponieważ kreator migracji w usłudze Web Console pomija następujące ustawienia reguł i nie migruje ich:

  - Zakaz modyfikacji ustawień **Ustawienia połączenia** („blokada").

    Domyślnie ustawienia można modyfikować („blokada" jest otwarta). Dlatego ustawienia nie są stosowane na komputerze. Należy zakazać modyfikacji ustawień i zamknąć „blokadę".

  - Kontener szyfrowania.

    Jeśli do łączenia się z serwerami Central Node używasz uwierzytelniania dwuskładnikowego, należy dodać kontener szyfrowania. Kreator migracji poprawnie migruje certyfikat TLS serwera.

  Kreator migracji reguł i zadań w Konsoli administracyjnej (MMC) migruje wszystkie ustawienia rozwiązania Kaspersky Anti Targeted Attack Platform (EDR).

- Stan aktywacji aplikacji jest nieprawidłowo wyświetlany, gdy aplikacja jest zainstalowana w trybie Endpoint Detection and Response Agent w celu obsługi rozwiązania Kaspersky Managed Detection and Response bez połączenia z Kaspersky Security Center. Po pobraniu pliku BLOB w obszarze powiadomień paska zadań systemu Windows wyświetlany jest nieprawidłowy stan: *Aplikacja nie została aktywowana*. Interfejs aplikacji poprawnie wyświetla jednak stan aktywacji. Aby aplikacja działała poprawnie, uruchom ponownie komputer.

- Kaspersky Endpoint Security umożliwia integrację z rozwiązaniem Kaspersky Anti Targeted Attack Platform przy użyciu komponentu EDR (KATA) lub Endpoint Sensor (nieobsługiwany). Należy pamiętać, że do interakcji z platformą Kaspersky Anti Targeted Attack Platform możesz używać tylko jednego z komponentów. Aby wyświetlić stan komponentu, otwórz właściwości komputera w Konsoli administracyjnej (MMC), w sekcji **Aplikacje** otwórz właściwości Kaspersky Endpoint Security for Windows i przejdź do sekcji **Komponenty**. Poniższe uwagi specjalne dotyczą wyświetlania stanu komponentu podczas interakcji z platformą Kaspersky Anti Targeted Attack Platform:

  - W przypadku wtyczki zarządzającej w wersji 12.0 i wcześniejszych aplikacja wyświetla aktualny stan komponentu **Endpoint Sensor**. W Kaspersky Endpoint Security 12.0 i wcześniejszych wersjach komponent EDR (KATA) nie jest dostępny. Komponent EDR (KATA) został wprowadzony w wersji 12.1.

  - W przypadku wtyczki zarządzającej w wersji 12.1 i nowszych aplikacja wyświetla ogólny stan komponentu **Endpoint Detection and Response (KATA)**, co może oznaczać stan komponentu Endpoint Sensor lub stan komponentu EDR (KATA). Zależy to od wersji aplikacji zainstalowanej na komputerze użytkownika i dostępnych komponentów, których można użyć do interakcji z Kaspersky Anti Targeted Attack Platform.

- Począwszy od Kaspersky Endpoint Security 12.6 i nowszych wersji, konsola Kaspersky Security Center Web Console w wersji 14.2 i wcześniejszych nie wyświetla poprawnie nazwy komponentu **Endpoint Detection and Response (KATA)** we właściwościach komputera. Zamiast komponentu **Endpoint Detection and Response (KATA)** aplikacja wyświetli nazwę komponentu **Endpoint Detection and Response Expert (KATA EDR)**. Aby wyświetlić listę komponentów, otwórz właściwości komputera w Web Console, w sekcji **Aplikacje** otwórz właściwości Kaspersky Endpoint Security for Windows i przejdź do sekcji **Komponenty**. Począwszy od konsoli Kaspersky Security Center Web Console w wersji 15.1 i w przypadku jej nowszych wersji, aplikacja poprawnie wyświetla nazwę komponentu.

- Podczas aktualizacji wtyczki zarządzającej Kaspersky Endpoint Detection and Response do wersji 15.3 zainstalowanej w Web Console w wersjach 14.0–14.2 szczegóły alertów są wyświetlane nieprawidłowo. Aby szczegóły alertów działały prawidłowo, należy ponownie uruchomić Serwer administracyjny Kaspersky Security Center.

- Wtyczka zarządzająca Kaspersky Endpoint Detection and Response w wersji 15.4 i nowszych nie obsługuje Kaspersky Security Center w wersji 14.0. Po zaktualizowaniu wtyczki zarządzającej szczegóły alertów są wyświetlane nieprawidłowo.

- Rozwiązania Kaspersky Extended Detection and Response (XDR) w wersji 1.4 nie obsługują wtyczki internetowej Kaspersky Endpoint Security for Windows w wersji 12.12 lub nowszej. Możesz pozostać przy obecnej wersji wtyczki internetowej lub zaktualizować rozwiązanie XDR do wersji 2.0 lub nowszej.

- Kaspersky Endpoint Security nie wysyła obiektów przeznaczonych dla architektury Arm do Kaspersky Sandbox.

- Integracja z Kaspersky Endpoint Detection and Response Expert nie jest obsługiwana na komputerach opartych na architekturze Arm.

- Kaspersky Endpoint Security obsługuje łącznie do 10 000 reguł przeznaczonych do filtrowania (uwzględniania i wykluczania) zdarzeń EDR Expert (on-premises).

- Reguły filtrowania zdarzeń EDR Expert (on-premises) nie zostaną przekazane z zasad do zarządzanych urządzeń z uruchomionym programem Kaspersky Endpoint Security w wersji 14.0 lub starszej, jeśli przekroczony zostanie obsługiwany limit przechowywanych reguł filtrowania. Aplikacja wyświetli odpowiednie ostrzeżenie.

Inne ograniczenia

- Systemy operacyjne Windows, począwszy od wersji 11 24H2, obsługują technologię UDP Receive Segment Coalescing Offload (URO). Technologia ta jest włączona domyślnie, jeśli na komputerze zainstalowano zgodną kartę sieciową i sterowniki. Wyłączenie technologii URO na komputerze użytkownika może znacząco obniżyć wydajność aplikacji.

- Kaspersky Endpoint Security obsługuje podsystem WSL (Windows Subsystem for Linux) z ograniczeniami:

  - WSL 1 Aplikacja monitoruje ruch sieciowy i wykrywa zagrożenia za pośrednictwem protokołu HTTP/HTTPS. Ponieważ Kaspersky Endpoint Security wykorzystuje własny certyfikat do skanowania bezpiecznych połączeń HTTPS, działanie niektórych aplikacji innych firm może zostać zakłócone.

  - WSL 2 Aplikacja nie obsługuje podsystemu WSL 2.

- Jeśli podczas działania aplikacja zwróci błędy lub zawiesi się, może zostać automatycznie uruchomiona ponownie. Jeśli aplikacja napotka powtarzające się błędy powodujące jej awarię, wykona ona następujące działania:

  1. Wyłączy funkcje kontroli i ochrony (funkcja szyfrowania pozostanie włączona).

  2. Powiadomi użytkownika o wyłączeniu funkcji.

  3. Podejmie próbę przywrócenia aplikacji do stanu funkcjonalności po zaktualizowaniu baz danych lub zastosowaniu uaktualnień modułów aplikacji.

- Adresy internetowe, które są dodawane do listy zaufanych, mogą zostać niepoprawnie przetworzone.

- W konsoli Kaspersky Security Center nie można zapisać pliku na dysku z folderu **Zaawansowane** → **Repozytoria** → **Aktywne zagrożenia**. Aby zapisać plik, należy wyleczyć zainfekowany plik. Podczas leczenia aplikacja zapisuje kopię pliku w kopii zapasowej. Teraz można zapisać plik na dysku z folderu **Zaawansowane** → **Repozytoria** → **Kopia zapasowa**.

- Dziedziczenie ustawień przesyłania danych do Serwera administracyjnego (**Ustawienia ogólne** → **Raporty i Kopia zapasowa** → **Przesyłanie danych do Serwera administracyjnego**) różni się od dziedziczenia innych ustawień. Jeżeli w zasadach zezwolono na zmianę ustawień przesyłania danych („kłódka" jest otwarta), ustawienia te zostaną przywrócone do wartości domyślnych we właściwościach komputera lokalnego w konsoli, jeśli nie były wcześniej zdefiniowane. Jeżeli te ustawienia były wcześniej zdefiniowane, to ich wartości zostaną przywrócone. Podczas usuwania zasad ustawienia są dziedziczone w ten sam sposób. W takich przypadkach inne ustawienia we właściwościach komputera lokalnego są dziedziczone z zasad.

- Kaspersky Endpoint Security monitoruje ruch sieciowy http, który jest zgodny ze standardami RFC 2616, RFC 7540, RFC 7541, RFC 7301. Jeśli Kaspersky Endpoint Security wykryje inny format wymiany danych w ruchu HTTP, aplikacja blokuje to połączenie, aby zapobiec pobieraniu szkodliwych plików z internetu.

- Kaspersky Endpoint Security uniemożliwia komunikację poprzez protokół QUIC. Przeglądarki używają standardowego protokołu transportu (TLS lub SSL) niezależnie od tego, czy obsługa QUIC jest włączona w przeglądarce.

- Błędy połączenia TLS mogą wystąpić, gdy oprogramowanie innych firm współpracuje z biblioteką Libcurl. Może to być związane z certyfikatem Kaspersky, którego Kaspersky Endpoint Security używa do skanowania połączeń szyfrowanych. Aby kontynuować pracę, możesz wyłączyć weryfikację certyfikatów dla oprogramowania innych firm (niezalecane) lub dodać treść certyfikatu Kaspersky do magazynu certyfikatów cURL. Aby uzyskać szczegółowe informacje, zapoznaj się z Bazą wiedzy Kaspersky.

- Jeśli Kaspersky Endpoint Security for Windows jest uruchamiany po raz pierwszy, aplikacja z podpisem cyfrowym może być tymczasowo umieszczona w złej grupie. Aplikacja z podpisem cyfrowym zostanie później umieszczona we właściwej grupie.

- Podczas ponownego skanowania szkodliwego obiektu, który został zablokowany przez oprogramowanie innej firmy, użytkownik nie zostanie poinformowany po ponownym wykryciu zagrożenia. Zdarzenie dotyczące ponownego wykrycia zagrożenia zostanie wyświetlone w raporcie aplikacji i w raporcie Kaspersky Security Center.

- Raport z szyfrowania urządzenia w Kaspersky Security Center nie będzie zawierał informacji o urządzeniach, które zostały zaszyfrowane przy użyciu technologii Microsoft BitLocker na platformach serwerowych lub na stacjach roboczych, na których nie zainstalowano komponentu Kontrola urządzeń.

- Nie można włączyć wyświetlania wszystkich wpisów w raporcie w konsoli Kaspersky Security Center Web Console. W konsoli Web Console możesz zmienić tylko liczbę wpisów wyświetlanych w raportach. Domyślnie, Kaspersky Security Center Web Console wyświetla 1000 wpisów w raporcie. Możesz włączyć wyświetlanie wszystkich wpisów w raporcie w Konsoli administracyjnej (MMC).

- Nie można ustawić wyświetlania więcej niż 1000 wpisów w raporcie w konsoli Kaspersky Security Center Console. Jeśli ustawisz wartość wyższą niż 1000, konsola Kaspersky Security Center Console wyświetli tylko 1000 wpisów w raporcie.

- Podczas korzystania z hierarchii zasad ustawienia sekcji Szyfrowanie nośników wymiennych w zasadzie potomnej są dostępne do edycji, jeśli zasada nadrzędna zapobiega modyfikacji tych ustawień.

- Musisz włączyć Przeprowadź inspekcję logowania w ustawieniach systemu operacyjnego, aby zapewnić poprawne funkcjonowanie wykluczeń dla ochrony folderów współdzielonych przed zewnętrznym szyfrowaniem.

- Jeśli ochrona folderu współdzielonego jest wyłączona, Kaspersky Endpoint Security for Windows monitoruje próby szyfrowania folderów współdzielonych dla każdej sesji zdalnego dostępu, które zostało uruchomione przed uruchomieniem Kaspersky Endpoint Security for Windows, w tym, jeśli komputer, z którego sesja zdalnego dostępu została uruchomiona, została dodana do wykluczeń. Jeśli nie chcesz, żeby Kaspersky Endpoint Security for Windows monitorował próby szyfrowania folderów współdzielonych dla sesji zdalnego dostępu, które były uruchomione na komputerze dodanym do wykluczeń i które były uruchomione przed uruchomieniem Kaspersky Endpoint Security for Windows, zakończ i ponownie rozpocznij sesję zdalnego dostępu lub ponownie uruchom komputer, na którym zainstalowano Kaspersky Endpoint Security for Windows.

- Jeśli zadanie aktualizacji jest uruchamiane z uprawnieniami określonego konta użytkownika, łaty produktu nie zostaną pobrane podczas aktualizacji ze źródła wymagającego autoryzacji.

- Aplikacja może nie zostać uruchomiona w wyniku słabej wydajności systemu. Aby rozwiązać ten problem, użyj opcji Ready Boot lub zwiększ limit czasu dla uruchamiania usług w systemie operacyjnym.

- Aplikacja nie może działać w systemie Windows Safe Mode.

- Nie można zagwarantować, że Kontrola audio będzie działała, aż do pierwszego ponownego uruchomienia po zainstalowaniu aplikacji.

- W Konsoli administracyjnej, w ustawieniach Ochrony przed włamaniami, w oknie konfigurowania uprawnień aplikacji przycisk **Usuń** jest niedostępny. Możesz usunąć aplikację z grupy zaufania z poziomu menu kontekstowego aplikacji.

- W lokalnym interfejsie aplikacji, w ustawieniach Ochrony przed włamaniami uprawnienia aplikacji i chronione zasoby nie są dostępne do przejrzenia, jeśli komputer jest zarządzany przez zasadę. Przewijanie, wyszukiwanie, filtrowanie i inne kontrolki okna są niedostępne. Uprawnienia aplikacji możesz przejrzeć we właściwościach zasady, w konsoli Kaspersky Security Center Console.

- Gdy włączone jest tworzenie plików śledzenia z rotacją, pliki śledzenia nie są tworzone dla komponentu AMSI i wtyczki programu Outlook.
- Pliki śledzenia wydajności nie mogą zostać ręcznie zebrane w Windows Server 2008.
- Pliki śledzenia wydajności dla typu śledzenia „Ponowne uruchomienie" nie są obsługiwane.
- Zapisywanie zrzutu pamięci nie jest obsługiwane dla procesów pico.
- Wyłączenie opcji **Wyłącz możliwość zewnętrznego zarządzania usługami systemowymi** nie zezwoli na zatrzymanie usługi aplikacji, która została zainstalowana z parametrem `AMPPL=1` (domyślnie, wartość parametru jest ustawiona na `1`, począwszy od systemu operacyjnego w wersji Windows 10RS2). Parametr `AMPPL` z wartością `1` włącza korzystanie z technologii procesów ochrony dla usługi produktu.
- Aby uruchomić skanowanie obiektów dla folderu, użytkownik, który uruchomił skanowanie obiektów, musi posiadać uprawnienia do odczytu atrybutów tego folderu. W przeciwnym razie skanowanie obiektów dla folderu będzie niemożliwe i zakończy się błędem.
- Jeśli reguła skanowania zdefiniowana w zasadzie zawiera ścieżkę bez znaku `\` na końcu, na przykład, `C:\folder1\folder2`, skanowanie zostanie uruchomione dla ścieżki `C:\folder1\`.
- Jeśli korzystasz z zasad ograniczeń oprogramowania (Software Restriction Policies, SRP), komputer może się nie załadować (czarny ekran). Aby zapobiec nieprawidłowościom, musisz zezwolić na używanie bibliotek aplikacji we właściwościach SRP. We właściwościach SRP dodaj regułę o poziomie bezpieczeństwa **Nieograniczone** dla pliku khkum.dll (pozycja menu **Nowa reguła sumy kontrolnej**). Plik znajduje się w folderze `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.1\klhk\klhk_x64\`. W przypadku wybrania tej metody musisz dodatkowo usunąć zaznaczenie pola wyboru **Pobierz aktualizacje składników aplikacji** ustawieniach zadania *Aktualizacja* dla Kaspersky Endpoint Security. Więcej informacji na temat korzystania z SRP znajdziesz w dokumentacji firmy Microsoft.

  Możesz również wyłączyć SRP i użyć komponentu Kontrola aplikacji Kaspersky Endpoint Security do kontrolowania użycia aplikacji.
- Jeśli komputer należy do domeny znajdującej się w obiekcie zasad grupy systemu Windows (Group Policy Object, GPO) z parametrem DriverLoadPolicy ustawionym na 8 (Good only), ponowne uruchomienie komputera z zainstalowanym programem Kaspersky Endpoint Security powoduje BSOD. Aby zapobiec usterkom, parametr Early Launch Antimalware (ELAM) w zasadach grupy musi być ustawiony na 1 (Good and unknown). Ustawienia ELAM są dostępne w zasadach: **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.
- Zarządzanie ustawieniami wtyczki dla programu Outlook za pośrednictwem API Rest nie jest obsługiwane.
- Ustawienia uruchamiania zadania dla określonego użytkownika nie mogą zostać przesłane między urządzeniami za pośrednictwem pliku konfiguracyjnego. Po zastosowaniu ustawień z pliku konfiguracyjnego, ręcznie określ nazwę użytkownika i hasło.
- Po zainstalowaniu aktualizacji, zadanie sprawdzania integralności nie będzie działało, aż system nie zostanie uruchomiony ponownie w celu zastosowania aktualizacji.
- Jeśli poziom śledzenia plików z rotacją zostanie zmieniony za pośrednictwem narzędzia do zdalnej diagnostyki, Kaspersky Endpoint Security for Windows niepoprawnie wyświetli pustą wartość dla poziomu śledzenia. Jednakże pliki śledzenia zostaną zapisane zgodnie z poprawnym poziomem śledzenia. Jeśli poziom śledzenia plików z rotacją zostanie zmieniony za pośrednictwem interfejsu lokalnego aplikacji, poziom śledzenia zostanie poprawnie zmodyfikowany, ale narzędzie do zdalnej diagnostyki będzie niepoprawnie wyświetlało poziom śledzenia, które zostało ostatnio zdefiniowane przez narzędzie. To może sprawić, że administrator nie będzie musiał aktualizować informacji o bieżącym poziomie śledzenia, a odpowiednie informacje mogą nie znajdować się w plikach śledzenia, jeśli użytkownik ręcznie zmieni poziom śledzenia w lokalnym interfejsie aplikacji.

- W interfejsie lokalnym ustawienia ochrony hasłem nie zezwalają na zmianę nazwy konta administratora (domyślnie KLAdmin). Aby zmienić nazwę konta administratora musisz wyłączyć Ochronę hasłem, a następnie włączyć Ochronę hasłem i określić nową nazwę konta administratora.

- Aplikacja Kaspersky Endpoint Security, gdy jest zainstalowana na serwerze Windows Server 2019, jest niekompatybilna z Docker. Zdalne instalowanie kontenerów Docker na komputerze z Kaspersky Endpoint Security powoduje awarię (BSOD).

- Jeżeli Kaspersky Endpoint Security jest zainstalowany na serwerze SQL Server DBMS, aplikacja wysyła żądania do instancji serwera. Jest to konieczne do skanowania zadań agenta SQL Server i zapobiegania uruchamianiu złośliwych zadań. Kaspersky Endpoint Security używa konta użytkownika SQL Server do skanowania zadań. Aplikacja wysyła zapytania do serwera podczas skanowania pamięci systemowej oraz po aktualizacji baz danych antywirusowych.

- Kompatybilność oprogramowania Kaspersky Endpoint Security i Secret Net Studio jest ograniczona:

  - Aplikacja Kaspersky Endpoint Security nie jest kompatybilna z komponentem Antivirus programu Secret Net Studio.

    Aplikacja nie może zostać zainstalowana na komputerze, na którym jest wdrożony program Secret Net Studio z komponentem Antivirus. Aby umożliwić interoperacyjność, musisz usunąć komponent Antivirus z Secret Net Studio.

  - Aplikacja Kaspersky Endpoint Security nie jest kompatybilna z komponentem ochrony dysku i szyfrowania danych programu Secret Net Studio.

    Aplikacji nie można zainstalować na komputerze, na którym wdrożono program Secret Net Studio z komponentem ochrony dysku i szyfrowania danych. Aby umożliwić współdziałanie, musisz usunąć komponent ochrony dysku i szyfrowania danych z programu Secret Net Studio.

  - Secret Net Studio nie jest kompatybilny z komponentem Szyfrowanie plików (FLE) programu Kaspersky Endpoint Security.

    Jeśli instalujesz Kaspersky Endpoint Security z komponentem Szyfrowanie plików (FLE), Secret Net Studio może działać z błędami. Aby zapewnić interoperacyjność, musisz usunąć komponent Szyfrowanie plików (FLE) z Kaspersky Endpoint Security.

- Podczas importowania reguł monitora integralności systemu aplikacja sprawdza identyfikator i nazwę reguły. Jeśli identyfikatory reguł są takie same, Kaspersky Endpoint Security zastępuje istniejące reguły nową regułą. Podczas eksportu reguł aplikacja przydziela identyfikatory automatycznie. Reguła o identycznych identyfikatorach może istnieć, na przykład, jeśli ręcznie edytowano wyeksportowane pliki XML reguł. Jeśli identyfikatory reguł są unikalne, ale nazwy reguł są takie same, Kaspersky Endpoint Security dodaje do nazwy reguły `(1)` i tak dalej.

- Począwszy od wersji 12.11 Kaspersky Endpoint Security for Windows, nie można przeglądać ustawień polityki nadrzędnej, która została otwarta w grupie podrzędnej w Web Console. Web Console wyświetla również ostrzeżenie: *Ta zasada jest dziedziczona. Możesz edytować ustawienia zasady tylko w grupie administracyjnej, w której została utworzona*.

- Powiadomienia wyskakujące o długości przekraczającej 256 znaków nie są wyświetlane w Konsoli administracyjnej (MMC).

- Nazwy komponentów w zasadzie i pakiecie instalacyjnym mogą być różne. Na przykład Endpoint Detection and Response Expert (on-premises) może nazywać się Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises) lub Kaspersky Anti Targeted Attack Platform Integration. Nazwy komponentów mogą się również różnić w zależności od wersji aplikacji.

Słownik

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 komponent jest wspólny dla wszystkich aplikacji firmy Kaspersky działających pod systemem Windows. Dla aplikacji działających pod innymi systemami operacyjnymi przeznaczone są dedykowane wersje Agenta sieciowego.

Aktywny klucz

Klucz, który jest aktualnie używany przez aplikację.

Antywirusowe bazy danych

Bazy danych zawierające informacje o zagrożeniach ochrony komputera znane specjalistom z Kaspersky w momencie opublikowania baz danych. Sygnatury antywirusowych baz danych pomagają wykrywać szkodliwy kod w skanowanych obiektach. Antywirusowe bazy danych są tworzone przez specjalistów z Kaspersky i aktualizowane co godzinę.

Archiwum

Jeden lub kilka plików spakowanych w jeden skompresowany plik. Do spakowania i wypakowania danych potrzebna jest specjalna aplikacja zwana archiwizatorem.

Baza adresów phishingowych

Lista adresów internetowych, które specjaliści z Kaspersky określili jako związane z phishingiem. Baza danych jest regularnie aktualizowana i jest częścią pakietu dystrybucyjnego aplikacji Kaspersky.

Baza danych szkodliwych adresów internetowych

Lista adresów internetowych o potencjalnie niebezpiecznej zawartości. Lista jest tworzona przez specjalistów z Kaspersky. Lista ta jest regularnie aktualizowana oraz znajduje się w pakiecie dystrybucyjnym aplikacji Kaspersky.

Certyfikat licencji

Dokument, który jest dostarczany użytkownikowi wraz z plikiem klucza lub kodem aktywacyjnym. Zawiera informacje o licencji nadanej użytkownikowi.

Cloud Discovery

Cloud Discovery umożliwia zarządzanie dostępem użytkowników do usług w chmurze. Usługami w chmurze są przykładowo aplikacje Microsoft Teams, Salesforce i Microsoft Office 365. Usługi w chmurze można podzielić na kategorie, takie jak *Udostępnianie plików*, *Komunikatory*, *Poczta elektroniczna*.

Fałszywy alarm

Fałszywy alarm występuje wtedy, gdy aplikacja Kaspersky uzna niezainfekowany plik za zainfekowany, gdyż sygnatura pliku przypomina sygnaturę wirusa.

Grupa administracyjna

Zbiór urządzeń posiadających takie same role i zainstalowany zestaw aplikacji Kaspersky. Urządzenia są grupowane, aby można było nimi wygodnie zarządzać jak pojedynczą jednostką. Grupa może zawierać w sobie inne grupy. Możliwe jest utworzenie profili grupowych i zadań grupowych dla każdej zainstalowanej aplikacji w grupie.

IOC

Wskaźnik naruszeń bezpieczeństwa. Zestaw danych dotyczących szkodliwego obiektu lub aktywności.

Leczenie

Metoda przetwarzania zainfekowanych obiektów skutkująca pełnym lub częściowym odzyskaniem danych. Nie każdy zainfekowany obiekt może zostać wyleczony.

Light Agent

Komponent Kaspersky Endpoint Security for Virtualization Light Agent. Jest instalowany na każdej maszynie wirtualnej, która wymaga ochrony.

Maska

Reprezentacja nazwy i rozszerzenia pliku przy użyciu symboli wieloznacznych.

Maski plików mogą zawierać dowolne znaki dozwolone w nazwach plików oraz symbole wieloznaczne:

- Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.

- Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską. Maska ** jest dostępna tylko do tworzenia wykluczeń ze skanowania.

- Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

Obiekt OLE

Załączony plik lub plik wbudowany w inny plik. Aplikacje firmy Kaspersky pozwalają na skanowanie obiektów OLE w poszukiwaniu wirusów. Na przykład, gdy dokument Microsoft Office Word zawiera tabelę Microsoft Office Excel®, będzie ona skanowana jako obiekt OLE.

Obszar ochrony

Obiekty, które są cały czas skanowane przez Podstawową ochronę przed zagrożeniami, gdy jest ona włączona. Obszary ochrony różnych modułów mają odmienne właściwości.

Obszar skanowania

Obiekty, które są skanowane przez Kaspersky Endpoint Security podczas uruchamiania zadania skanowania.

OpenIOC

Otwarty standard opisów Wskaźników naruszeń bezpieczeństwa (IOC) oparty na XML i zawierający ponad 500 różnych Wskaźników naruszeń bezpieczeństwa.

Plik infekowalny

Plik, który ze względu na swoją strukturę lub format może zostać użyty przez hakerów jako „kontener” do przechowywania i rozprzestrzeniania szkodliwego kodu. Zazwyczaj chodzi tu o pliki wykonywalne o rozszerzeniach, takich jak .com, .exe i .dll. Istnieje dość wysokie ryzyko wprowadzenia szkodliwego kodu do takich plików.

Plik IOC

Plik zawierający zestaw wskaźników naruszeń bezpieczeństwa (IOC), które aplikacja próbuje dopasować do licznika wykryć. Prawdopodobieństwo wykrycia może być wyższe, jeśli w wyniku skanowania dla obiektu znaleziono dokładne dopasowania z kilkoma plikami IOC.

Przenośny menedżer plików

To jest aplikacja oferującą interfejs do pracy z zaszyfrowanymi plikami na dyskach wymiennych, gdy funkcja szyfrowania nie jest dostępna na komputerze.

Serwer integracyjny

Komponent Kaspersky Endpoint Security for Virtualization Light Agent. Współpracuje z komponentami Kaspersky Endpoint Security i infrastrukturą wirtualną.

SVM

Bezpieczna maszyna wirtualna – specjalna maszyna wirtualna, na której zainstalowana jest usługa scanserver (serwer ochrony, komponent rozwiązania Kaspersky Endpoint Security for Virtualization Light Agent).

Trusted Platform Module (moduł TPM)

Mikroczip zaprojektowany do zapewnienia podstawowych funkcji związanych z bezpieczeństwem (na przykład do przechowywania kluczy szyfrowania). Trusted Platform Module jest zazwyczaj instalowany w płycie głównej komputera i komunikuje się z wszystkimi pozostałymi komponentami systemu za pośrednictwem magistrali sprzętowej.

Uwierzytelnianie Kerberos

Mechanizm wzajemnego uwierzytelniania klienta i serwera przed nawiązaniem między nimi połączenia, umożliwiający komunikację w obrębie niezabezpieczonych sieci. Mechanizm ten opiera się na zgłoszeniu, który użytkownik otrzymuje od zaufanego centrum uwierzytelniania.

Wystawca certyfikatu

Centrum certyfikacji, które wydało certyfikat.

Zadanie

Funkcje wykonywane przez aplikacje firmy Kaspersky jako zadania, na przykład: Ochrona plików w czasie rzeczywistym, Pełne skanowanie urządzenia, Aktualizacja baz danych.

Zainfekowany plik

Plik zawierający szkodliwy kod (kod znanego szkodliwego programu, który został wykryty podczas skanowania pliku). Kaspersky nie zaleca korzystania z takich plików, ponieważ mogą prowadzić do zainfekowania komputera.

Znormalizowana postać adresu zasobu sieciowego

Znormalizowana postać adresu zasobu sieciowego to tekstowa reprezentacja adresu zasobu sieciowego, uzyskana poprzez normalizację. *Normalizacja* to proces, w którym tekstowa reprezentacja adresu zasobu sieciowego zmienia się zgodnie z określonymi regułami (na przykład, wykluczenie portu połączenia, hasła i loginu użytkownika z reprezentacji adresu zasobu sieciowego; dodatkowo adres zasobu sieciowego jest zmieniany z dużych znaków na małe).

W kontekście działania składników ochrony celem normalizacji adresu zasobu sieciowego jest pominięcie kolejnych skanowań adresów stron internetowych, które mają różną składnię, a fizycznie są takie same.

Na przykład:
Nieznormalizowana postać adresu: www.Example.com\.
Znormalizowana postać adresu: www.example.com.

Dodatki

Ta sekcja zawiera informacje uzupełniające treść dokumentu.

Dodatek 1. Ustawienia aplikacji

Do skonfigurowania Kaspersky Endpoint Security można użyć zasady, zadań lub interfejsu aplikacji. Szczegółowe informacje o komponentach aplikacji są dostępne w odpowiednich sekcjach.

Ochrona plików

Komponent Ochrona plików pozwala zapobiegać infekcjom systemu plików komputera. Domyślnie komponent Ochrona plików znajduje się na stałe w pamięci RAM komputera i na bieżąco skanuje wszystkie otwierane, zapisywane i uruchamiane pliki. Ten komponent skanuje pliki na wszystkich dyskach komputera, także na dyskach podłączonych. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej.

Komponent skanuje pliki otwierane przez użytkownika lub aplikację. Jeśli zostanie wykryty szkodliwy plik, Kaspersky Endpoint Security blokuje operację na pliku. Następnie aplikacja leczy lub usuwa szkodliwy plik, w zależności od ustawień komponentu Ochrona plików.

Podczas próby uzyskania dostępu do pliku, którego zawartość znajduje się w chmurze OneDrive, Kaspersky Endpoint Security pobierze i przeskanuje zawartość pliku.

Ustawienia komponentu Ochrona plików

Parametr	Opis
Poziom ochrony *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Dla modułu Ochrona plików program Kaspersky Endpoint Security można zastosować różne grupy ustawień. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane *poziomami ochrony*. • **Wysoki**. Jeśli wybrano ten poziom ochrony plików, moduł Ochrona plików będzie dokładnie kontrolować wszystkie otwierane, zapisywane i uruchamiane pliki. Komponent Ochrona plików skanuje wszystkie typy plików na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera. Moduł ten skanuje także archiwa, pakiety instalacyjne i osadzone obiekty OLE. • **Zalecany**. Ten poziomy ochrony plików jest zalecany przez specjalistów z Kaspersky Lab. Komponent Ochrona plików skanuje wszystkie formaty plików na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera, a także osadzonych obiektów OLE. Moduł Ochrona plików nie skanuje archiwów oraz pakietów instalacyjnych. • **Niski**. Ustawienia tego poziomu ochrony plików zapewniają maksymalną prędkość skanowania. Komponent Ochrona plików skanuje tylko pliki z określonymi rozszerzeniami na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera. Moduł Ochrona plików nie skanuje plików złożonych.
Typy plików *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	**Wszystkie pliki**. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanować wszystkie pliki bez wyjątku (wszystkie formaty i rozszerzenia). **Pliki skanowane według formatu**. Jeżeli wybierzesz tę opcję, aplikacja będzie skanować tylko infekowalne pliki. Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików. **Pliki skanowane według rozszerzenia**. Jeżeli wybierzesz tę opcję, aplikacja będzie skanować tylko infekowalne pliki. Format pliku będzie określany w oparciu o jego rozszerzenie.
Obszar skanowania	Zawiera obiekty skanowane przez moduł Ochrona plików. Skanowanym obiektem może być dysk twardy, nośnik wymienny, dysk sieciowy, folder, plik lub kilka plików zdefiniowanych według maski. Domyślnie Ochrona plików skanuje pliki uruchamiane na dyskach twardych, dyskach wymiennych i dyskach sieciowych. Obszar ochrony dla tych obiektów nie może zostać zmieniony ani usunięty. Możesz wykluczać ze skanowań tylko obiekty (np. nośniki wymienne).

Parametr	Opis
Uczenie maszynowe i analiza sygnatur *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Metoda uczenia maszynowego i analiza sygnatur używa baz danych Kaspersky Endpoint Security, które zawierają opisy znanych zagrożeń oraz metody ich neutralizowania. Ochrona korzystająca z tej metody zapewnia minimalny dopuszczalny poziom ochrony. W oparciu o zalecenia ekspertów z Kaspersky, uczenie maszynowe i analiza sygnatur jest zawsze włączona.
Analiza heurystyczna *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa. Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.
Działanie po wykryciu zagrożenia	**Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja usunie plik. **Wylecz; blokuj, jeśli leczenie nie jest możliwe**. Jeśli wybrano tę opcję, aplikacja automatycznie podejmuje próbę wyleczenia zainfekowanego pliku, który został wykryty. Jeżeli leczenie nie powiedzie się, aplikacja zablokuje ten plik. **Blokuj**. Jeśli wybrano tę opcję, aplikacja automatycznie zablokuje zainfekowany plik, bez podjęcia próby jego wyleczenia lub usunięcia. Przed próbą wyleczenia lub usunięcia zainfekowanego pliku, aplikacja utworzy kopię zapasową pliku w przypadku, gdy potrzebujesz przywrócić plik lub jeśli może zostać wyleczony w przyszłości.
Skanuj tylko nowe i zmienione pliki	Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.
Skanuj archiwa	Skanowanie ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE i innych archiwów. Aplikacja skanuje archiwa nie tylko według rozszerzenia, ale także według formatu. Podczas sprawdzania archiwów aplikacja przeprowadzi cykliczne rozpakowywanie. Pozwala to na wykrywanie zagrożeń w archiwach wielopoziomowych (archiwach wewnątrz archiwów).
Skanuj pakiety dystrybucyjne	Skanowanie pakietów dystrybucyjnych aplikacji firm trzecich.
Skanuj pliki w formatach Microsoft Office	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty. Aplikacja skanuje pliki w formacie Office, które są mniejsze niż 1 MB, niezależnie od tego, czy pole wyboru jest zaznaczone, czy nie.
Skanuj pliki formatu poczty elektronicznej	Skanuje pliki w formacie e-mail. Aplikacja skanuje pliki MSG i EML. Pliki w formacie e-mail zawierają także obiekty OLE oraz pliki MHT. Kaspersky Endpoint Security skanuje pliki w formacie e-mail, które są mniejsze niż 1 MB, niezależnie od tego, czy pole wyboru jest zaznaczone, czy nie.
Nie rozpakowuj dużych plików złożonych	Jeżeli to pole jest zaznaczone, aplikacja nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość. Jeśli pole nie jest zaznaczone, aplikacja skanuje pliki złożone o wszystkich rozmiarach. Aplikacja skanuje pliki o dużych rozmiarach, które zostają wypakowane z archiwów niezależnie od tego, czy pole jest zaznaczone.

Parametr	Opis
Rozpakowywanie plików złożonych w tle	Jeśli pole jest zaznaczone, aplikacja oferuje dostęp do plików złożonych, które mają większy rozmiar niż wartość określona przed skanowaniem tych plików. W tym przypadku Kaspersky Endpoint Security rozpakowuje i skanuje pliki złożone w tle. Aplikacja oferuje dostęp do plików złożonych, których rozmiar jest mniejszy niż ta wartość dopiero po rozpakowaniu i przeskanowaniu tych plików. Jeśli pole nie jest zaznaczone, aplikacja oferuje dostęp do plików złożonych dopiero po rozpakowaniu i przeskanowaniu plików dowolnego rozmiaru.
Tryb skanowania *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Kaspersky Endpoint Security skanuje pliki, do których dostęp uzyskał użytkownik, system operacyjny lub aplikacja uruchomiona z poziomu konta użytkownika. **Tryb Inteligentny**. W tym trybie Ochrona plików skanuje obiekt w oparciu o analizę akcji podejmowanych na obiekcie. Na przykład, jeżeli wykorzystywany jest dokument Microsoft Office, Kaspersky Endpoint Security skanuje plik przy jego pierwszym otwieraniu i ostatnim zamykaniu. Wszystkie operacje wykonywane w międzyczasie, które nadpisują plik, nie są skanowane. **Podczas dostępu i modyfikacji**. W tym trybie moduł Ochrona plików skanuje obiekty za każdym razem, gdy są otwierane lub modyfikowane. **Podczas dostępu**. W tym trybie moduł Ochrona plików skanuje obiekty podczas ich otwierania. **Podczas wykonywania**. W tym trybie moduł Ochrona plików skanuje obiekty jedynie podczas ich uruchamiania.
Technologia iSwift *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.
Użyj technologii iChecker *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).
Wstrzymaj moduł Ochrona plików *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	To powoduje tymczasowe i automatyczne wstrzymanie działania modułu Ochrona plików o określonym czasie lub podczas pracy z określonymi aplikacjami.
Skanowanie operacji na plikach wykonywanych w kontenerach Windows	W razie wykrycia zagrożenia wewnątrz kontenera aplikacja zastosuje czynność wybraną dla komponentu Ochrona plików. **Zatrzymaj kontener, jeśli dezynfekcja się nie powiedzie**. Aplikacja może nie mieć wystarczających uprawnień do odczytu i zapisu wykrytego obiektu. W takim przypadku wyleczenie lub usunięcie wykrytego obiektu będzie niemożliwe. Jeśli to pole wyboru jest zaznaczone, aplikacja blokuje wykryty obiekt i wstrzymuje kontener. Jeśli to pole wyboru nie jest zaznaczone, aplikacja tylko blokuje wykryty obiekt. **Nie skanuj operacji na plikach wykonywanych w kontenerach Windows**. Jeśli to pole wyboru jest zaznaczone, aplikacja skanuje kontener tylko podczas jego uruchamiania. Jeśli to pole wyboru nie jest zaznaczone, aplikacja będzie stale skanować kontener w czasie rzeczywistym.

Ochrona WWW

Komponent Ochrona WWW zapobiega pobieraniu szkodliwych plików z internetu, a także blokuje szkodliwe i phishingowe strony internetowe. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej.

Kaspersky Endpoint Security skanuje ruch HTTP, HTTPS i FTP. Kaspersky Endpoint Security skanuje adresy internetowe i adresy IP.

Aby móc korzystać z Ochrony WWW, należy wykonać początkową konfigurację aplikacji:

- Do monitorowania ruchu HTTPS, włącz skanowanie połączeń szyfrowanych (domyślnie włączone).
- Wybierz porty, które musi monitorować Kaspersky Endpoint Security (domyślnie aplikacja monitoruje wszystkie porty).
- Wybierz aplikacje, których ruch ma być monitorowany za pomocą Kaspersky Endpoint Security. Większość przeglądarek znajduje się już na liście aplikacji zalecanych przez Kaspersky. Jeśli Twojej przeglądarki nie ma na liście, dodaj ją ręcznie.
- Zalecamy wstrzyknąć skrypt interakcji ze stroną internetową do ruchu sieciowego (domyślnie wstrzykiwanie skryptów jest wyłączone). Ten skrypt umożliwia rejestrację zdarzeń Ochrony WWW dla dziennika zdarzeń aplikacji, dziennika zdarzeń systemu operacyjnego i raportów.

Gdy użytkownik próbuje otworzyć złośliwą lub phishingową stronę internetową, Kaspersky Endpoint Security zablokuje dostęp i wyświetli ostrzeżenie.

Ustawienia komponentu Ochrona WWW

Parametr	Opis
Poziom ochrony *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Dla modułu Ochrona WWW aplikacja można zastosować różne grupy ustawień. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane *poziomami ochrony*. • **Wysoki**. Poziom ochrony, zgodnie z którym Ochrona WWW przeprowadza maksymalne skanowanie ruchu sieciowego, odbieranego przez komputer poprzez protokoły HTTP i FTP. Ochrona WWW szczegółowo skanuje wszystkie obiekty ruchu sieciowego, używając pełnego zestawu baz danych aplikacji, a także przeprowadza najbardziej szczegółową analizę heurystyczną. • **Zalecany**. Jest to poziom ochrony zapewniający optymalna równowagę pomiędzy wydajnością aplikacji a ochroną ruchu sieciowego. Ochrona WWW wykonuje analizę heurystyczną na średnim poziomie. Ten poziom ochrony ruchu sieciowego jest zalecany przez specjalistów z Kaspersky. • **Niski**. Ustawienia tego poziomu ochrony ruchu sieciowego zapewniają maksymalną prędkość skanowania ruchu sieciowego. Ochrona WWW wykonuje analizę heurystyczną na niskim poziomie.
Działanie po wykryciu zagrożenia	**Blokuj**. Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Ochrona WWW zablokuje dostęp do obiektu i wyświetli komunikat w przeglądarce. **Poinformuj**. Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Kaspersky Endpoint Security pozwala na pobranie tego obiektu na komputer, ale dodaje informacje o zainfekowanym obiekcie do listy aktywnych zagrożeń.
Sprawdź adres internetowy w bazie danych szkodliwych adresów internetowych *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Skanowanie odnośników do określenia, czy znajdują się w bazie danych szkodliwych odnośników pozwoli na śledzenie stron internetowych, które zostały dodane do listy zablokowanych. Baza danych szkodliwych adresów internetowych, która została stworzona przez Kaspersky, znajduje się w pakiecie instalacyjnym aplikacji i jest aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.
Użyj analizy heurystycznej *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa. Jeśli ruch sieciowy jest skanowany w poszukiwaniu wirusów i innych aplikacji, które stwarzają zagrożenie, analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.

Parametr	Opis
Sprawdź adres internetowy w bazie danych phishingowych adresów internetowych *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Baza danych phishingowych adresów internetowych zawiera adresy internetowe obecnie znanych stron wykorzystywanych przy atakach phishingowych. Kaspersky uzupełnia tę bazę odnośników phishingowych o adresy uzyskane z międzynarodowej organizacji znanej jako Anti-Phishing Working Group. Baza danych adresów phishingowych znajduje się w pakiecie instalacyjnym aplikacji, jest również aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.
Nie skanuj ruchu sieciowego z zaufanych adresów internetowych	Jeśli ta opcja jest zaznaczona, moduł Ochrona WWW nie skanuje zawartości stron internetowych lub stron, których adresy znajdują się na liście zaufanych adresów internetowych. Do listy zaufanych adresów internetowych możesz dodać określony adres i maskę adresu strony internetowej. Możesz także utworzyć ogólną listę wykluczeń dla połączeń szyfrowanych. W tym przypadku program Kaspersky Endpoint Security nie skanuje ruchu sieciowego HTTPS zaufanych adresów internetowych, gdy komponenty Ochrona WWW, Ochrona poczty, Kontrola sieci wykonują swoją pracę.

Ochrona poczty

Ochrona poczty skanuje załączniki odbieranych i wysyłanych wiadomości e-mail w poszukiwaniu wirusów i innych zagrożeń. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej.

Ochrona poczty może skanować zarówno wiadomości odbierane, jak i wysyłane. Aplikacja obsługuje protokoły POP3, SMTP, IMAP i NNTP w następujących klientach pocztowych:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Aby skanować ruch w klientach pocztowych Mozilla Thunderbird, MyOffice Mail i R7-Office Organizer, musisz dodać certyfikat Kaspersky do magazynu certyfikatów oraz wybrać własny magazyn certyfikatów.

Ochrona poczty nie obsługuje innych protokołów i klientów pocztowych.

Ochrona poczty może nie zawsze być w stanie zyskać dostęp do wiadomości na *poziomie protokołu* (na przykład podczas korzystania z rozwiązania Microsoft Exchange). Z tego powodu Ochrona poczty obejmuje rozszerzenie dla programu Microsoft Office Outlook. Rozszerzenie umożliwia skanowanie wiadomości na *poziomie klienta pocztowego*. Rozszerzenie Ochrony poczty obsługuje 32- i 64-bitowe wersje programów Outlook 2010, 2013, 2016, 2019, 2021, 2024 i 365. Na komputerach opartych na architekturze Arm rozszerzenie Ochrony poczty obsługuje 32- i 64-bitowe wersje programów Outlook 2016, Outlook 2021, Outlook 2024 i Outlook 365 dla architektury Arm64.

Komponent Ochrona poczty nie skanuje wiadomości, jeśli klient poczty jest otwarty w przeglądarce.

Gdy w załączniku zostanie wykryty szkodliwy plik, Kaspersky Endpoint Security dodaje informację o wykonanej akcji do tematu wiadomości, na przykład: *[Wiadomość została przetworzona] <temat wiadomości>*.

Parametr	Opis
Poziom ochrony *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Dla modułu Ochrona poczty aplikacja może zastosować różne grupy ustawień. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane *poziomami ochrony*. • **Wysoki**. Jeśli wybrany jest ten poziom ochrony, moduł Ochrona poczty szczegółowo skanuje wiadomości e-mail. Ochrona poczty skanuje przychodzące i wychodzące wiadomości e-mail, a także przeprowadza szczegółową analizę heurystyczną. Wysoki poziom ochrony poczty jest zalecany dla środowisk wysokiego ryzyka. Przykładem takiego środowiska jest korzystanie z darmowego serwera pocztowego, który nie jest chroniony żadnym systemem antywirusowym. • **Zalecany**. Jest to poziom ochrony zapewniający optymalną równowagę pomiędzy wydajnością aplikacji a ochroną poczty. Ochrona poczty skanuje wiadomości przychodzące i wychodzące, a także przeprowadza analizę heurystyczną na średnim poziomie intensywności. Ten poziom ochrony ruchu pocztowego jest zalecany przez specjalistów z Kaspersky. • **Niski**. Jeśli wybrany jest ten poziom ochrony, moduł Ochrona poczty skanuje tylko wiadomości przychodzące, wykonuje analizę heurystyczną na niskim poziomie, a także nie skanuje archiwów załączonych do wiadomości e-mail. Na tym poziomie moduł Ochrona poczty skanuje wiadomości z maksymalną prędkością i używa minimalnej ilości zasobów systemu operacyjnego. Niski poziom ochrony jest zalecany podczas pracy w dobrze chronionym środowisku. Przykładem takiego środowiska może być firmowa sieć LAN ze scentralizowaną ochroną poczty.
Działanie po wykryciu zagrożenia	**Wylecz; usuń, jeśli leczenie nie jest możliwe**. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej lub wychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, aplikacja usunie zainfekowany obiekt. Aplikacja doda informacje o wykonanym działaniu do tematu wiadomości, na przykład: *[Przetworzono wiadomość] <temat wiadomości>*. **Wylecz; blokuj, jeśli leczenie nie jest możliwe**. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, aplikacja doda ostrzeżenie do tematu wiadomości. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, aplikacja podejmie próbę wyleczenia wykrytego obiektu. Jeśli obiektu nie można wyleczyć, aplikacja zablokuje transmisję wiadomości, a klient poczty wyświetli błąd. **Blokuj**. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, aplikacja doda ostrzeżenie do tematu wiadomości. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, aplikacja zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.
Obszar ochrony *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	*Obszar ochrony* zawiera obiekty, które komponent sprawdza podczas działania: wiadomości odbierane i wysyłane lub tylko wiadomości przychodzące. Aby chronić komputery, należy skanować tylko wiadomości przychodzące. Możesz włączyć skanowanie wiadomości wychodzących, aby zapobiec wysłaniu zainfekowanych plików w archiwach. Możesz także włączyć skanowanie wiadomości wychodzących, jeśli chcesz zapobiec wysłaniu plików w określonych formatach, na przykład plików audio i wideo.
Skanuj ruch POP3, SMTP, NNTP i IMAP	Skanowanie ruchu przesyłanego przez protokoły POP3, SMTP, NNTP i IMAP wykonywane przez komponent Ochrona poczty.
Włącz rozszerzenie Microsoft Outlook	Jeśli pole jest zaznaczone, skanowanie wiadomości przesyłanych poprzez protokoły POP3, SMTP, NNTP, IMAP jest włączone po stronie rozszerzenia zintegrowanego w Microsoft Outlook. Jeśli poczta jest skanowana przy użyciu rozszerzenia dla programu Microsoft Outlook, zalecane jest korzystanie z Cached Exchange Mode. Więcej informacji dotyczących trybu buforowanego programu Exchange oraz zalecenia dotyczące korzystania z tego trybu można znaleźć w Bazie wiedzy Microsoft.
Analiza heurystyczna *(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)*	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa. Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.
Skanuj załączone archiwa	Skanowanie ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE i innych archiwów. Aplikacja skanuje archiwa nie tylko według rozszerzenia, ale także według formatu. Podczas sprawdzania archiwów aplikacja przeprowadzi cykliczne rozpakowywanie. Pozwala to na wykrywanie zagrożeń w archiwach wielopoziomowych (archiwach wewnątrz archiwów). Jeżeli podczas skanowania aplikacja wykryje w tekście wiadomości hasło do archiwum, hasło to zostanie wykorzystane do przeskanowania zawartości archiwum w poszukiwaniu szkodliwych aplikacji. W tym przypadku hasło nie zostaje zapisane. Archiwum jest rozpakowywane podczas skanowania. Jeśli podczas rozpakowywania wystąpi błąd aplikacji, można ręcznie usunąć rozpakowane pliki, które są zapisywane w następującej ścieżce: %systemroot%\temp. Pliki mają prefiks PR.

Parametr	Opis
Skanuj załączone pliki w formatach Microsoft Office	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty. Aplikacja skanuje pliki w formacie Office, które są mniejsze niż 1 MB, niezależnie od tego, czy pole wyboru jest zaznaczone, czy nie.
Nie skanuj archiwów większych niż N MB	Jeżeli pole jest zaznaczone, moduł Ochrona poczty wyklucza ze skanowania archiwa, załączone do wiadomości, których rozmiar przekracza określoną wartość. Jeżeli pole nie jest zaznaczone, moduł Ochrona poczty skanuje załączone archiwa o dowolnym rozmiarze.
Ogranicz czas sprawdzania archiwów do N sec	Jeżeli pole jest zaznaczone, czas skanowania załączonych archiwów jest ograniczony.
Filtr załączników	Filtr załączników nie jest stosowany do wychodzących wiadomości e-mail. **Wyłącz filtrowanie**. Jeśli ta opcja jest wybrana, Ochrona poczty nie filtruje plików załączonych do wiadomości e-mail. **Zmień nazwy załączników określonych typów**. Jeśli wybierzesz tę opcję, Ochrona poczty zastąpi ostatni znak rozszerzenia wykryty w załączonych plikach określonych typów znakiem podkreślenia (na przykład: attachment.doc_). Dlatego, aby otworzyć plik, użytkownik musi zmienić jego nazwę. **Usuń załączniki wybranych typów**. Jeśli ta opcja jest zaznaczona, Ochrona poczty usuwa załączone pliki określonych typów z wiadomości e-mail. Na liście masek plików możesz określić typy załączonych plików, których nazwy mają zostać zmienione lub które mają zostać usunięte z wiadomości e-mail.

Ochrona sieci

Składnik *Ochrona sieci* (zwany także Intrusion Detection System, IDS) monitoruje przychodzący ruch sieciowy pod kątem aktywności charakterystycznej dla ataków sieciowych. Gdy Kaspersky Endpoint Security wykryje próbę ataku sieciowego na komputerze użytkownika, zablokuje połączenie sieciowe z komputerem atakującym. Opisy znanych typów ataków sieciowych oraz sposoby ich zwalczania znajdują się w bazach danych aplikacji. Lista ataków sieciowych, wykrywanych przez komponent Ochrona sieci, jest uaktualniana podczas aktualizacji baz danych i modułów aplikacji.

Ustawienia komponentu Ochrona sieci

Parametr	Opis
Traktuj skanowanie portów i "network flooding" jako ataki	*Zalewanie sieci* jest atakiem na zasoby sieciowe (takie jak serwery internetowe). Ten atak obejmuje wysyłanie dużej liczby żądań w celu przeciążenia przepustowości zasobów sieciowych. W takiej sytuacji użytkownicy nie mogą uzyskać dostępu do zasobów sieciowych organizacji. Atak *Skanowanie portów* obejmuje skanowanie portów UDP, portów TCP, a także usługi sieciowe komputera. Ten atak umożliwia atakującemu zidentyfikowanie stopnia podatności komputera przed przeprowadzeniem bardziej niebezpiecznych rodzajów ataków sieciowych. Skanowanie portów umożliwia atakującemu także zidentyfikowanie systemu operacyjnego na komputerze i wybranie odpowiednich ataków sieciowych dla tego systemu operacyjnego. Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security monitoruje ruch sieciowy do wykrywania następujących ataków dla. W przypadku wykrycia ataku aplikacja powiadamia użytkownika i wysyła odpowiednie zdarzenie do Kaspersky Security Center. Aplikacja dostarcza informacji o atakującym komputerze, co jest niezbędne do szybkiego reagowania na zagrożenia. Możesz wyłączyć wykrywanie tych rodzajów ataków w przypadku, gdy niektóre z Twoich dozwolonych aplikacji wykonują działania typowe dla tych rodzajów ataków. Pomoże to w uniknięciu fałszywych alarmów.
Blokuj atakujące urządzenia przez N min	Jeśli pole jest zaznaczone, Ochrona sieci dodaje atakujący komputer do listy zablokowanych. Oznacza to, że komponent Ochrona sieci zablokuje na określony czas połączenie sieciowe z atakującym komputerem po pierwszej próbie ataku sieciowego. Ta blokada automatycznie chroni komputer użytkownika przed przyszłymi atakami sieciowymi pochodzącymi z tego samego adresu. Minimalny czas, przez jaki atakujący komputer będzie znajdować się na liście blokowanych, to jedna minuta. Maksymalny czas to 999 minut. W oknie Narzędzia Monitor sieci możesz przejrzeć listę blokowania. Kaspersky Endpoint Security czyści listę blokowania, gdy aplikacja zostanie ponownie uruchomiona, a ustawienia Ochrony sieci zostaną zmienione.

Parametr	Opis
Wykluczenia	Lista zawiera adresy IP, z których Ochrona sieci nie blokuje ataków sieciowych. Możesz dodać adres IP z określonym portem i protokołem. Aplikacja nie zapisuje informacji o atakach sieciowych pochodzących z adresów IP, które znajdują się na liście wykluczeń.
Ochrona przed fałszowaniem adresu MAC	*Atak przez fałszowanie adresu MAC* obejmuje zmianę adresu MAC urządzenia sieciowego (karty sieciowej). W rezultacie osoba atakująca może przekierować dane wysłane do urządzenia na inne urządzenie i uzyskać dostęp do tych danych. Kaspersky Endpoint Security umożliwia blokowanie ataków przez fałszowanie adresu MAC i otrzymywanie powiadomień o atakach.

Zapora sieciowa

Zapora sieciowa blokuje nieautoryzowane połączenia z komputerem podczas pracy w Internecie lub sieci lokalnej. Zapora sieciowa kontroluje również aktywność sieciową aplikacji na komputerze. Pozwala to chronić korporacyjną sieć LAN przed kradzieżą tożsamości i innymi atakami. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i predefiniowanych *reguł sieciowych*.

Agent sieciowy jest używany do interakcji z Kaspersky Security Center. Zapora sieciowa automatycznie tworzy reguły sieciowe wymagane do działania aplikacji i Agenta sieciowego. W wyniku działania Zapora sieciowa otwiera kilka portów na komputerze. Które porty są otwarte w zależności od roli komputera (na przykład, punkt dystrybucji). Więcej informacji o portach, które zostaną otwarte na komputerze, można znaleźć w pomocy dla Kaspersky Security Center.

Reguły sieciowe

Możesz skonfigurować reguły sieciowe na następujących poziomach:

- *Reguły pakietów sieciowych*. Reguły pakietów sieciowych nakładają ograniczenia na pakiety sieciowe, niezależnie od aplikacji. Takie reguły ograniczają ruch sieciowy wychodzący i przychodzący przez określone porty wybranego protokołu. Kaspersky Endpoint Security wstępnie zdefiniował reguły pakietów sieciowych z uprawnieniami zalecanymi przez ekspertów z Kaspersky.
- *Reguły sieciowe dla aplikacji*. Reguły sieciowe dla aplikacji nakładają ograniczenia na aktywność sieciową określonej aplikacji. W tym przypadku brane są pod uwagę cechy charakterystyczne pakietu sieciowego, a także aplikacja, dla której jest on przeznaczony lub która zainicjowała jego przesyłanie.

Kontrolowany dostęp aplikacji do zasobów systemu operacyjnego, procesów i danych osobowych jest zapewniany przez komponent Ochrona przed włamaniami przy użyciu *uprawnień aplikacji*.

Podczas pierwszego uruchomienia aplikacji Zapora sieciowa wykonuje następujące działania:

1. Sprawdza bezpieczeństwo aplikacji przy użyciu pobranych antywirusowych baz danych.
2. Sprawdza bezpieczeństwo aplikacji w Kaspersky Security Network.

   Zalecane jest uczestniczenie w Kaspersky Security Network, aby zapewnić bardziej efektywne działanie Zapory sieciowej.
3. Umieszcza aplikację w jednej z grup zaufania: *Zaufane*, *Niskie ograniczenia*, *Wysokie ograniczenia*, *Niezaufane*.

Grupa zaufania określa uprawnienia, do których program Kaspersky Endpoint Security odnosi się podczas kontrolowania aktywności aplikacji. Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera.

Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania dla składników Zapora sieciowa i Ochrona przed włamaniami. Nie można zmienić grupy zaufania tylko dla Zapory sieciowej lub Ochrony przed włamaniami.

Jeśli odmówiłeś uczestnictwa w KSN lub nie ma sieci, Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od ustawień modułu Ochrona przed włamaniami. Po otrzymaniu reputacji aplikacji od KSN, grupę zaufania można zmienić automatycznie.

4. Blokuje aktywność sieciową aplikacji w zależności od grupy zaufania. Na przykład, aplikacje z grupy *Wysokie ograniczenia* nie mogą korzystać z żadnych połączeń sieciowych.

Przy następnym uruchomieniu aplikacji, Kaspersky Endpoint Security sprawdzi integralność aplikacji. Jeżeli aplikacja nie została zmieniona, moduł użyje dla niej bieżących reguł sieciowych. Jeżeli aplikacja została zmodyfikowana, Kaspersky Endpoint Security analizuje aplikację tak, jakby była uruchamiana po raz pierwszy.

Priorytety reguł sieciowych

Każda reguła posiada priorytet. Im wyżej reguła znajduje się na liście reguł, tym wyższy priorytet posiada. Jeśli aktywność sieci zostanie dodana do kilku reguł, Zapora sieciowa reguluje aktywność sieciową zgodnie z regułą o najwyższym priorytecie.

Reguły pakietów sieciowych mają wyższy priorytet niż reguły sieciowe dla aplikacji. Jeżeli do tego samego typu aktywności sieciowej są zastosowane reguły pakietów sieciowych i reguły sieciowe dla aplikacji, będzie ona przetwarzana zgodnie z regułami pakietów sieciowych.

Reguły sieciowe dla aplikacji działają w określony sposób. Reguła sieciowa dla aplikacji zawiera reguły dostępu oparte na stanie sieci: *Sieć publiczna*, *Sieć lokalna*, *Sieć zaufana*. Na przykład, aplikacje z grupy zaufania *Wysokie ograniczenia* domyślnie nie zezwalają na żadną aktywność sieciową w sieciach o wszystkich stanach. Jeśli dla pojedynczej aplikacji (aplikacji nadrzędnej) zostanie określona reguła sieciowa, procesy potomne innych aplikacji będą działać zgodnie z regułą sieciową aplikacji nadrzędnej. Jeśli nie istnieje reguła sieciowa dla aplikacji, procesy potomne będą działały zgodnie z regułą dostępu do sieci grupy zaufania aplikacji.

Na przykład, zabroniona jest jakakolwiek aktywność sieciowa w sieciach o wszystkich stanach dla wszystkich aplikacji, za wyjątkiem przeglądarki X. Jeśli rozpoczniesz instalację przeglądarki Y (proces potomny) z przeglądarki X (aplikacja nadrzędna), wówczas instalator przeglądarki Y uzyska dostęp do sieci i pobierze niezbędne pliki. Po instalacji przeglądarka Y będzie odmawiała jakichkolwiek połączeń sieciowych zgodnie z ustawieniami Zapory sieciowej. Aby zabronić aktywności sieciowej instalatora przeglądarki Y jako procesu potomnego, należy dodać regułę sieciową dla instalatora przeglądarki Y.

Typy połączenia sieciowego

Zapora sieciowa pozwala kontrolować aktywność sieciową w zależności od typu połączenia sieciowego. Kaspersky Endpoint Security otrzymuje typ połączenia sieciowego z systemu operacyjnego komputera. Typ połączenia sieciowego w systemie operacyjnym jest ustawiany przez użytkownika podczas konfigurowania połączenia. Możesz zmienić typ połączenia sieciowego w ustawieniach Kaspersky Endpoint Security. Zapora sieciowa będzie monitorować aktywność sieci w zależności od typu sieci określonego w ustawieniach Kaspersky Endpoint Security, a nie w systemie operacyjnym.

Dostępne są następujące typy połączeń sieciowych:

- **Sieć publiczna**. Sieć nie jest chroniona przez aplikacje antywirusowe, zapory sieciowe ani filtry (takie jak Wi-Fi w kawiarni). Podczas korzystania z komputera podłączonego do tego typu sieci Zapora sieciowa blokuje dostęp do plików i drukarek tego komputera. Użytkownicy z zewnątrz nie będą mogli również uzyskać dostępu do danych poprzez folder współdzielony oraz zdalnego dostępu do pulpitu tego komputera. Zapora sieciowa filtruje aktywność sieciową każdej aplikacji zgodnie z utworzoną dla niej regułą sieciową.

  Domyślnie zapora sieciowa przypisuje do internetu typ *Sieć publiczna*. Nie możesz zmienić typu przypisanego do internetu.

- **Sieć lokalna**. Sieć dla użytkowników z ograniczonym dostępem do plików i drukarek na tym komputerze (na przykład dla firmowej sieci LAN lub sieci domowej).

- **Sieć zaufana**. Bezpieczna sieć, w której komputer nie jest wystawiony na ataki lub nieautoryzowane próby dostępu do danych. Zapora sieciowa zezwala na dowolną aktywność sieciową w obrębie sieci o tym stanie.

Ustawienia komponentu Zapora sieciowa

Parametr	Opis
Reguły dla pakietów	Tabela zawierająca reguły pakietów sieciowych. Reguły pakietów sieciowych nakładają ograniczenia na pakiety sieciowe, niezależnie od aplikacji. Takie reguły ograniczają ruch sieciowy wychodzący i przychodzący przez określone porty wybranego protokołu. Tabela wyświetla predefiniowane reguły pakietów sieciowych, które są zalecane przez ekspertów z Kaspersky dla optymalnej ochrony ruchu sieciowego komputerów działających pod kontrolą systemów operacyjnych Microsoft Windows. Zapora sieciowa ustawia priorytet wykonania każdej reguły dla pakietu sieciowego. Zapora sieciowa przetwarza reguły w kolejności, w jakiej występują na liście reguł dla pakietów sieciowych (od góry do dołu). Zapora sieciowa odnajduje pierwszą regułę pakietu sieciowego odpowiadającą danemu połączeniu sieciowemu i stosuje ją, zezwalając na lub blokując aktywność sieciową. Następnie Zapora sieciowa ignoruje wszystkie kolejne reguły pakietów sieciowych dla określonego połączenia sieciowego. Reguły pakietów sieciowych mają wyższy priorytet niż reguły sieciowe dla aplikacji.
Dostępne sieci	Ta tabela zawiera informacje o połączeniach sieciowych wykrywanych na komputerze przez Zaporę sieciową. Domyślnie do internetu przypisywany jest stan *Sieć publiczna*. Nie możesz zmienić stanu przypisanego do internetu.
Reguły dla aplikacji	**Aplikacja**. Tabela aplikacji kontrolowanych przez komponent Zapora sieciowa. Aplikacje są przypisywane do grup zaufania. Grupa zaufania określa prawa używane przez Kaspersky Endpoint Security podczas kontrolowania aktywności sieciowej aplikacji. Możesz wybrać aplikację z jednej listy wszystkich aplikacji zainstalowanych na komputerach pod kontrolą zasady i dodać aplikację do grupy zaufania. **Reguły sieciowe**. Tabela reguł sieciowych dla aplikacji należących do grupy zaufania. Zgodnie z tymi regułami Zapora sieciowa reguluje aktywność sieciową aplikacji. Tabela wyświetla predefiniowane reguły sieciowe, które są zalecane przez ekspertów z Kaspersky. Te reguły sieciowe zostały dodane w celu optymalnej ochrony ruchu sieciowego komputerów z systemami operacyjnymi Windows. Nie można usunąć predefiniowanych reguł sieciowych.

Ochrona przed atakami BadUSB

Niektóre wirusy modyfikują oprogramowanie wbudowane urządzeń USB w celu zmylenia systemu operacyjnego do wykrywania urządzenia USB jako klawiatury. W wyniku tego działania wirus może wykonać polecenia z poziomu konta użytkownika, na przykład, w celu pobrania szkodliwego oprogramowania.

Komponent Ochrona przed atakami BadUSB zapobiega podłączeniu do komputera zainfekowanych urządzeń USB emulujących klawiaturę.

Po podłączeniu urządzenia USB do komputera i zidentyfikowaniu go przez system operacyjny jako klawiatury, aplikacja wyświetli pytanie o wprowadzenie kodu numerycznego, wygenerowanego przez aplikację, z poziomu tej klawiatury lub Klawiatury ekranowej, jeśli jest dostępna (patrz rysunek poniżej). Ta procedura jest znana jako autoryzacja klawiatury.

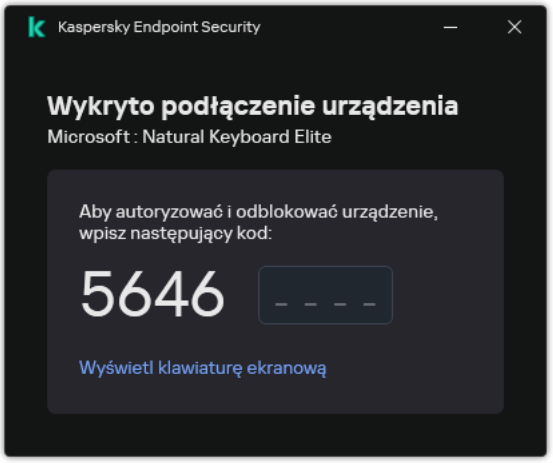
Jeśli kod został wpisany poprawnie, aplikacja zapisuje parametry identyfikujące – VID/PID klawiatury oraz numer portu, do którego została podłączona – na liście uprawnionych klawiatur. Po ponownym podłączeniu klawiatury lub po ponownym uruchomieniu systemu nie ma konieczności powtarzania procesu autoryzacji klawiatury.

Jeśli autoryzowana klawiatura zostanie podłączona do innego portu USB, aplikacja ponownie wyświetli prośbę o przeprowadzenie autoryzacji tej klawiatury.

Jeśli kod numeryczny zostanie wprowadzony niepoprawnie, aplikacja wygeneruje nowy kod. Możesz skonfigurować liczbę prób wprowadzenia kodu numerycznego. Jeśli kod numeryczny zostanie wprowadzony niepoprawnie kilka razy lub okno autoryzacji klawiatury jest zamknięte (patrz rysunek poniżej), aplikacja zablokuje wprowadzenie z poziomu tej klawiatury. Po upłynięciu czasu blokowania urządzenia USB lub ponownym uruchomieniu systemu operacyjnego, aplikacja ponownie wyświetli pytanie o przeprowadzenie autoryzacji klawiatury.

Aplikacja zezwoli na użycie zautoryzowanej klawiatury, a zablokuje klawiaturę, która nie została zautoryzowana.

Komponent Ochrona przed atakami BadUSB nie jest domyślnie instalowany. Jeśli potrzebujesz składnika Ochrona przed atakami BadUSB, możesz dodać ten składnik we właściwościach pakietu instalacyjnego przed zainstalowaniem aplikacji lub zmienić dostępne składniki aplikacji po zainstalowaniu aplikacji.



Autoryzacja klawiatury

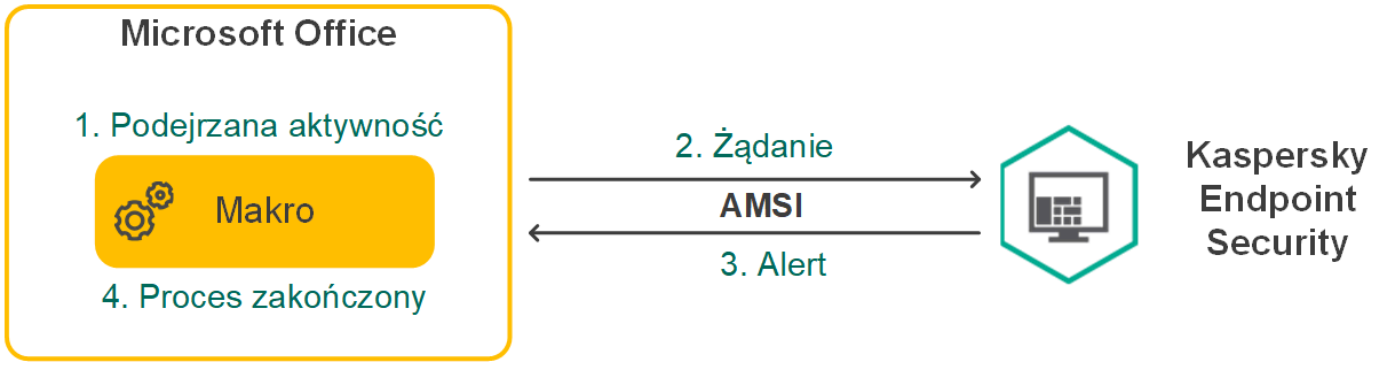
Ustawienia komponentu Ochrona przed atakami BadUSB

Parametr	Opis
Zabroń korzystania z klawiatury ekranowej do autoryzacji urządzeń USB	Jeśli ten przełącznik jest włączony, aplikacja zablokuje użycie Klawiatury ekranowej podczas autoryzacji urządzenia USB, z poziomu którego nie można wpisać kodu autoryzacyjnego.
Blokuj korzystanie z kodu kreskowego do autoryzacji urządzeń USB	Jeśli ten przełącznik jest włączony, aplikacja nie wyświetla kodu kreskowego w powiadomieniu o uwierzytelnieniu czytnika kodów kreskowych.
Maksymalna liczba prób autoryzacji urządzenia USB	Automatyczne blokowanie urządzenia USB, jeśli kod autoryzacyjny jest wprowadzany niepoprawnie określoną liczbę. Ważne wartości to 1 do 10. Na przykład, jeśli zezwolisz na pięć prób wprowadzenia kodu autoryzacyjnego, aplikacja zablokuje urządzenie USB po piątej nieudanej próbie. Kaspersky Endpoint Security wyświetla czas blokowania dla urządzenia USB. Po upływie tego czasu możliwe będzie podjęcie pięciu prób wprowadzenia kodu autoryzacyjnego.
Przerwa po osiągnięciu maksymalnej liczby prób	Czas trwania blokady urządzenia USB po określonej liczbie nieudanych prób wprowadzenia kodu autoryzacyjnego. Ważne wartości to 1 do 180 (minuty).

Ochrona AMSI

Komponent Ochrona AMSI jest przeznaczony do obsługi Antimalware Scan Interface firmy Microsoft. *Antimalware Scan Interface (AMSI)* umożliwia aplikacjom firm trzecich z obsługą AMSI wysyłanie obiektów (na przykład, skryptów PowerShell) do Kaspersky Endpoint Security w celu przeprowadzenia dodatkowego skanowania i otrzymania wyników ze skanowania tych obiektów. Aplikacje firm trzecich mogą obejmować, na przykład, aplikacje Microsoft Office (patrz rysunek poniżej). Więcej informacji na temat AMSI znajdziesz w dokumentacji firmy Microsoft.

Ochrona AMSI może tylko wykrywać zagrożenia i informować aplikację firmy trzeciej o wykrytym zagrożeniu. Aplikacja zewnętrzna, po odebraniu powiadomienia o zagrożeniu, nie zezwala na wykonanie szkodliwych działań (na przykład kończy proces).



Przykład działania AMSI

Komponent Ochrona AMSI może odrzucić żądanie z aplikacji firmy trzeciej, na przykład, jeśli ta aplikacja przekracza maksymalną liczbę żądań w określonym przedziale czasu. Kaspersky Endpoint Security wyśle informacje o odrzuconym żądaniu z aplikacji firmy trzeciej do Serwera administracyjnego. Komponent Ochrona AMSI nie zablokuje żądań od tych aplikacji firm trzecich, dla których jest włączona trwała integracja z komponentem Ochrona AMSI.

Ochrona AMSI jest dostępny dla następujących systemów operacyjnych dla stacji roboczych i serwerów:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise wielosesyjny
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter (w tym tryb Server Core)

- Windows Server 2019 Essentials / Standard / Datacenter (w tym tryb Server Core)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (w tym tryb Server Core)
- Windows Server 2025 Standard / Datacenter

Ustawienia Ochrony AMSI

Parametr	Opis
Skanuj archiwa	Skanowanie ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE i innych archiwów. Aplikacja skanuje archiwa nie tylko według rozszerzenia, ale także według formatu. Podczas sprawdzania archiwów aplikacja przeprowadzi cykliczne rozpakowywanie. Pozwala to na wykrywanie zagrożeń w archiwach wielopoziomowych (archiwach wewnątrz archiwów).
Skanuj pakiety dystrybucyjne	Skanowanie pakietów dystrybucyjnych aplikacji firm trzecich.
Skanuj pliki w formatach Microsoft Office	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty. Aplikacja skanuje pliki w formacie Office, które są mniejsze niż 1 MB, niezależnie od tego, czy pole wyboru jest zaznaczone, czy nie.
Nie rozpakowuj dużych plików złożonych	Jeżeli to pole jest zaznaczone, aplikacja nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość. Jeśli pole nie jest zaznaczone, aplikacja skanuje pliki złożone o wszystkich rozmiarach. Aplikacja skanuje pliki o dużych rozmiarach, które zostają wypakowane z archiwów niezależnie od tego, czy pole jest zaznaczone.

Ochrona przed exploitami

Komponent Ochrona przed exploitami wykrywa kod programu, który wykorzystuje luki na komputerze, aby użyć uprawnień administratora lub wykonać szkodliwe aktywności. Na przykład, exploity mogą używać ataku typ buffer overflow (przepełnienie bufora). Aby to zrobić, exploit wysyła dużą ilość danych do aplikacji zawierającej lukę. Podczas przetwarzania tych danych aplikacja zawierająca lukę wykona szkodliwy kod. W wyniku tego ataku exploit może uruchomić nieautoryzowaną instalację szkodliwego programu. Po wykryciu, że próba uruchomienia pliku wykonywalnego z aplikacji zawierającej luki nie została zainicjowana przez użytkownika, Kaspersky Endpoint Security zablokuje uruchomienie tego pliku lub poinformuje użytkownika.

Komponent Ochrona przed exploitami dodatkowo monitoruje porty sieciowe w poszukiwaniu procesów aplikacji, które mogą zagrozić bezpieczeństwu komputera. Aplikacja pobiera informacje o takich procesach z baz danych programów antywirusowych.

Ustawienia komponentu Ochrona przed exploitami

Parametr	Opis
Po wykryciu exploita	**Zablokuj**. Jeśli ten element jest wybrany, po wykryciu exploita, Kaspersky Endpoint Security zablokuje działania tego exploita i zarejestruje w raporcie informacje o tym exploicie. **Poinformuj**. Jeśli ten element jest wybrany, gdy Kaspersky Endpoint Security wykryje exploita, zarejestruje w raporcie informacje o exploicie i doda informacje o tym exploicie do listy aktywnych zagrożeń.
Włącz ochronę pamięci procesów systemowych	Jeśli ten przycisk przełącznika jest ustawiony w pozycji włączenia, Kaspersky Endpoint Security zablokuje zewnętrzne procesy, które próbują uzyskać dostęp do pamięci procesów systemowych.

Wykrywanie zachowań

Komponent Wykrywanie zachowań gromadzi dane na temat działań aplikacji na komputerze i dostarcza te informacje innym składnikom ochrony w celu udoskonalenia ich działania. Komponent Wykrywanie zachowań używa sygnatur strumieni zachowań (BSS) dla aplikacji. Jeśli aktywność aplikacji odpowiada sygnaturze strumienia zachowań, Kaspersky Endpoint Security wykona wybrane działanie. Funkcjonalność Kaspersky Endpoint Security oparta na sygnaturach strumieni zachowań zapewnia proaktywną ochronę komputera.

Komponent Wykrywanie zachowań dodatkowo monitoruje porty sieciowe w poszukiwaniu procesów aplikacji, które mogą zagrozić bezpieczeństwu komputera. Aplikacja pobiera informacje o takich procesach z baz danych programów antywirusowych.

Ustawienia komponentu Wykrywanie zachowań

Parametr	Opis
Akcja wykonywana po wykryciu aktywności szkodliwego oprogramowania	**Usuń**. Jeśli ta opcja jest zaznaczona, po wykryciu szkodliwej aktywności program Kaspersky Endpoint Security usunie plik wykonywalny szkodliwej aplikacji i utworzy kopię zapasową pliku w Kopii zapasowej. **Zablokuj**. Jeśli ta opcja jest zaznaczona, po wykryciu szkodliwej aktywności Kaspersky Endpoint Security zakończy działanie tej aplikacji. **Poinformuj**. Jeśli ta opcja jest zaznaczona i zostanie wykryta szkodliwa aktywność aplikacji, Kaspersky Endpoint Security nie zakończy działania tej aplikacji, ale doda informację o szkodliwej aktywności tej aplikacji do listy aktywnych zagrożeń.

Ochrona przed włamaniami

Ochrona przed włamaniami uniemożliwia aplikacjom wykonywanie działań niebezpiecznych dla systemu operacyjnego i zapewnia kontrolę dostępu do zasobów systemu operacyjnego i danych osobowych. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network.

Komponent kontroluje działanie aplikacji za pomocą *uprawnień aplikacji*. Uprawnienia aplikacji obejmują następujące parametry dostępu:

- Dostęp do zasobów systemu operacyjnego (na przykład opcje automatycznego uruchamiania, klucze rejestru)
- Dostęp do danych osobowych (takich jak pliki i aplikacje)

Aktywność sieciowa aplikacji jest kontrolowana przez Zaporę sieciową za pomocą *reguł sieciowych*.

Podczas pierwszego uruchomienia aplikacji Ochrona przed włamaniami wykonuje następujące działania:

1. Sprawdza bezpieczeństwo aplikacji przy użyciu pobranych antywirusowych baz danych.
2. Sprawdza bezpieczeństwo aplikacji w Kaspersky Security Network.

   Zalecane jest uczestniczenie w Kaspersky Security Network, aby zapewnić bardziej efektywne działanie komponentu Ochrona przed włamaniami.

3. Umieszcza aplikację w jednej z grup zaufania: *Zaufane*, *Niskie ograniczenia*, *Wysokie ograniczenia*, *Niezaufane*.

   Grupa zaufania określa uprawnienia, do których program Kaspersky Endpoint Security odnosi się podczas kontrolowania aktywności aplikacji. Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera.

   Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania dla składników Zapora sieciowa i Ochrona przed włamaniami. Nie można zmienić grupy zaufania tylko dla Zapory sieciowej lub Ochrony przed włamaniami.

Jeśli odmówiłeś uczestnictwa w KSN lub nie ma sieci, Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od ustawień modułu Ochrona przed włamaniami. Po otrzymaniu reputacji aplikacji od KSN, grupę zaufania można zmienić automatycznie.

4. Blokuje działania aplikacji w zależności od grupy zaufania. Na przykład, aplikacje z grupy *Wysokie ograniczenia* mają zablokowany dostęp do modułów systemu operacyjnego.

Przy następnym uruchomieniu aplikacji, Kaspersky Endpoint Security sprawdzi integralność aplikacji. Jeżeli aplikacja nie została zmieniona, moduł użyje dla niej bieżących uprawnień aplikacji. Jeżeli aplikacja została zmodyfikowana, Kaspersky Endpoint Security analizuje aplikację tak, jakby była uruchamiana po raz pierwszy.

Ustawienia komponentu Ochrona przed włamaniami

Parametr	Opis
Uprawnienia aplikacji	Tabela aplikacji monitorowanych przez komponent Ochrona przed włamaniami. Aplikacje są przypisywane do grup zaufania. Grupa zaufania określa uprawnienia, do których program Kaspersky Endpoint Security odnosi się podczas kontrolowania aktywności aplikacji. Możesz wybrać aplikację z jednej listy wszystkich aplikacji zainstalowanych na komputerach pod kontrolą zasady i dodać aplikację do grupy zaufania. Prawa dostępu do aplikacji zostały przedstawione w następujących tabelach: • **Pliki i rejestr systemu**. Tabela praw dostępu do zasobów systemu operacyjnego i danych osobowych dla aplikacji należących do grupy zaufania. • **Uprawnienia**. Tabela praw dostępu do procesów i zasobów systemu operacyjnego dla aplikacji należących do grupy zaufania. • **Reguły sieciowe**. Tabela reguł sieciowych dla aplikacji należących do grupy zaufania. Zgodnie z tymi regułami Zapora sieciowa reguluje aktywność sieciową aplikacji. Tabela wyświetla predefiniowane reguły sieciowe, które są zalecane przez ekspertów z Kaspersky. Te reguły sieciowe zostały dodane w celu optymalnej ochrony ruchu sieciowego komputerów z systemami operacyjnymi Windows. Nie można usunąć predefiniowanych reguł sieciowych.
Chronione zasoby	Tabela zawiera zasoby komputera podzielone na kategorie. Ochrona przed włamaniami monitoruje próby dostępu innych aplikacji do zasobów znajdujących się w tabeli. Zasobem może być kategoria rejestru, plik lub folder, bądź klucz rejestru.
Grupa zaufania dla aplikacji uruchamianych zanim Kaspersky Endpoint Security zacznie działać	Grupa zaufania, w której Kaspersky Endpoint Security umieści aplikacje uruchomione przed Kaspersky Endpoint Security.
Uaktualnij reguły dla wcześniej nieznanych aplikacji z KSN	Jeśli pole jest zaznaczone, Ochrona przed włamaniami aktualizuje uprawnienia dla wcześniej nieznanych aplikacji przy użyciu bazy danych Kaspersky Security Network.
Ufaj aplikacjom podpisanym cyfrowo	Jeśli pole jest zaznaczone, Ochrona przed włamaniami umieszcza aplikacje posiadające podpis cyfrowy zaufanych dostawców w grupie *Zaufane*. *Zaufani producenci* to producenci oprogramowania, którzy zostali umieszczeni w grupie zaufania przez Kaspersky. Możesz także ręcznie dodać certyfikat producenta do magazynu zaufanych certyfikatów. Jeśli pole nie jest zaznaczone, Ochrona przed włamaniami nie uważa takich aplikacji za zaufane i wykorzystuje inne parametry do określenia ich grupy zaufania.
Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni (od 1 do 90)	Jeśli pole jest zaznaczone, Kaspersky Endpoint Security automatycznie usuwa informacje o aplikacji (grupa zaufania i uprawnienia dostępu), jeśli spełnione są następujące warunki: • Możesz ręcznie umieścić aplikację w grupie zaufania lub skonfigurować jej uprawnienia dostępu. • Aplikacja nie została uruchomiona w określonym przedziale czasu. Jeśli grupa zaufania i uprawnienia aplikacji zostały określone automatycznie, Kaspersky Endpoint Security usunie informacje o tej aplikacji po 30 dniach. Nie jest możliwa zmiana okresu przechowywania informacji o aplikacji ani wyłączenie automatycznego usuwania. Następnym razem, gdy uruchomisz tę aplikację, Kaspersky Endpoint Security analizuje aplikację w taki sposób, jakby była uruchamiana po raz pierwszy.
Grupa zaufania dla aplikacji niezawartych w innych grupach	Elementy na liście rozwijalnej określają, do której grupy zaufania program Kaspersky Endpoint Security przydzieli nieznaną aplikację. Możesz wybrać jeden z następujących elementów: • **Niskie ograniczenia**. • **Wysokie ograniczenia**. • **Niezaufane**.

Silnik korygujący

Silnik korygujący umożliwia Kaspersky Endpoint Security wycofanie działań, które zostały wykonane przez szkodliwe oprogramowanie w systemie operacyjnym.

Podczas cofania szkodliwej aktywności w systemie operacyjnym Kaspersky Endpoint Security podejmuje działanie na następujących typach szkodliwej aktywności:

- **Aktywność plikowa**

  Kaspersky Endpoint Security wykonuje następujące działania:

  - Usuwa pliki wykonywalne, które zostały utworzone przez szkodliwe oprogramowanie (na wszystkich mediach za wyjątkiem dysków sieciowych).
  - Usuwa pliki wykonywalne, które zostały utworzone przez programy, do których przeniknęło szkodliwe oprogramowanie.
  - Przywraca pliki, które zostały zmodyfikowane lub usunięte przez szkodliwe oprogramowanie.

  Funkcja odzyskiwania plików posiada kilka ograniczeń.

- **Aktywność w rejestrze**

  Kaspersky Endpoint Security wykonuje następujące działania:

  - Usuwa klucze rejestru, które zostały utworzone przez szkodliwe oprogramowanie.
  - Nie przywraca kluczy rejestru, które zostały zmodyfikowane lub usunięte przez szkodliwe oprogramowanie.

- **Aktywność w systemie**

  Kaspersky Endpoint Security wykonuje następujące działania:

  - Kończy procesy, które zostały zainicjowane przez szkodliwe oprogramowanie.
  - Kończy procesy, do których przeniknęła szkodliwa aplikacja.
  - Nie wznawia procesów zatrzymanych przez szkodliwy program.

- **Aktywność sieciowa**

  Kaspersky Endpoint Security wykonuje następujące działania:

  - Blokuje aktywność sieciową szkodliwego oprogramowania.
  - Blokuje aktywność sieciową procesów, do których przeniknęło szkodliwe oprogramowanie.

Wycofanie działań szkodliwych programów może być zainicjowane przez komponent Ochrona plików lub Wykrywanie zachowań lub podczas skanowania antywirusowego.

Wycofywanie działań szkodliwego oprogramowania oddziałuje na ściśle określony zestaw danych. Nie ma negatywnego wpływu na system operacyjny i integralność danych komputera.

Kaspersky Security Network

Aby lepiej chronić Twój komputer, Kaspersky Endpoint Security wykorzystuje dane otrzymane od użytkowników z całego świata. Usługa Kaspersky Security Network została zaprojektowana do gromadzenia tych danych.

Funkcja KSN może nie być dostępna w oprogramowaniu na terytorium Stanów Zjednoczonych.

Kaspersky Security Network (KSN) jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobów sieciowych oraz oprogramowania. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi programu Kaspersky Endpoint Security na nowe zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów. Jeśli uczestniczysz w Kaspersky Security Network, usługi KSN zapewniają Kaspersky Endpoint Security informacje o reputacji przeskanowanych adresów internetowych, a także informacje o kategorii i reputacji przeskanowanych plików. Więcej szczegółowych informacji o konfigurowaniu dostępu do KSN można znaleźć w pomocy do Kaspersky Security Center.

Korzystanie z Kaspersky Security Network jest dobrowolne. Aplikacja oferuje użytkownikowi możliwość korzystania z KSN podczas wstępnej konfiguracji aplikacji. Użytkownik może rozpocząć lub zakończyć uczestniczenie w KSN w dowolnym momencie.

Więcej informacji na temat wysyłania do Kaspersky informacji statystycznych, wygenerowanych w trakcie uczestnictwa w KSN, a także informacji o przechowywaniu i niszczeniu takich informacji można znaleźć w Umowie Kaspersky Security Network oraz na stronie Kaspersky. Plik ksn_<ID języka>.txt zawierający treść Oświadczenia Kaspersky Security Network znajduje się w pakiecie dystrybucyjnym aplikacji.

Infrastruktura baz danych reputacji firmy Kaspersky

Kaspersky Endpoint Security obsługuje następujące rozwiązania infrastrukturalne do pracy z bazami danych reputacji Kaspersky:

- *Kaspersky Security Network (KSN)* to rozwiązanie używane przez większość aplikacji Kaspersky. Uczestnicy KSN otrzymują informacje od firmy Kaspersky i wysyłają do Kaspersky informacje o obiektach wykrytych na komputerze użytkownika w celu dodatkowego przeanalizowania przez analityków Kaspersky i dołączenia ich do baz danych reputacji oraz statystycznych.

- *Kaspersky Private Security Network (KPSN)* to rozwiązanie, które umożliwia użytkownikom komputerów z zainstalowanym programem Kaspersky Endpoint Security lub innymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów. Sieć KPSN została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z dowolnego z następujących powodów:

  - Lokalne stacje robocze nie są połączone z internetem.

Przesyłanie wszelkich danych poza kraj lub poza korporacyjną sieć LAN są zabronione przez prawo lub ograniczone przez politykę bezpieczeństwa firmy.

Parametr	Opis
Włącz rozszerzony tryb KSN	*Rozszerzony tryb KSN* to tryb, w którym Kaspersky Endpoint Security wysyła dodatkowe dane do Kaspersky. Kaspersky Endpoint Security używa KSN do wykrywania zagrożeń niezależnie od pozycji przełącznika.
Włącz tryb chmury	*Tryb chmury* odnosi się do trybu działania aplikacji, w którym Kaspersky Endpoint Security używa lekkiej wersji antywirusowych baz danych. Kaspersky Security Network obsługuje działanie aplikacji, gdy używana jest lekka wersja antywirusowych baz danych. Lekka wersja antywirusowych baz danych umożliwia korzystanie z około połowy pamięci RAM komputera, która inaczej zostałaby użyta ze zwykłymi bazami danych. Jeśli nie uczestniczysz w Kaspersky Security Network lub jeśli tryb chmury jest wyłączony, Kaspersky Endpoint Security pobierze pełną wersję antywirusowych baz danych z serwerów Kaspersky. Jeśli przycisk przełącznika jest ustawiony w pozycji włączenia, Kaspersky Endpoint Security używa podstawowej wersji antywirusowych baz danych, co zmniejsza zużycie zasobów systemu operacyjnego. Po zaznaczeniu pola, Kaspersky Endpoint Security pobierze podstawową wersję antywirusowych baz danych podczas kolejnej aktualizacji. Jeśli przycisk przełącznika jest ustawiony w pozycji wyłączenia, Kaspersky Endpoint Security używa kompletnej wersji antywirusowych baz danych. Po odznaczeniu pola, Kaspersky Endpoint Security pobierze kompletną wersję antywirusowych baz danych podczas kolejnej aktualizacji.
Stan komputera, gdy serwery KSN są niedostępne *(dostępny tylko w Kaspersky Security Center Console)*	Elementy na liście rozwijalnej określają stan komputera w Kaspersky Security Center, gdy serwery KSN są niedostępne.
Użyj serwera administracyjnego jako serwera proxy KSN *(dostępny tylko w Kaspersky Security Center Console)*	Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security używa usługi KSN Proxy. Możliwe jest skonfigurowanie ustawień usługi KSN Proxy we właściwościach Serwera administracyjnego.
Użyj serwerów Kaspersky Security Network, jeżeli KSN Proxy jest niedostępny *(dostępny tylko w Kaspersky Security Center Console)*	Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security używa serwerów KSN, jeśli usługa KSN Proxy jest niedostępna. Serwery KSN mogą znajdować się zarówno po stronie firmy Kaspersky, jak i stron trzecich (w przypadku korzystania z Kaspersky Private Security Network).

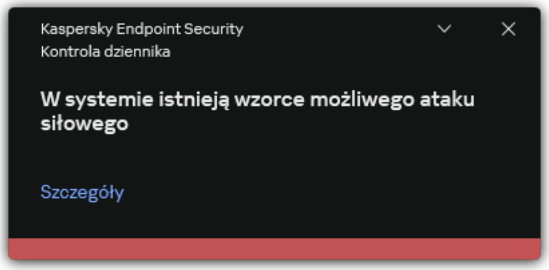
Kontrola dziennika

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych.

Począwszy od wersji 11.11.0 Kaspersky Endpoint Security for Windows zawiera komponent Kontrola dziennika. Komponent Kontrola dziennika monitoruje integralność chronionego środowiska na podstawie analizy dziennika zdarzeń systemu Windows. Gdy aplikacja wykryje oznaki nietypowego zachowania w systemie, informuje o tym administratora, gdyż zachowanie to może świadczyć o próbie cyberataku.

Kaspersky Endpoint Security analizuje dzienniki zdarzeń systemu Windows i wykrywa naruszenia zgodnie z regułami. Komponent ten zawiera wstępnie zdefiniowane reguły. Wstępnie zdefiniowane reguły są oparte na analizie heurystycznej. Można również dodać własne reguły (reguły niestandardowe). W momencie uruchomienia reguły aplikacja tworzy zdarzenie o stanie *Krytyczny* (patrz rysunek poniżej).

Jeśli chcesz użyć komponentu Kontrola dziennika, upewnij się, że skonfigurowane są ustawienia zabezpieczeń polityki audytu, a system rejestruje odpowiednie zdarzenia (szczegóły znajdziesz na stronie pomocy technicznej firmy Microsoft).



Powiadomienie z kontroli dziennika

Ustawienia kontroli dziennika

Parametr	Opis
Wstępnie zdefiniowane reguły	Lista reguł modułu Kontrola dziennika. Wstępnie zdefiniowane reguły zawierają szablony nieprawidłowej aktywności na chronionym komputerze. Nietypowa aktywność może oznaczać próbę ataku.
Reguły niestandardowe	Lista reguł modułu Kontrola dziennika dodanych przez użytkownika. Można ustawić własne kryteria wyzwalania reguły kontroli dziennika. Aby to zrobić, należy wprowadzić identyfikator zdarzenia i wybrać źródło zdarzenia. Można wybrać źródło zdarzeń spośród standardowych dzienników: *Application*, *Security* lub *System*. Można również określić dziennik aplikacji innej firmy.

Anti-Cryptor

Komponent Anti-Cryptor analizuje aktywność w folderach współdzielonych. Jeśli to działanie jest zgodne z sygnaturą strumieni zachowań, która jest typowa dla zewnętrznego szyfrowania, Kaspersky Endpoint Security wykonuje wybraną akcję.

Kaspersky Endpoint Security zapobiega szyfrowaniu zewnętrznemu tylko tych plików, które znajdują się na nośniku z systemem plików NTFS i nie są szyfrowane przez system EFS.

Parametr	Opis
Wykluczenia według nazwy lub adresu IP	**Wykluczenia według nazwy lub adresu IP**. Lista komputerów, z których próby zaszyfrowania folderów współdzielonych nie będą monitorowane. Aby zastosować listę wykluczeń komputerów z ochrony folderów współdzielonych przed zewnętrznym szyfrowaniem, należy włączyć Przeprowadź inspekcję logowania w zasadach inspekcji zabezpieczeń Windows. Domyślnie Przeprowadź inspekcję logowania jest wyłączone. Więcej informacji o zasadach inspekcji zabezpieczeń Windows można znaleźć na stronie internetowej firmy Microsoft. **Wykluczenia wg maski**. Wyłączenia z zakresu ochrony. Wykluczenie folderu z zakresu ochrony może zmniejszyć liczbę fałszywych alarmów, jeśli Twoja organizacja używa szyfrowania danych podczas wymiany plików za pomocą folderów współdzielonych. Na przykład Wykrywanie zachowania może dawać fałszywe alarmy, gdy użytkownik pracuje z plikami z rozszerzeniem ENC w folderze współdzielonym. Takie działanie odpowiada wzorcowi zachowania, który jest typowy dla szyfrowania zewnętrznego. Jeśli w celu ochrony danych zaszyfrowałeś pliki w folderze współdzielonym, dodaj ten folder do wykluczeń. Użyj masek: • Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach. • Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską. • Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.
Działanie po wykryciu zagrożenia	• **Poinformuj**. Jeśli ta opcja jest zaznaczona, po wykryciu próby modyfikacji plików w folderach współdzielonych Kaspersky Endpoint Security doda informacje o tym zdarzeniu do listy aktywnych zagrożeń oraz wpis do raportów dotyczących interfejsu aplikacji lokalnej i wyśle informacje o wykrytej szkodliwej aktywności do Kaspersky Security Center. • **Blokuj połączenie przez (min) N min**. Jeśli ta opcja jest zaznaczona, gdy Kaspersky Endpoint Security wykryje próbę zmodyfikowania plików w folderach współdzielonych, zablokuje dostęp do modyfikacji pliku w sesji, która zainicjowała podejrzane działanie i utworzy kopie zapasowe zmodyfikowanych plików. Jeśli komponent Silnik korygujący jest włączony, a opcja **Blokuj połączenie przez (min) N min** jest zaznaczona, zmodyfikowane pliki zostaną przywrócone z kopii zapasowych.
Obszar ochrony	Ten *zakres ochrony* jest listą ścieżek do folderów współdzielonych, w których Kaspersky Endpoint Security monitoruje aktywność plików. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`. Domyślnie aplikacja automatycznie identyfikuje foldery współdzielone i monitoruje aktywność plików we wszystkich folderach.

Kontrola sieci

Kontrola sieci zarządza dostępem użytkowników zasobów sieciowych. Pomaga to zmniejszyć ruch sieciowy i nieodpowiednie dysponowanie czasem pracy. Gdy użytkownik próbuje otworzyć stronę internetową ograniczoną przez Kontrolę sieci, Kaspersky Endpoint Security zablokuje dostęp lub wyświetli ostrzeżenie (patrz rysunek poniżej).

Aby móc korzystać z Kontroli sieci, należy wykonać początkową konfigurację aplikacji:

- Do monitorowania ruchu HTTPS, włącz skanowanie połączeń szyfrowanych (domyślnie włączone).
- Wybierz porty, które musi monitorować Kaspersky Endpoint Security (domyślnie aplikacja monitoruje wszystkie porty).

- Wybierz aplikacje, których ruch ma być monitorowany za pomocą Kaspersky Endpoint Security. Większość przeglądarek znajduje się już na liście aplikacji zalecanych przez Kaspersky. Jeśli Twojej przeglądarki nie ma na liście, dodaj ją ręcznie.

- Zalecamy wstrzyknąć skrypt interakcji ze stroną internetową do ruchu sieciowego (domyślnie wstrzykiwanie skryptów jest wyłączone). Ten skrypt umożliwia rejestrację zdarzeń Kontroli sieci dla dziennika zdarzeń aplikacji, dziennika zdarzeń systemu operacyjnego i raportów.

Metody zarządzania dostępem do stron internetowych

Kontrola sieci umożliwia konfigurowanie dostępu do stron internetowych przy użyciu następujących metod:

- **Kategoria strony internetowej**. Strony internetowe są kategoryzowane zgodnie z usługą chmury Kaspersky Security Network, analizą heurystyczną i bazą danych znanych stron internetowych (znajdującą się w bazach danych aplikacji). Na przykład, możesz ograniczyć dostęp użytkownika do kategorii *Sieci społecznościowe* lub do innych kategorii.

- **Typ danych**. Na przykład, możesz ograniczyć dostęp użytkowników do danych na stronie internetowej i ukryć zawartość graficzną. Kaspersky Endpoint Security określa typ danych w oparciu o format pliku, a nie w oparciu o jego rozszerzenie.

  > Kaspersky Endpoint Security nie skanuje plików w archiwach. Na przykład, jeśli pliki obrazów zostały umieszczone w archiwum, Kaspersky Endpoint Security identyfikuje typ danych *Archiwa*, a nie *Grafika*.

- **Określony adres**. Możesz wprowadzić adres internetowy lub użyć masek.

Możesz jednocześnie użyć kilku metod do regulowania dostępu do stron internetowych. Na przykład, możesz ograniczyć dostęp do typu danych *Pliki aplikacji pakietu Office* tylko dla kategorii stron internetowych *Poczta elektroniczna przez WWW*.

Reguły dostępu do stron internetowych

Kontrola sieci zarządza dostępem użytkowników do stron internetowych przy użyciu *reguł dostępu*. Możesz skonfigurować następujące zaawansowane ustawienia reguły dostępu do stron internetowych:

- Użytkowników, do których stosowana jest reguła.

  Na przykład, możesz ograniczyć dostęp do internetu poprzez przeglądarkę dla wszystkich użytkowników firmy, za wyjątkiem działu IT.

- Terminarz reguły.

  Na przykład, możesz ograniczyć dostęp do internetu poprzez przeglądarkę tylko w trakcie godzin pracy.

Priorytety reguł dostępu

Każda reguła posiada priorytet. Im wyżej reguła znajduje się na liście reguł, tym wyższy priorytet posiada. Jeśli strona internetowa została dodana do kilku reguł, Kontrola sieci reguluje dostęp do strony internetowej w oparciu o regułę z najwyższym priorytetem. Na przykład, Kaspersky Endpoint Security może identyfikować portal firmowy jako sieć społecznościową. Aby ograniczyć dostęp do sieci społecznościowych i zapewnić dostęp do firmowego portalu internetowego, utwórz dwie reguły: jedną regułę blokady dla kategorii stron internetowych *Sieci społecznościowe* i jedną regułę zezwalającą dla firmowego portalu internetowego. Reguła dostępu dla firmowego portalu internetowego musi posiadać wyższy priorytet niż reguła dostępu dla sieci społecznościowych.



Wiadomości Kontroli sieci

Parametr	Opis
Reguły dostępu do zasobów sieciowych	Lista zawierająca reguły dostępu do zasobu sieciowego. Każda reguła posiada priorytet. Im wyżej reguła znajduje się na liście reguł, tym wyższy priorytet posiada. Jeśli strona internetowa została dodana do kilku reguł, Kontrola sieci reguluje dostęp do strony internetowej w oparciu o regułę z najwyższym priorytetem.
Reguła domyślna	*Domyślna reguła* to reguła dostępu do zasobów internetowych, które nie są objęte żadną inną regułą. Dostępne są następujące opcje: • **Zezwól na wszystko poza listą reguł**, także znana jako tryb listy zablokowanych dla zabronionych stron internetowych. • **Odrzuć wszystko poza listą reguł**, także znana jako tryb listy zezwolonych dla dozwolonych stron internetowych.
Przerwij aktywne sesje przeglądarki użytkownika po zastosowaniu zasady	Jeżeli to pole wyboru jest zaznaczone, Kontrola sieci natychmiast po zastosowaniu zasad zakończy połączenie z zablokowanymi zasobami internetowymi. Przeglądarka natychmiast zatrzymuje pobieranie danych ze strony internetowej. Gdy odświeżysz stronę internetową lub przejdziesz na inną zabronioną stronę, aplikacja wyświetli ostrzeżenie. Kontrola sieci pozwala na natychmiastowe rozłączanie zasobów sieciowych wyłącznie w przeglądarkach. W innych aplikacjach Kontrola sieci ogranicza tylko nowe połączenia. Jeśli pole wyboru jest odznaczone, Kontrola sieci ogranicza nowe połączenia tylko do zabronionych zasobów sieciowych. Kontrola sieci nie kończy aktywnych połączeń.
Szablony	**Ostrzeżenie**. Pole do wprowadzenia danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła ostrzegająca o próbach uzyskania dostępu do niechcianych zasobów sieciowych. **Wiadomość dotycząca blokowania**. To pole do wprowadzania danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła blokująca dostęp do zasobu sieciowego. **Wiadomość do administratora**. Szablon wiadomości wysyłanej do administratora sieci LAN, gdy użytkownik uważa blokadę za pomyłkę. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania dostępu do strony internetowej**. Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkownika**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail. Do zarządzania szablonami wiadomości dostępne są zmienne specjalne (na przykład `%USER_NAME%`). Zmienne umożliwiają stosowanie tego samego szablonu wiadomości na różnych komputerach.
Zapisuj informacje o otwarciu dozwolonych stron	Kaspersky Endpoint Security zapisuje dane dotyczące odwiedzin na wszystkich stronach internetowych, w tym dozwolonych stronach internetowych. Kaspersky Endpoint Security wysyła zdarzenia do Kaspersky Security Center, do lokalnego raportu Kaspersky Endpoint Security, a także do dziennika zdarzeń systemu Windows. Aby monitorować aktywność internetową użytkownika, należy skonfigurować ustawienia zapisywania zdarzeń. Przeglądarki obsługujące funkcję monitorowania: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Monitorowanie aktywności użytkownika nie działa w innych przeglądarkach. Monitorowanie aktywności użytkownika w internecie może wymagać więcej zasobów komputera podczas deszyfrowania ruchu HTTPS.

Kontrola urządzeń

Kontrola urządzeń zarządza dostępem użytkownika do urządzeń, które są instalowane na komputerze lub są podłączone do komputera (na przykład: dyski twarde, kamery lub moduły Wi-Fi). Umożliwia to ochronę komputera przed infekcją, gdy takie urządzenia są podłączone, oraz zapobieganie utracie lub wyciekowi danych.

Jeśli komponent Kontrola urządzeń jest włączony, aplikacja przekazuje informacje o podłączonych urządzeniach do Kaspersky Security Center. Listę podłączonych urządzeń można przejrzeć w Kaspersky Security Center, w folderze **Zaawansowane** → **Repozytoria** → **Sprzęt**.

Poziomy dostępu do urządzenia

Kontrola urządzeń kontroluje dostęp na następujących poziomach:

- **Typ urządzenia**. Na przykład: drukarki, dyski wymienne oraz płyty CD/DVD.

  Dostęp urządzenia możesz skonfigurować w następujący sposób:

  - Zezwól –  .
  - Blokuj –  .
  - Zgodnie z regułami (tylko drukarki i urządzenia przenośne) –  .
  - W zależności od magistrali połączenia (z wyłączeniem Wi-Fi) –  .
  - Blokuj z wyjątkami (Tylko Wi-Fi) –  .

- **Magistrala połączeń**. *Magistrala połączeń* to interfejs używany do podłączania urządzeń do komputera (na przykład: USB lub FireWire). Jeśli tryb **W zależności od magistrali połączenia** jest wybrany dla typu urządzenia, aplikacja zezwala lub odmawia dostępu do urządzenia w zależności od interfejsu połączenia (np. USB).

  Dostęp urządzenia możesz skonfigurować w następujący sposób:

  - Zezwól – .
  - Blokuj –  .

- **Zaufane urządzenia**. *Zaufane urządzenia* są urządzeniami, do których użytkownicy, określeni w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

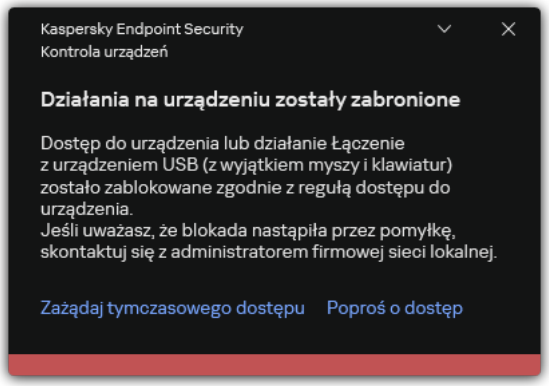
  Możesz dodać zaufane urządzenia w oparciu o następujące dane:

  - **Urządzenia według ID**. Każde urządzenie posiada unikatowy identyfikator (identyfikator sprzętu lub HWID). Możesz sprawdzić identyfikator we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Przykładowy identyfikator urządzenia: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Dodawanie urządzeń według identyfikatora jest wygodne, jeśli chcesz dodać kilka określonych urządzeń.
  - **Urządzenia według modelu**. Każde urządzenie posiada identyfikator producenta (VID) oraz identyfikator produktu (PID). Możesz sprawdzić identyfikatory we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Szablon do wprowadzenia VID i PID: `VID_1234&PID_5678`. Dodawanie urządzeń według modelu jest wygodne, jeśli w swojej organizacji używasz urządzeń pewnego modelu. W ten sposób możesz dodać wszystkie urządzenia tego modelu.
  - **Urządzenia według maski ID**. Jeśli używasz kilku urządzeń z podobnymi identyfikatorami, możesz dodać urządzenia do listy zaufanych, korzystając z maski. Znak `*` zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku `?` podczas wprowadzania maski. Na przykład, `WDC_C*`.
  - **Urządzenia według maski modelu**. Jeśli używasz kilku urządzeń z podobnymi numerami VID lub PID (na przykład, urządzeń od tego samego producenta), możesz dodać urządzenia do listy zaufanych przy użyciu masek. Znak `*` zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku `?` podczas wprowadzania maski. Na przykład, `VID_05AC&PID_*`.

Kontrola urządzeń reguluje dostęp użytkownika do urządzeń przy użyciu *reguł dostępu*. Kontrola urządzeń umożliwia także zapisywanie zdarzeń podłączenia/odłączenia urządzenia. Aby zapisać zdarzenia, musisz skonfigurować rejestrację zdarzeń w profilu.

Jeśli dostęp do urządzenia zależy od magistrali połączenia (stan), Kaspersky Endpoint Security nie zapisuje zdarzeń podłączenia/odłączenia urządzenia. Aby umożliwić Kaspersky Endpoint Security zapisywanie zdarzeń podłączenia/odłączenia urządzenia, zezwól na dostęp do odpowiedniego typu urządzenia (stan) lub dodaj urządzenie do listy zaufanych.

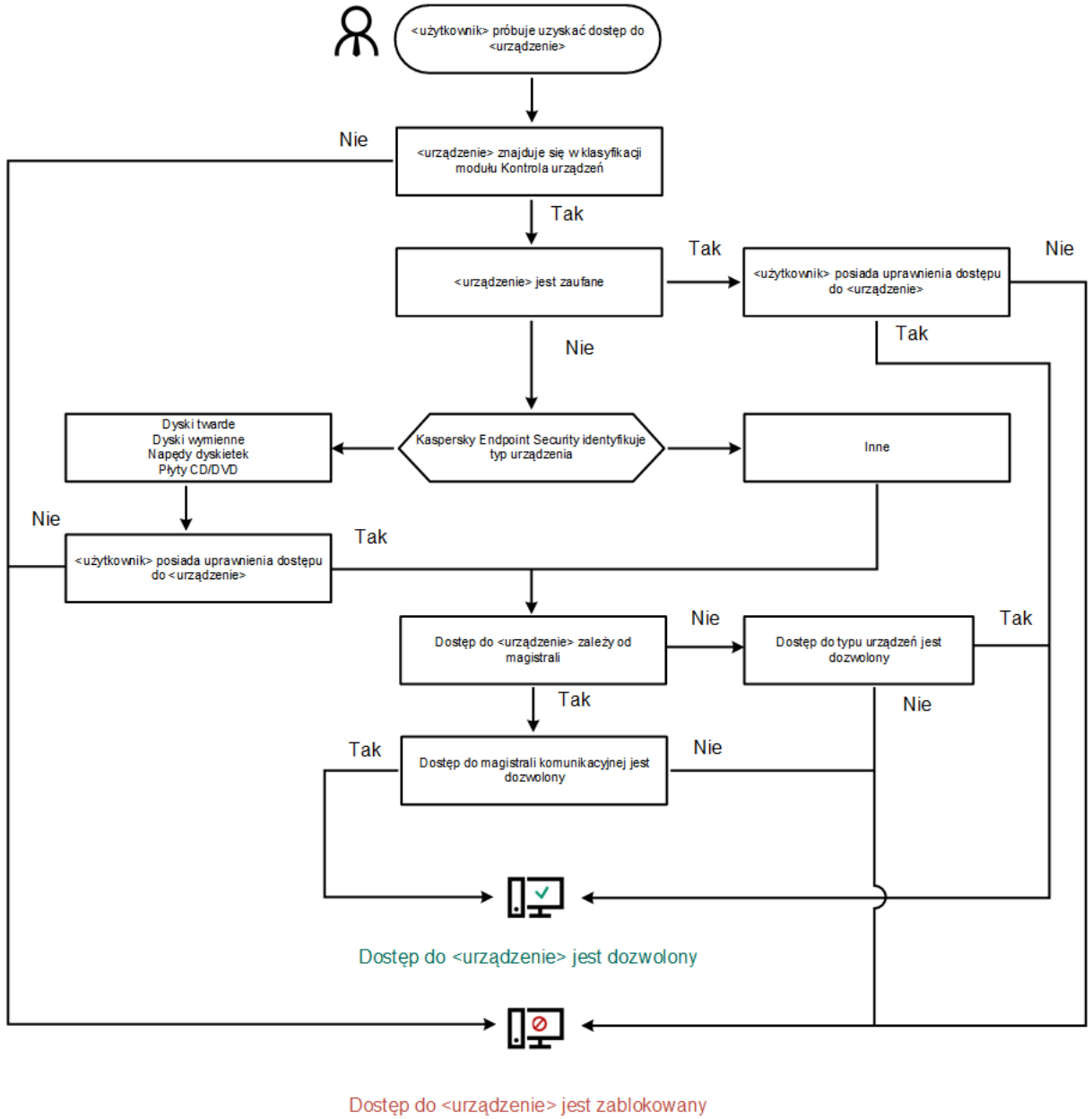
Jeśli urządzenie, które jest zablokowane przez Kontrolę urządzeń, zostanie podłączone do komputera, Kaspersky Endpoint Security zablokuje dostęp i wyświetli komunikat (patrz rysunek poniżej).



Komunikat Kontroli urządzeń

Algorytm działania Kontroli urządzeń

Kaspersky Endpoint Security podejmuje decyzję dotyczącą zezwolenia na dostęp do urządzenia po podłączeniu urządzenia do komputera przez użytkownika (patrz rysunek poniżej).



Algorytm działania Kontroli urządzeń

Jeśli urządzenie jest podłączone i dostęp jest dozwolony, możesz edytować regułę dostępu i zablokować dostęp. W tym przypadku, kolejnym razem, gdy ktoś spróbuje uzyskać dostęp do urządzenia (np. przejrzeć drzewo folderów lub wykonać operacje odczytu lub zapisu), Kaspersky Endpoint Security zablokuje dostęp. Urządzenie bez systemu plików jest blokowane dopiero przy następnym podłączeniu.

Jeśli użytkownik komputera, na którym jest zainstalowany program Kaspersky Endpoint Security, poprosi o dostęp do urządzenia, które uważa, że zostało zablokowane przez pomyłkę, wyślij do użytkownika instrukcje wysyłania pliku żądania dostępu.

Parametr	Opis
Zezwól na żądania dostępu tymczasowego *(dostępny tylko w Kaspersky Security Center Console)*	Jeśli pole jest zaznaczone, przycisk **Poproś o dostęp** staje się dostępny poprzez lokalny interfejs Kaspersky Endpoint Security. Za pomocą tego przycisku można poprosić o tymczasowy dostęp do zablokowanego urządzenia.
Urządzenia i sieci Wi-Fi	Ta tabela zawiera wszystkie możliwe typy urządzeń, zgodnie z klasyfikacją modułu Kontrola urządzeń, uwzględniając ich odpowiednie stany dostępu.
Magistrale	Lista wszystkich dostępnych magistrali połączeń zgodnie z klasyfikacją modułu Kontrola urządzeń, uwzględniając ich stany dostępu. Kaspersky Endpoint Security zezwala lub odmawia dostępu do urządzenia w zależności od typu magistrali połączenia, jeżeli wybrano tryb **W zależności od magistrali połączenia**.
Zaufane urządzenia	Lista zaufanych urządzeń i użytkowników, którym udzielono dostępu do tych urządzeń.
Przenieś wartości podczas dziedziczenia *(dostępny tylko w Kaspersky Security Center Console)*	To powoduje scalenie listy zaufanych urządzeń w zasadach nadrzędnych i podrzędnych konsoli Kaspersky Security Center. Aby scalić listy, zasada potomna musi być skonfigurowana do dziedziczenia ustawień zasady nadrzędnej programu Kaspersky Security Center. Jeśli pole jest zaznaczone, w zasadach potomnych wyświetlane są elementy listy z zasady nadrzędnej Kaspersky Security Center. W ten sposób możesz, na przykład, utworzyć skonsolidowaną listę zaufanych urządzeń dla całej organizacji. Dziedziczone elementy listy w zasadzie potomnej nie mogą zostać usunięte ani edytowane. Elementy na liście zaufanych urządzeń, które są scalone podczas dziedziczenia, można usuwać i edytować tylko w zasadzie nadrzędnej. Możesz dodawać, edytować lub usuwać elementy z list w zasadach niższego poziomu. Jeśli elementy na listach zasady potomnej i nadrzędnej pasują do siebie, te elementy są wyświetlane jak podobne elementy zasady nadrzędnej. Jeśli pole nie zostało zaznaczone, elementy z list nie są scalane podczas dziedziczenia ustawień zasad programu Kaspersky Security Center. Ta funkcja umożliwia również scalanie list w profilach zasad. Aby scalić listy, w profilu o najwyższym priorytecie należy włączyć dziedziczenie ustawień z profilu o niższym priorytecie. Aby uzyskać szczegółowe informacje na temat priorytetów profilu zasady, zapoznaj się z pomocą do Kaspersky Security Center.
Anti-Bridging	Anti-Bridging zapobiega tworzeniu mostków sieciowych poprzez uniemożliwienie jednoczesnego nawiązania kilku połączeń sieciowych dla komputera. To umożliwia ochronę sieci firmowej przed atakami na niechronione, nieautoryzowane sieci. Anti-Bridging blokuje nawiązanie kilku połączeń zgodnie z priorytetami urządzeń. Im wyżej urządzenie znajduje się na liście, tym wyższy priorytet posiada. Jeśli aktywne połączenie i nowe połączenie są tego samego typu (np. Wi-Fi), Kaspersky Endpoint Security zablokuje aktywne połączenie i zezwoli na nawiązanie nowego połączenia. Jeśli aktywne połączenie i nowe połączenie są różnych typów (na przykład, karta sieciowa i Wi-Fi), Kaspersky Endpoint Security zablokuje połączenie z niższym priorytetem i zezwoli na połączenie z wyższym priorytetem. Anti-Bridging obsługuje działanie na następujących typach urządzeń: karta sieciowa, Wi-Fi i modem.
Szablony wiadomości	**Wiadomość dotycząca blokowania**. Szablon wiadomości, która pojawia się, gdy użytkownik próbuje uzyskać dostęp do zablokowanego urządzenia. Ta wiadomość pojawia się, gdy użytkownik próbuje wykonać działanie na zawartości urządzenia, które zostało zablokowane dla tego użytkownika. **Wiadomość do administratora**. Szablon wiadomości, która jest wysyłana do administratora sieci LAN, gdy użytkownik uważa, że dostęp do urządzenia lub wykonywanie działań na zawartości urządzenia zostały zablokowane przez przypadek. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania dostępu do urządzenia**. Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkowników**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

Kontrola aplikacji

Kontrola aplikacji zarządza uruchamianiem aplikacji na komputerach użytkowników. Pozwala to na wdrożenie polityki bezpieczeństwa firmy podczas korzystania z aplikacji. Kontrola aplikacji zmniejsza także ryzyko infekcji komputera poprzez ograniczenie dostępu do aplikacji.

Konfiguracja Kontroli aplikacji obejmuje następujące kroki:

1. Tworzenia kategorii aplikacji.

   Administrator tworzy kategorie aplikacji, którymi chce zarządzać. Kategorie aplikacji są przeznaczone dla wszystkich komputerów w sieci firmowej, niezależnie od grup administracyjnych. Aby utworzyć kategorię, możesz użyć następujących kryteriów: kategoria KL (na przykład: *Przeglądarki*), skrót pliku, dostawca aplikacji i inne kryteria.

2. Tworzenie reguł Kontroli aplikacji.

   Administrator tworzy reguły Kontroli aplikacji w zasadzie dla grupy administracyjnej. Reguła obejmuje kategorie aplikacji i stan uruchamiania aplikacji z tych kategorii: zablokowane lub dozwolone. Administrator może utworzyć wiele reguł. Jeden wniosek może spełniać kryteria wielu zasad. Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Kaspersky Endpoint Security sprawdza, czy aplikacja pasuje do reguły przy każdym uruchomieniu. Kaspersky Endpoint Security sekwencyjnie porównuje aplikację ze wszystkimi regułami Kontroli aplikacji.

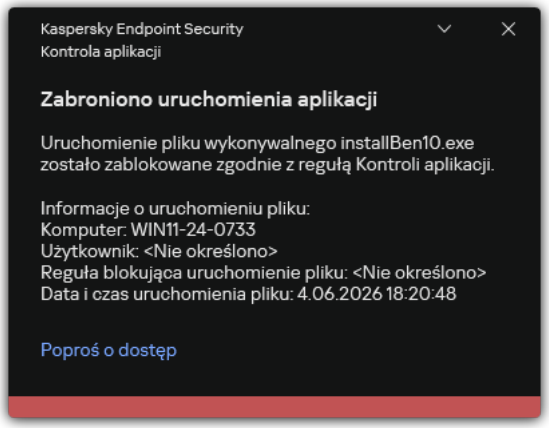
3. Wybieranie trybu Kontroli aplikacji.

   Administrator wybiera tryb pracy z aplikacjami, które nie są uwzględnione w żadnej z reguł (lista zablokowanych i lista zezwolonych).

Jeśli użytkownik spróbuje uruchomić niedozwoloną aplikację, Kaspersky Endpoint Security zablokuje uruchomienie aplikacji i wyświetli powiadomienie (patrz rysunek poniżej).

Tryb testowy służy do sprawdzania konfiguracji Kontroli aplikacji. W tym trybie Kaspersky Endpoint Security wykonuje następujące czynności:

- Umożliwia uruchamianie aplikacji, w tym zabronionych.
- Wyświetla powiadomienie o uruchomieniu zabronionej aplikacji i dodaje informacje do raportu na komputerze użytkownika.
- Wysyła dane o uruchomieniu zabronionych aplikacji do Kaspersky Security Center.



Powiadomienie Kontroli aplikacji

Tryby działania Kontroli aplikacji

Komponent Kontrola aplikacji działa w dwóch trybach:

- **Lista zablokowanych**. W tym trybie Kontrola aplikacji umożliwia użytkownikom uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji zabronionych w regułach Kontroli aplikacji.

  Ten tryb jest włączony domyślnie.

- **Lista zezwolonych**. W tym trybie Kontrola aplikacji blokuje użytkownikom możliwość uruchamiania dowolnych aplikacji, za wyjątkiem aplikacji, które są dozwolone i nie są zabronione w regułach Kontroli aplikacji.

  Jeżeli reguły zezwalające Kontroli aplikacji zostaną w pełni skonfigurowane, moduł zablokuje uruchamianie wszystkich nowych aplikacji, które nie zostały zweryfikowane przez administratora sieci LAN, natomiast zezwoli na działanie systemu operacyjnego i zaufanych aplikacji potrzebnych użytkownikom w ich pracy.

  Możesz przeczytać zalecenia odnośnie konfiguracji reguł Kontroli aplikacji w trybie listy zezwolonych.

Moduł Kontrola aplikacji można skonfigurować do pracy w tych trybach, korzystając z lokalnego interfejsu Kaspersky Endpoint Security oraz programu Kaspersky Security Center.

Jednakże Kaspersky Security Center oferuje narzędzia, które nie są dostępne w lokalnym interfejsie Kaspersky Endpoint Security, a które są potrzebne do:

- Tworzenia kategorii aplikacji.

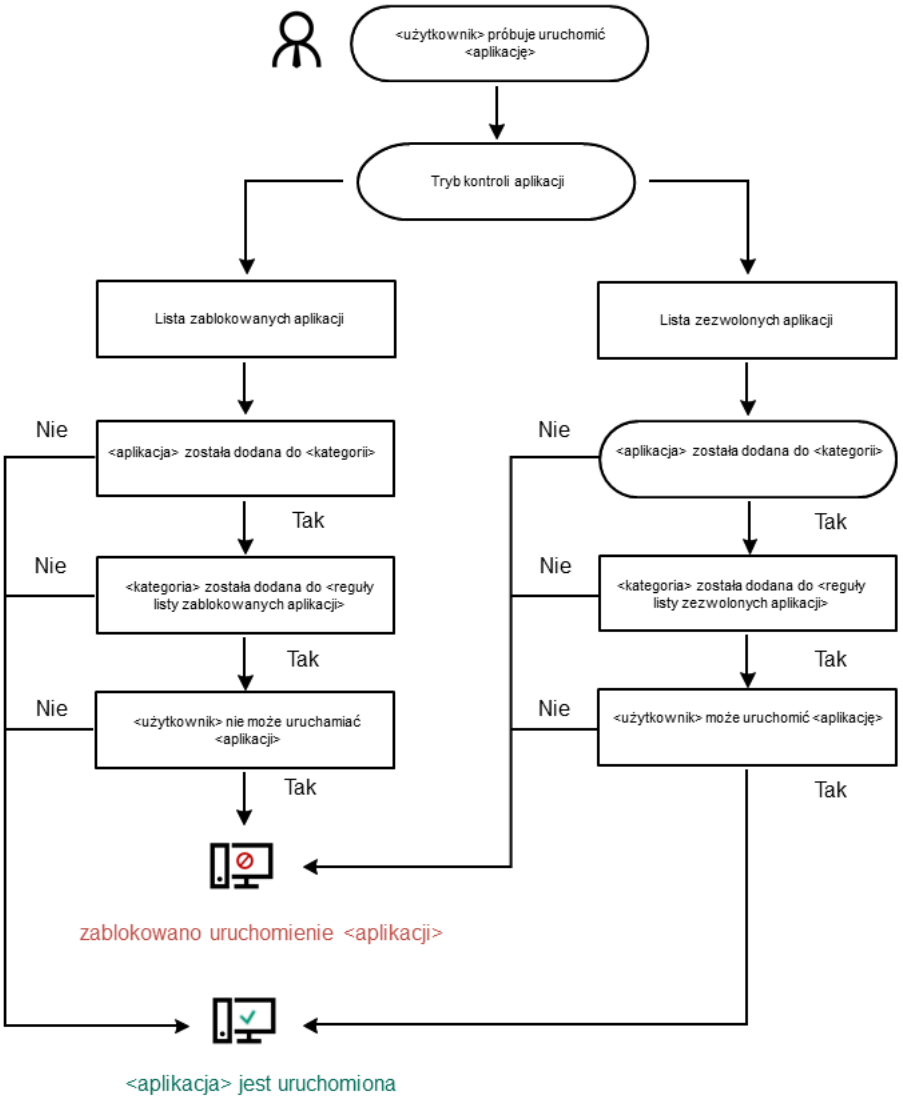
  Reguły Kontroli aplikacji utworzone w Konsoli administracyjnej Kaspersky Security Center są oparte o niestandardowe kategorie aplikacji, a nie o warunki włączenia i wykluczenia, jak ma to miejsce w przypadku lokalnego interfejsu Kaspersky Endpoint Security.

- Otrzymywania informacji o aplikacjach zainstalowanych na komputerach w korporacyjnej sieci LAN.

Dlatego zalecane jest korzystanie z Kaspersky Security Center podczas konfigurowania działania modułu Kontrola aplikacji.

Algorytm działania Kontroli aplikacji

Kaspersky Endpoint Security wykorzystuje algorytm do podjęcia decyzji o uruchomieniu aplikacji (patrz rysunek poniżej).



Algorytm działania Kontroli aplikacji

Parametr	Opis
Akcja wykonywana podczas uruchamiania aplikacji zablokowanych przez reguły	**Zastosuj reguły**. Kaspersky Endpoint Security zarządza uruchamianiem aplikacji w zależności od wybranego trybu. **Przetestuj reguły**. Kaspersky Endpoint Security zezwala na uruchomienie aplikacji, która jest blokowana w bieżącym trybie Kontroli aplikacji, ale zapisuje informacje o uruchomieniu aplikacji w raporcie.
Tryb Kontroli uruchamiania aplikacji	Możesz wybrać jedną z następujących opcji: • **Lista zablokowanych**. Jeśli ta opcja jest zaznaczona, Kontrola aplikacji zezwala wszystkim użytkownikom na uruchomienie dowolnej aplikacji, za wyjątkiem przypadków, gdy aplikacje spełniają warunki reguł blokowania Kontroli aplikacji. • **Lista zezwolonych**. Jeśli ta opcja jest zaznaczona, Kontrola aplikacji blokuje wszystkim użytkownikom możliwość uruchomienia jakiejkolwiek aplikacji, za wyjątkiem przypadków, gdy aplikacje spełniają warunki reguł zezwalających Kontroli aplikacji. Jeśli wybrany jest tryb **Lista zezwolonych**, automatycznie tworzone są dwie reguły Kontroli aplikacji: • **Obraz systemu**. • **Zaufane programy aktualizujące**. Nie możesz zmodyfikować ustawień ani usunąć automatycznie utworzonych reguł. Możesz włączyć lub wyłączyć te reguły.
Monitoruj ładowanie modułów DLL	Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security kontroluje wczytywanie modułów DLL, gdy użytkownicy próbują uruchomić aplikacje. Informacja na temat modułu DLL i aplikacji, która załadowała ten moduł DLL, jest zapisywana w raporcie. Po włączeniu funkcji kontrolowania wczytywania modułów DLL i sterowników, upewnij się, że w ustawieniach Kontroli aplikacji włączona jest jedna z następujących reguł: domyślna reguła **Obraz systemu** lub inna reguła, która zawiera kategorię KL „**Obraz systemu\Zaufane certyfikaty**" i zapewnia, że moduły DLL i sterowniki są ładowane przed uruchomieniem Kaspersky Endpoint Security. Włączanie kontroli ładowania modułów DLL i sterowników, gdy reguła **Obraz systemu** jest wyłączona, może spowodować niestabilność systemu operacyjnego. Kaspersky Endpoint Security monitoruje tylko moduły DLL i sterowniki ładowane po zaznaczeniu pola. Po zaznaczeniu pola zalecane jest ponowne uruchomienie komputera w celu zapewnienia, że aplikacja monitoruje wszystkie sterowniki i moduły DLL, w tym te załadowane przed uruchomieniem Kaspersky Endpoint Security.
Używaj ścisłej weryfikacji podpisem cyfrowym	Można wybrać certyfikat jako warunek wyzwalający regułę kontroli aplikacji. Jeśli to pole wyboru jest zaznaczone, Kaspersky Endpoint Security stosuje reguły do aplikacji podpisanych certyfikatami wyłącznie z zaufanych systemowych magazynów certyfikatów. Aplikacje podpisane takim certyfikatem są także uznawane za zaufane przez komponenty ochrony, na przykład zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Jeśli jednak w regule kontroli aplikacji określisz certyfikat z innego magazynu, Kaspersky Endpoint Security nie zastosuje takiej reguły. Jeśli pole wyboru nie jest zaznaczone, Kaspersky Endpoint Security stosuje reguły do aplikacji podpisanych certyfikatem z Głównego magazynu zaufanych certyfikatów systemu Windows. Takie aplikacje nie należą do strefy zaufanej. Komponenty ochrony monitorują aktywność takich aplikacji.
Szablony wiadomości o blokowaniu aplikacji	**Wiadomość dotycząca blokowania**. Szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła Kontroli aplikacji, która blokuje uruchamianie aplikacji. **Wiadomość do administratora**. Szablon wiadomości, którą użytkownik może wysłać do administratora korporacyjnej sieci LAN, jeśli uważa, że aplikacja została przypadkowo zablokowana. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania uruchomienia aplikacji**. Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkownika**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

Adaptacyjna kontrola anomalii

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Komponent Adaptacyjna kontrola anomalii monitoruje i blokuje działania, które nie są typowe dla komputerów w sieci firmowej. Adaptacyjna kontrola anomalii wykorzystuje zestaw reguł do śledzenia nietypowych zachowań (na przykład reguła *Uruchomienie procesora poleceń Microsoft Office z aplikacji biurowej*). Reguły są tworzone przez specjalistów z Kaspersky w oparciu o typowe scenariusze złośliwej aktywności. Można skonfigurować, w jaki sposób Adaptacyjna kontrola aplikacji obsługuje każdą regułę i, na przykład, zezwolić na wykonywanie skryptów PowerShell, które automatyzują określone zadania przepływu pracy. Kaspersky Endpoint Security aktualizuje zestaw reguł wraz z bazami danych aplikacji. Aktualizacje zestawów reguł muszą być potwierdzone ręcznie.

Ustawienia komponentu Adaptacyjna kontrola anomalii

Konfiguracja Adaptacyjnej kontroli anomalii składa się z następujących kroków:

1. Uczenie modułu Adaptacyjna kontrola anomalii.

   Po włączeniu Adaptacyjnej kontroli anomalii, jej reguły działają w *trybie uczenia*. Podczas uczenia moduł Adaptacyjna kontrola anomalii monitoruje wyzwalanie reguł i wysyła zdarzenia wyzwalające do Kaspersky Security Center. Każda reguła ma swój czas trwania trybu uczenia. Czas trwania trybu uczenia jest ustawiany przez ekspertów z Kaspersky. Zazwyczaj tryb uczenia jest aktywny przez dwa tygodnie.

   Jeśli podczas treningu reguła nie została w ogóle uruchomiona, Adaptacyjna kontrola anomalii uzna działania związane z tą regułą za nietypowe. Kaspersky Endpoint Security zablokuje wszystkie działania związane z tą regułą.

   Jeśli reguła została wyzwolona podczas treningu, Kaspersky Endpoint Security rejestruje zdarzenia w raporcie wyzwalającym regułę oraz w repozytorium **Wyzwalacze reguł w Trybie inteligentnego uczenia**.

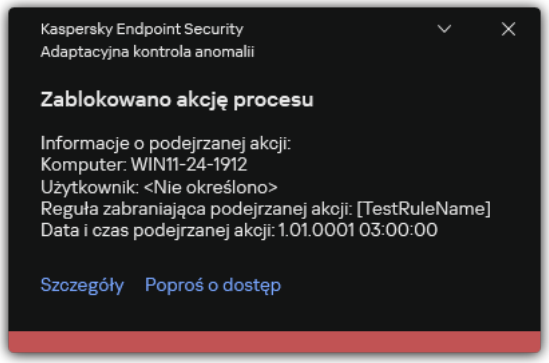
2. Analizowanie raportu dotyczącego wyzwalania reguły.

   Administrator analizuje raport wyzwalania reguł lub zawartość repozytorium **Wyzwalacze reguł w Trybie inteligentnego uczenia**. Następnie administrator może wybrać zachowanie Adaptacyjnej kontroli anomalii, gdy reguła jest wyzwalana: albo zablokować, albo zezwolić. Administrator może również kontynuować monitorowanie działania reguły i wydłużyć czas trwania trybu uczenia. Jeśli administrator nie podejmie żadnych działań, aplikacja będzie również kontynuować pracę w trybie uczenia. Czas trwania trybu uczenia zostanie zrestartowany.

Adaptacyjna kontrola anomalii jest konfigurowana w czasie rzeczywistym poprzez następujące kanały:

- Adaptacyjna kontrola anomalii automatycznie rozpoczyna blokowanie działań związanych z regułami, które nigdy nie zostały wyzwolone w trybie uczenia.
- Kaspersky Endpoint Security dodaje nowe reguły lub usuwa przestarzałe.
- Administrator konfiguruje działanie Adaptacyjnej kontroli anomalii po przejrzeniu raportu dotyczącego wyzwalania reguły i zawartości repozytorium **Wyzwalacze reguł w Trybie inteligentnego uczenia**. Zalecamy sprawdzenie raportu o wyzwalaniu reguł i zawartości magazynu **Wyzwalacze reguł w Trybie inteligentnego uczenia**.

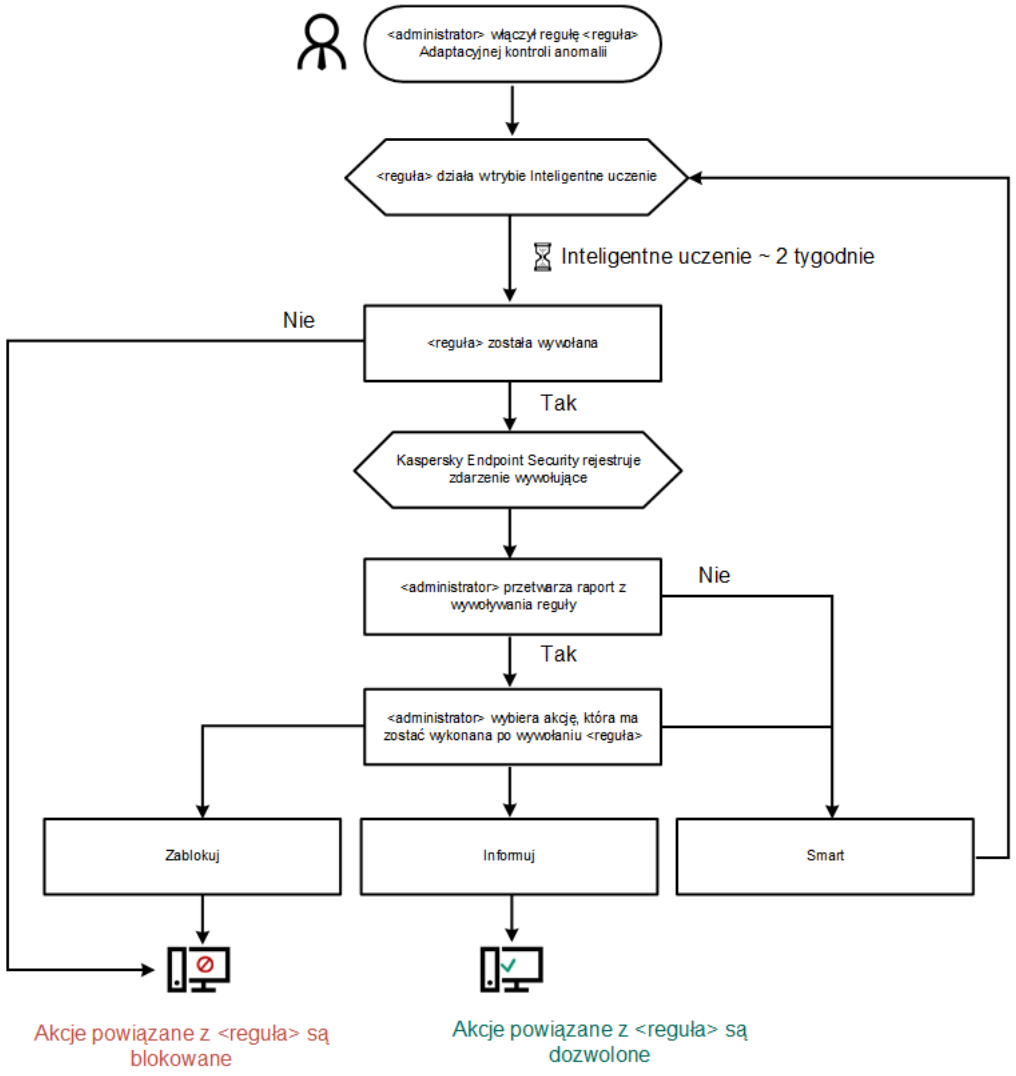
Jeśli złośliwa aplikacja spróbuje wykonać akcję, Kaspersky Endpoint Security zablokuje tę akcję i wyświetli powiadomienie (patrz rysunek poniżej).



Powiadomienie Adaptacyjnej kontroli anomalii

Algorytm działania Adaptacyjnej kontoli anomalii

Kaspersky Endpoint Security decyduje, czy zezwolić na lub zablokować działanie skojarzone z regułą opartą o następujący algorytm (patrz rysunek poniżej).



Algorytm działania Adaptacyjnej kontoli anomalii

Parametr	Opis
Raport o stanie reguł Adaptacyjnej kontroli anomalii *(dostępny tylko w Kaspersky Security Center Console)*	Ten raport zawiera informacje o stanie reguł wykrywania komponentu Adaptacyjna kontrola anomalii (na przykład: *Wyłączono* lub *Zablokuj*). Raport jest generowany dla wszystkich grup administracyjnych.
Raport o wywołanych regułach Adaptacyjnej kontroli anomalii *(dostępny tylko w Kaspersky Security Center Console)*	Ten raport zawiera informacje o nietypowych działaniach wykrytych przy użyciu komponentu Adaptacyjna kontrola anomalii. Raport jest generowany dla wszystkich grup administracyjnych.
Reguły	Tabela reguł komponentu Adaptacyjna kontrola anomalii. Reguły są tworzone przez specjalistów z Kaspersky w oparciu o typowe scenariusze złośliwej aktywności.
Szablony	**Wiadomość dotycząca blokowania**. Szablon komunikatu, który jest wyświetlany użytkownikowi po wyzwoleniu reguły komponentu Adaptacyjna kontrola anomalii, która blokuje nietypowe działanie. **Wiadomość do administratora**. Szablon wiadomości dla użytkownika, która może zostać wysłana do lokalnego administratora sieci korporacyjnej, jeśli użytkownik uzna, że zablokowanie jest pomyłką. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania aktywności aplikacji**. Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkownika**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

Monitor integralności systemu

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych.

Począwszy odd wersji 12.6 Kaspersky Endpoint Security for Windows zawiera komponent Monitorowanie integralności systemu zamiast komponentu Monitora integralności plików. Komponent Monitorowanie integralności systemu zawiera całą funkcjonalność Monitora integralności plików oraz dodatkowo pozwala na monitorowanie zmian w rejestrze i podłączania urządzeń zewnętrznych.

Monitorowanie integralności systemu monitoruje zmiany w systemie operacyjnym, które mogą wskazywać na naruszenia bezpieczeństwa komputera. Po wykryciu takich zmian Kaspersky Endpoint Security generuje odpowiednie zdarzenia i powiadamia administratora. Monitorowanie integralności systemu może działać w trybie czasu rzeczywistego i może również przeprowadzać sprawdzanie integralności systemu na żądanie.

Monitorowanie integralności systemu w czasie rzeczywistym

W trybie czasu rzeczywistego Monitor integralności systemu śledzi zmiany w obiektach, które włączono w zakres komponentu (*zakres monitorowania*). Monitorowanie integralności systemu umożliwia także blokowanie nieuprawnionego dostępu do takich obiektów w czasie rzeczywistym.

Sprawdzanie integralności systemu na żądanie

Sprawdzanie integralności systemu na żądanie to zadanie, które możesz uruchomić ręcznie lub zgodnie z harmonogramem. Aby uruchomić zadanie *Sprawdzanie integralności systemu*, musisz skonfigurować zakres komponentu (*zakres monitorowania*) i utworzyć punkt odniesienia. *Punkt odniesienia* to zarejestrowany status obiektów w systemie, który aplikacja wykorzystuje jako odniesienie przy porównywaniu ze stanem bieżącym.

Ustawienia Monitorowania integralności systemu

Parametr	Opis
Tryb działania reguł blokowania	• **Zablokuj**. W tym trybie Monitorowanie integralności systemu blokuje działania na plikach i kluczach rejestru z zakresu monitorowania oraz generuje odpowiadające temu zdarzenie. • **Poinformuj**. W tym trybie Monitorowanie integralności systemu zezwala na działania na plikach i kluczach rejestru z zakresu monitorowania oraz generuje odpowiadające temu zdarzenie.
Monitorowanie integralności systemu w czasie rzeczywistym	W trybie czasu rzeczywistego Monitor integralności systemu śledzi zmiany w obiektach, które włączono w zakres komponentu (*zakres monitorowania*). Monitorowanie integralności systemu umożliwia także blokowanie nieuprawnionego dostępu do takich obiektów w czasie rzeczywistym.
Monitoruj urządzenia	Monitorowanie integralności systemu monitoruje podłączanie i odłączanie urządzeń zewnętrznych.
Monitoruj pliki i rejestr	Monitorowanie integralności systemu monitoruje zmiany w plikach, folderach i rejestrze.
Sprawdzanie integralności systemu	Sprawdzanie integralności systemu na żądanie to zadanie, które możesz uruchomić ręcznie lub zgodnie z harmonogramem. Aby uruchomić zadanie *Sprawdzanie integralności systemu*, musisz skonfigurować zakres komponentu (*zakres monitorowania*) i utworzyć punkt odniesienia. *Punkt odniesienia* to zarejestrowany status obiektów w systemie, który aplikacja wykorzystuje jako odniesienie przy porównywaniu ze stanem bieżącym.

Endpoint Sensor

Endpoint Sensor nie jest zawarty w Kaspersky Endpoint Security 11.4.0.

Możesz zarządzać Endpoint Sensor w konsoli Kaspersky Security Center Web Console i Konsoli administracyjnej Kaspersky Security Center. Nie można zarządzać Endpoint Sensor w konsoli Kaspersky Security Center Cloud Console.

Endpoint Sensor to komponent zaprojektowany do interakcji z Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* to rozwiązanie zaprojektowane w celu szybkiego wykrywania złożonych zagrożeń, takich jak ataki ukierunkowane, zaawansowane trwałe zagrożenia (APT), ataki zero-day i inne. Kaspersky Anti Targeted Attack Platform składa się z trzech jednostek funkcjonalnych:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Można zakupić wszystkie jednostki funkcjonalne lub poszczególne jednostki funkcjonalne osobno. Szczegółowe informacje na temat rozwiązania można znaleźć w systemie pomocy dla Kaspersky Anti Targeted Attack Platform.

Zarządzanie Endpoint Sensor posiada następujące ograniczenia:

- Możesz skonfigurować ustawienia Endpoint Sensor w zasadzie, pod warunkiem że na komputerze jest zainstalowany Kaspersky Endpoint Security w wersji od 11.0.0 do 11.3.0. Aby uzyskać więcej informacji na temat konfigurowania ustawień Endpoint Sensor przy użyciu zasady, zapoznaj się z artykułami pomocy dotyczącymi poprzednich wersji Kaspersky Endpoint Security.

- Jeśli na komputerze jest zainstalowany program Kaspersky Endpoint Security w wersji 11.4.0 i nowszej, nie można skonfigurować ustawień Endpoint Sensor przy użyciu zasady.

Endpoint Sensor jest zainstalowany na komputerach klienckich. Na tych komputerach komponent ciągle monitoruje procesy, aktywne połączenia sieciowe oraz pliki, które są modyfikowane. Endpoint Sensor przekazuje informacje do serwera KATA.

Funkcjonalność komponentu jest dostępna w następujących systemach operacyjnych:

- Windows 7 Service Pack 1 Home / Professional / Enterprise;
- Windows 8.1.1 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2016 Essentials / Standard (64-bit).

Szczegółowe informacje na temat działania KATA można znaleźć w systemie pomocy dla Kaspersky Anti Targeted Attack Platform.

Sandbox

Kaspersky Endpoint Security for Windows zawiera wbudowanego agenta do integracji z rozwiązaniem Kaspersky Sandbox. Komponent *Sandbox* wykrywa i automatycznie blokuje zaawansowane zagrożenia na komputerach. Sandbox analizuje zachowanie obiektów w celu wykrywania szkodliwej aktywności oraz aktywności charakterystycznej dla ataków docelowych ukierunkowanych na infrastrukturę IT organizacji. Sandbox analizuje i skanuje obiekty na specjalnych serwerach z wdrożonymi obrazami wirtualnymi systemów operacyjnych Microsoft Windows (serwery Sandbox). Szczegółowe informacje na temat rozwiązania można znaleźć w systemie pomocy dla Kaspersky Sandbox i dla Kaspersky Anti Targeted Attack Platform.

Począwszy od wersji 12.7 Kaspersky Endpoint Security for Windows obsługuje komponent Sandbox wchodzący w skład rozwiązania Kaspersky Anti Targeted Attack Platform. W przeciwieństwie do rozwiązania Kaspersky Sandbox, komponent KATA Sandbox umożliwia skanowanie plików nie tylko automatycznie, ale również ręcznie z poziomu menu kontekstowego pliku.

Do wdrożenia komponentu KATA Sandbox wymagane jest rozwiązanie Kaspersky Anti Targeted Attack Platform w wersji 7.0 lub nowszej.

Komponent może być zarządzany tylko przy użyciu konsoli Kaspersky Security Center Web Console. Nie możesz zarządzać tym komponentem przy użyciu Konsoli administracyjnej (MMC).

Ustawienia komponentu Sandbox

Parametr	Opis
Tryb integracji	**Kaspersky Sandbox**. Integracja z rozwiązaniem Kaspersky Sandbox. Aplikacja wysyła pliki do skanowania w Kaspersky Sandbox wyłącznie w trybie automatycznym. **KATA Sandbox**. Integracja ze składnikiem Sandbox rozwiązania Kaspersky Anti Targeted Attack Platform. Możesz wybrać tryb przesyłania pliku do skanowania: • **Ręcznie**. Użytkownik ręcznie przesyła plik do skanowania z menu kontekstowego (**Wyślij do Sandbox**). • **Automatycznie**. Aplikacja automatycznie wykrywa obiekty i przesyła je do Sandboxa w celu zeskanowania. • **Powiązany**.
Ustawienia połączenia z serwerem	**Limit czasu (ms)**. Przekroczono limit czasu połączenia dla serwera Sandbox (dla komponentu Kaspersky Sandbox) lub serwera Central Node (dla komponentu KATA). Po skonfigurowaniu upłynięcia określonej ilości czasu, Kaspersky Endpoint Security wyśle żądanie do następnego serwera. Możesz zwiększyć limit czasu połączenia dla serwera, jeśli prędkość Twojego połączenia spada lub jeśli połączenie jest niestabilne. Zalecany limit czasu żądania wynosi 0,5 sekundy lub mniej. **Kolejka żądań**. Rozmiar folderu kolejki żądań. Podczas wysyłania kilku obiektów do skanowania w Sandbox Kaspersky Endpoint Security tworzy kolejkę żądań. Domyślnie, rozmiar folderu kolejki żądań jest ograniczony do 100 MB. Po osiągnięciu maksymalnego rozmiaru, Sandbox przestanie dodawać nowe żądania do kolejki i wyśle odpowiednie zdarzenie do Kaspersky Security Center. Możesz skonfigurować rozmiar folderu kolejki żądań w zależności od konfiguracji Twojego serwera. **Certyfikat TLS serwera**. Aby skonfigurować zaufane połączenie z serwerem Sandbox (dla komponentu Kaspersky Sandbox) lub serwerem Central Node (dla komponentu KATA), należy przygotować certyfikat TLS. Następnie należy dodać certyfikat do komputera, stosując zasady. Należy również dodać certyfikat do serwera Sandbox (dla komponentu Kaspersky Sandbox) lub serwera Central Node (dla komponentu KATA). **Zastosuj uwierzytelnianie dwukierunkowe** (tylko w przypadku KATA Sandbox). Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem Central Node. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera Central Node, a następnie uzyskać kontener szyfrowania i ustawić hasło chroniące kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform). Po skonfigurowaniu ustawień węzła centralnego należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny.
Połączenie z serwerami Sandbox	**Kaspersky Sandbox**. Ustawienia połączenia z serwerem Sandbox. Serwery używają wdrożonych obrazów wirtualnych systemów operacyjnych Microsoft Windows do uruchamiania obiektów, które muszą zostać przeskanowane. Możesz wprowadzić adres IP (IPv4 lub IPv6) lub w pełni kwalifikowaną nazwę domeny. **KATA Sandbox**. Ustawienia połączenia z serwerem Central Node. Central Node wybiera optymalne ustawienia skanowania i równoważy obciążenie pomiędzy serwerami Sandbox.
Działanie po wykryciu zagrożenia	**Przenieś kopię do Kwarantanny, usuń obiekt**. Jeśli ta opcja została zaznaczona, Kaspersky Endpoint Security usunie szkodliwy obiekt wykryty na komputerze. Przed usunięciem obiektu Kaspersky Endpoint Security utworzy kopię zapasową w przypadku, gdy obiekt musi zostać przywrócony w późniejszym czasie. Kaspersky Endpoint Security przeniesie kopię zapasową do Kwarantanny. **Uruchom skanowanie obszarów krytycznych**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security uruchamia zadanie *Skanowanie obszarów krytycznych*. Domyślnie, Kaspersky Endpoint Security skanuje pamięć jądra, uruchomione procesy i sektory startowe dysku. **Utwórz zadanie skanowania IOC**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security automatycznie tworzy zadanie *Skanowanie IOC (autonomiczne zadanie skanowania IOC)*. Dla tego zadania możesz skonfigurować tryb uruchamiania, obszar skanowania oraz akcję po wykryciu IOC (*Przenieś kopię do Kwarantanny, usuń obiekt* lub *Uruchom skanowanie obszarów krytycznych*). Aby zmodyfikować inne ustawienia zadania *Skanowanie IOC*, przejdź do ustawień zadania.
Zakres skanowania IOC	**Krytyczne obszary plików**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security wykonuje skanowanie IOC tylko w krytycznych obszarach plików komputera: pamięci jądra i sektorów startowych. **Obszary plików na dysku systemowym komputera**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security nie skanuje IOC na dysku systemowym komputera.

Parametr	Opis
Uruchom zadanie skanowania IOC	**Ręcznie**. Tryb uruchamiania, w którym możesz ręcznie uruchomić zadanie *Skanowanie IOC* w wygodnym dla siebie momencie. **Automatycznie**. Tryb uruchamiania, w którym Kaspersky Endpoint Security automatycznie uruchamia zadanie *Skanowanie IOC* po wykryciu zagrożenia. **Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności**. Tryb uruchamiania, w którym Kaspersky Endpoint Security uruchomi zadanie *Skanowanie IOC*, jeśli wygaszacz ekranu jest aktywny lub ekran jest zablokowany. Jeśli użytkownik odblokuje komputer, Kaspersky Endpoint Security wstrzyma zadanie. To oznacza, że wykonanie zadania może zająć kilka dni.

Managed Detection and Response

Kaspersky Endpoint Security for Windows obsługuje integrację z rozwiązaniem Managed Detection and Response. Rozwiązanie *Kaspersky Managed Detection and Response (MDR)* automatycznie wykrywa i analizuje incydenty naruszenia bezpieczeństwa w Twojej infrastrukturze. W tym celu MDR używa danych telemetrycznych, otrzymanych z punktów końcowych i uczenia maszynowego. MDR wysyła dane incydentu do ekspertów z Kaspersky. Eksperci mogą następnie przetworzyć incydent i, na przykład, dodać nowy wpis do antywirusowych baz danych. Zamiast tego eksperci mogą opublikować zalecenia odnośnie przetwarzania incydentu i, na przykład, zasugerować odizolowanie komputera od sieci. Szczegółowe informacje dotyczące sposobu działania rozwiązania można znaleźć w pomocy do Kaspersky Managed Detection and Response.

Ustawienia Managed Detection and Response

Parametr	Opis
Plik konfiguracyjny MDR	Plik BLOB zawiera ID klienta oraz informacje o licencji dla Kaspersky Managed Detection and Response. Plik BLOB znajduje się w archiwum ZIP pliku konfiguracyjnego MDR. Archiwum ZIP możesz uzyskać w Kaspersky Managed Detection and Response Console. Więcej informacji o pliku BLOB można znaleźć w pomocy dla Kaspersky Managed Detection and Response.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows zawiera wbudowanego agenta dla rozwiązania Kaspersky Endpoint Detection and Response Optimum (zwanego dalej również „EDR Optimum"). Począwszy od wersji 11.8.0 Kaspersky Endpoint Security for Windows zawiera wbudowanego agenta dla rozwiązania Kaspersky Endpoint Detection and Response Expert (zwanego dalej również „EDR Expert"). *Kaspersky Endpoint Detection and Response* to szereg rozwiązań do ochrony infrastruktury IT korporacji przed zaawansowanymi cyberzagrożeniami. Funkcjonalność rozwiązań łączy automatyczne wykrywanie zagrożeń z możliwością reagowania na te zagrożenia w celu przeciwdziałania zaawansowanym atakom, w tym nowym exploitom, oprogramowaniu ransomware, atakom bezplikowym, a także metodom z użyciem legalnych narzędzi systemowych. EDR Expert oferuje więcej funkcji monitorowania zagrożeń i reakcji na nie niż EDR Optimum. Więcej informacji o rozwiązaniach można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Optimum oraz w pomocy do Kaspersky Endpoint Detection and Response Expert.

Kaspersky Endpoint Detection and Response monitoruje i analizuje rozwój zagrożeń i zapewnia *personel ds. bezpieczeństwa* lub *Administratora* z informacjami o potencjalnym ataku, które są niezbędne do reagowania w odpowiednim momencie. Kaspersky Endpoint Detection and Response wyświetla szczegóły wykrycia w oddzielnym oknie. *Wykrycie* to zdarzenie w korporacyjnej infrastrukturze IT, które aplikacja zidentyfikowała jako nietypowe lub podejrzane i które może stanowić zagrożenie dla bezpieczeństwa korporacyjnej infrastruktury IT. *Szczegóły wykrycia* to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Optimum oraz w pomocy do Kaspersky Endpoint Detection and Response Expert.

Możesz skonfigurować komponent Endpoint Detection and Response Optimum w Web Console i Cloud Console. Ustawienia tego komponentu Endpoint Detection and Response Expert (cloud) są dostępne tylko w Cloud Console.

Ustawienia Endpoint Detection and Response

Parametr	Opis
Włącz zaawansowane rejestrowanie aktywności systemu	Rozszerzona telemetria poprawia dokładność wykrywania IOC, ale wykorzystuje więcej zasobów komputera. Zalecamy włączenie rozszerzonej telemetrii na komputerze w celu retrospektywnego skanowania IOC. *Retrospektywne skanowanie IOC* jest trybem zadania *Skanowanie IOC*, w ramach którego Kaspersky Endpoint Security skanuje dane w poszukiwaniu oznak naruszenia bezpieczeństwa przez określony czas. Tryb ten jest przeznaczony do wyszukiwania wskaźników zagrożenia na podstawie danych telemetrycznych chronionego komputera, takich jak aktywność sieciowa, procesy, pliki i inne dane telemetryczne. Jeśli rozszerzona telemetria jest wyłączona, Kaspersky Endpoint Security może wymieniać informacje o wykrytych wskaźnikach naruszeń bezpieczeństwa.
Izolacja od sieci	Automatyczna izolacja komputera od sieci w odpowiedzi na wykryte zagrożenia. Jeśli izolacja sieci jest włączona, aplikacja zrywa wszystkie aktywne połączenia i blokuje wszystkie nowe połączenia TCP/IP na komputerze. Aplikacja pozostawia aktywne tylko następujące połączenia: • Połączenia znajdujące się w wykluczeniach Izolacji sieci. • Połączenia zainicjowane przez usługi Kaspersky Endpoint Security. • Połączenia zainicjowane przez agenta sieciowego Kaspersky Security Center.
Automatycznie odblokuj izolowane urządzenie za (godz.)	Izolacja sieci może zostać wyłączona automatycznie po określonym czasie lub ręcznie. Domyślnie, Kaspersky Endpoint Security wyłączy Izolację sieci 5 godzin od rozpoczęcia izolacji.
Wykluczenia izolacji od sieci	Lista reguł dla wykluczeń z izolacji sieci. Połączenia sieciowe, które odpowiadają regułom, nie są blokowane na komputerach, gdy Izolacja sieci jest włączona. Aby skonfigurować wykluczenia izolacji sieci, możesz użyć listy *standardowych profili sieciowych*. Domyślnie, wykluczenia obejmują profile sieciowe zawierające reguły, które zapewniają nieprzerwane działanie urządzeń z rolami serwera DNS/DHCP i klienta DNS/DHCP. Możesz także ręcznie zmodyfikować ustawienia standardowych profili sieciowych lub zdefiniować wykluczenia. Wykluczenia określone we właściwościach zasady są stosowane tylko wtedy, gdy Izolacja sieci zostaje włączona automatycznie w odpowiedzi na wykryte zagrożenie. Wykluczenia określone we właściwościach komputera są stosowane tylko wtedy, gdy Izolacja od sieci zostanie włączona ręcznie we właściwościach komputera w konsoli Kaspersky Security Center lub w szczegółach alertu.
Zapobieganie wykonywaniu	Kontrola wykonania plików wykonywalnych i skryptów oraz otwarcia plików formatów office. Na przykład, możesz zapobiec wykonaniu aplikacji, które są uznawane za niezabezpieczone na wybranym komputerze. Zapobieganie wykonywaniu obsługuje zestaw rozszerzeń plików pakietu office oraz zestaw interpreterów skryptu. Aby korzystać z komponentu Zapobieganie wykonywaniu, należy dodać reguły zapobiegania wykonywaniu. *Reguły zapobiegania wykonywaniu* to zestaw kryteriów, które aplikacja bierze pod uwagę podczas reagowania na wykonanie obiektu, na przykład, podczas blokowania wykonania obiektu. Aplikacja identyfikuje pliki według ich ścieżek lub sum kontrolnych wyliczonych przy użyciu algorytmów haszowania MD5 i SHA256.

Parametr	Opis
Akcja podczas wykonywania lub otwierania zabronionego obiektu	**Zablokuj i dodaj do dziennika zdarzeń**. W tym trybie aplikacja blokuje wykonanie obiektów lub otwieranie dokumentów, które odpowiadają kryteriom reguły blokowania. Aplikacja publikuje także zdarzenie dotyczące prób wykonania obiektów lub otwarcia dokumentów w Dzienniku zdarzeń Windows oraz dzienniku zdarzeń Kaspersky Security Center. **Dodaj do dziennika zdarzeń**. W tym trybie Kaspersky Endpoint Security publikuje zdarzenie dotyczące prób uruchomienia obiektów wykonywalnych lub otwarcia dokumentów, które odpowiadają kryteriom reguły blokowania, w Dzienniku zdarzeń Windows oraz w Kaspersky Security Center, ale nie blokują próby uruchomienia lub otwarcia obiektu lub dokumentu. Ten tryb jest wybrany domyślnie.
Reguły zapobiegania wykonywaniu	*Reguły zapobiegania wykonywaniu* to zestaw kryteriów, które aplikacja bierze pod uwagę podczas reagowania na wykonanie obiektu, na przykład, podczas blokowania wykonania obiektu. Aplikacja identyfikuje pliki według ich ścieżek lub sum kontrolnych wyliczonych przy użyciu algorytmów haszowania MD5 i SHA256.
Cloud Sandbox	*Cloud Sandbox* to technologia pozwalająca na wykrywanie zaawansowanych zagrożeń na komputerze. Kaspersky Endpoint Security automatycznie przesyła usunięte pliki do Cloud Sandbox w celu ich przeanalizowania. Cloud Sandbox uruchamia te pliki w odizolowanym środowisku, aby zidentyfikować złośliwą aktywność i zdecydować o ich reputacji. Dane z tych plików są następnie wysyłane do Kaspersky Security Network. Dlatego też, jeżeli Cloud Sandbox wykrył szkodliwy plik, Kaspersky Endpoint Security wykona odpowiednią akcję w celu wyeliminowania tego zagrożenia na wszystkich komputerach, na których ten plik został wykryty. Technologia Cloud Sandbox jest stale włączona i jest dostępna dla wszystkich użytkowników Kaspersky Security Network, niezależnie od typu licencji, z której korzystają. Jeżeli to pole wyboru jest zaznaczone, Kaspersky Endpoint Security włączy licznik dla zagrożeń wykrytych przy użyciu Cloud Sandbox w głównym oknie aplikacji pod **Technologie wykrywania zagrożeń**. Kaspersky Endpoint Security będzie również wskazywał technologię wykrywania zagrożeń Cloud Sandbox w zdarzeniach aplikacji oraz w *Raport o zagrożeniach* w konsoli Kaspersky Security Center.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security for Windows obsługuje integrację z rozwiązaniem Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* to korporacyjne rozwiązanie z zakresu bezpieczeństwa cybernetycznego obejmujące aplikacje Kaspersky, które umożliwiają organizacji obronę przed większością typów zagrożeń cybernetycznych i obejmują najważniejsze scenariusze rozprzestrzeniania się zagrożeń. Komponenty EDR Expert (on-premises) są wdrażane na platformie OSMP (Open Single Management Platform). Platforma ta obsługuje scenariusze wieloplatformowe w ramach jednego interfejsu i umożliwia integrację aplikacji Kaspersky z aplikacjami innych firm w ramach jednego kompleksowego systemu bezpieczeństwa.

Jednym z centralnych elementów rozwiązania jest *SIEM*. SIEM śledzi zdarzenia pochodzące ze wszystkich komponentów i koreluje je ze sobą, wykorzystując reguły zdefiniowane przez dostawcę i użytkownika. Rozwiązanie EDR Expert (on-premises) analizuje logi i dane telemetryczne otrzymane z infrastruktury korporacyjnej w celu automatycznego wykrywania ataków i umożliwia badanie incydentów przy użyciu ujednoliconego wykresu dochodzeniowego, który łączy wszystkie zdarzenia zebrane w rozwiązaniu EDR Expert (on-premises), w tym zdarzenia z aplikacji firmy Kaspersky i produktów zabezpieczających informacje innych firm.

W przypadku zaawansowanych incydentów rozwiązanie EDR Expert (on-premises) wykorzystuje scenariusze wstępnie ustawione i zdefiniowane przez użytkownika. Można również wykorzystać akcje reagowania z aplikacji innych firm i scenariusze reagowania obejmujące wiele aplikacji.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security for Windows obsługuje zarządzanie komponentem Kaspersky Endpoint Detection and Response w ramach rozwiązania Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* to rozwiązanie zaprojektowane w celu szybkiego wykrywania złożonych zagrożeń, takich jak ataki ukierunkowane, zaawansowane trwałe zagrożenia (APT), ataki zero-day i inne. Kaspersky Anti Targeted Attack Platform składa się z trzech jednostek funkcjonalnych:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Można zakupić wszystkie jednostki funkcjonalne lub poszczególne jednostki funkcjonalne osobno. Szczegółowe informacje na temat rozwiązania można znaleźć w systemie pomocy dla Kaspersky Anti Targeted Attack Platform.

Aplikacja Kaspersky Endpoint Security jest instalowana na pojedynczych komputerach w korporacyjnej infrastrukturze IT i cały czas monitoruje procesy, otwiera połączenia sieciowe i modyfikowane pliki. Informacje o zdarzeniach na komputerze (dane telemetryczne) są wysyłane na serwer Kaspersky Anti Targeted Attack Platform. W takim przypadku Kaspersky Endpoint Security wysyła również informacje do serwera Kaspersky Anti Targeted Attack Platform o zagrożeniach wykrytych przez aplikację oraz informacje o wynikach przetwarzania tych zagrożeń.

Integracja EDR (KATA) i NDR (KATA) jest konfigurowana na konsoli Kaspersky Security Center. Wbudowany agent jest następnie zarządzany przy użyciu konsoli Kaspersky Anti Targeted Attack Platform, w tym uruchamianie zadań, zarządzanie obiektami poddanymi kwarantannie, przeglądanie raportów i inne działania.

Ustawienia Endpoint Detection and Response Expert (on-premises)

Parametr	Opis
Połączenie z serwerami gromadzenia danych telemetrycznych	*Serwer gromadzenia danych telemetrycznych* jest serwerem stanowiącym część rozwiązania SIEM, które zbiera, normalizuje, koreluje, analizuje i przechowuje informacje o zdarzeniach mających miejsce na komputerze. Skonfiguruj poniższe elementy, aby nawiązać połączenie z serwerami gromadzącymi dane telemetryczne (KUMA): • **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem. • **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem. Certyfikat TLS można uzyskać na platformie Open Single Management Platform (instrukcje można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera, a następnie uzyskać kontener kryptograficzny i ustawić hasło chroniące kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać na platformie Open Single Management Platform (instrukcje znajdują się w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)). Po skonfigurowaniu ustawień serwera należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener szyfrowania. Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.
Adres i **Port** (serwery zbierające dane telemetryczne)	Ustawienia połączeń z serwerami gromadzenia danych telemetrycznych. Możesz wprowadzić adres IP (IPv4 lub IPv6). Można dodać wiele adresów serwerów gromadzących dane telemetryczne. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.

Parametr	Opis
Wyślij dane telemetryczne do serwerów gromadzenia danych telemetrycznych	Ta funkcja pozwala całkowicie wyłączyć przesyłanie danych telemetrycznych do serwera KATA. Na przykład, jeśli używasz Kaspersky Anti Targeted Attack Platform wraz z innym rozwiązaniem, które również wykorzystuje telemetrię, możesz wyłączyć wysyłanie telemetrii dla KATA (EDR). Pozwala to zoptymalizować obciążenie serwera dla tych rozwiązań. Jeśli masz wdrożone rozwiązanie Managed Detection and Response i KATA (EDR), możesz użyć telemetrii MDR i utworzyć zadania Threat Response w KATA (EDR). • **Wysyłaj telemetrię tylko za pomocą wskaźnika IOA**. Umożliwia to optymalizację telemetrii i wysyłanie wyłącznie danych telemetrycznych za pomocą IOA. *Wskaźnik ataku (IOA)* jest regułą zawierającą opis podejrzanego zachowania w systemie, które może wskazywać na ukierunkowany atak. Aplikacja porównuje bieżące zachowanie systemu z tymi regułami i rejestruje zdarzenia wskazujące na ukierunkowany atak. Aplikacja wykorzystuje technologię *skanowania strumieniowego* umożliwiającą śledzenie takich zdarzeń w czasie rzeczywistym. • **Maksymalne opóźnienie transmisji zdarzeń (s)**. Aplikacja synchronizuje się z serwerem w celu wysyłania zdarzeń po wygaśnięciu przedziału synchronizacji. Domyślnie ustawienie to 30 sekund. • **Ogranicz liczbę pakietów zdarzeń na transmisję**. Aplikacja synchronizuje się z serwerem, gdy bufor zostanie zapełniony zdarzeniami. Domyślnie ustawienie to 1024 zdarzenia. Funkcja ta umożliwia wyłączenie buforowania zdarzeń przed synchronizacją z serwerem.
Włącz ograniczanie żądań	Ta funkcja pomaga zoptymalizować obciążenie serwera. Jeśli ta funkcja jest włączona, aplikacja ogranicza przesyłanie zdarzeń. Jeśli liczba zdarzeń przekroczy skonfigurowane limity, Kaspersky Endpoint Security przestanie wysyłać zdarzenia. Skonfiguruj ustawienia telemetrii: • **Maksymalna liczba zdarzeń na godzinę**. Aplikacja analizuje strumień danych telemetrycznych i ogranicza wysyłanie zdarzeń, jeśli strumień zdarzeń przekroczy skonfigurowany limit zdarzeń na godzinę. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń po godzinie. Ustawienie domyślne to 3000 zdarzeń na godzinę. Jeżeli aplikacja jest zainstalowana na serwerze, strumień danych telemetrycznych jest większy. W przypadku serwerów zaleca się zwiększenie wartości do 60 000 zdarzeń na godzinę. • **Procent przekroczenia limitu zdarzeń**. Aplikacja sortuje zdarzenia według typu (np. zdarzenia „zmiany w rejestrze") i ogranicza transmisję zdarzeń, jeśli stosunek zdarzeń tego samego typu do całkowitej liczby zdarzeń przekroczy skonfigurowany limit w procentach. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń, gdy stosunek innych zdarzeń do łącznej liczby zdarzeń ponownie stanie się wystarczająco duży. Ustawienie domyślne to 15%.
Wysyłaj żądanie synchronizacji do serwera co (min)	Częstotliwość żądań synchronizacji wysyłanych do serwera. Podczas synchronizacji Kaspersky Endpoint Security wysyła informacje o zmodyfikowanych ustawieniach i zadaniach aplikacji.
Połączenie z serwerami odpowiedzi	*Serwer odpowiedzi* jest serwerem służącym do odbierania i skanowania danych, badania zachowań obiektów i publikowania wyników tych badań. Skonfiguruj następujące elementy dla połączenia z serwerami odpowiedzi: • **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem. • **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem. Certyfikat TLS można uzyskać na platformie Open Single Management Platform (instrukcje można znaleźć w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera, a następnie uzyskać kontener kryptograficzny i ustawić hasło chroniące kontener kryptograficzny. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać na platformie Open Single Management Platform (instrukcje znajdują się w pomocy do Kaspersky Endpoint Detection and Response Expert (on-premises)). Po skonfigurowaniu ustawień serwera należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener szyfrowania.
Adres i **Port** (serwery odpowiedzi)	Ustawienia połączeń z serwerami odpowiedzi. Możesz wprowadzić adres IP (IPv4 lub IPv6). Można dodać wiele adresów serwerów gromadzących dane telemetryczne. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.

Parametr	Opis
Wysyłaj żądanie synchronizacji do serwera co (min)	Częstotliwość żądań synchronizacji wysyłanych do serwera. Podczas synchronizacji Kaspersky Endpoint Security wysyła informacje o zmodyfikowanych ustawieniach i zadaniach aplikacji.
Połączenie z serwerami KATA	Skonfiguruj następujące elementy dla połączenia z serwerem Central Node: • **Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera węzła centralnego. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem węzła centralnego. • **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem Central Node. Możesz uzyskać certyfikat TLS w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w Pomoc Kaspersky Anti Targeted Attack Platform). • **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem Central Node. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera Central Node, a następnie uzyskać kontener szyfrowania i ustawić hasło chroniące kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform). Po skonfigurowaniu ustawień węzła centralnego należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny. Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.
Adres i **Port** (serwery KATA)	Ustawienia połączeń z serwerami Kaspersky Anti Targeted Attack Platform. Aby nawiązać połączenie, wprowadź adres IP (IPv4 lub IPv6) i port serwera Central Node. Można dodać wiele adresów serwera węzła centralnego. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.
Wyślij dane telemetryczne do KATA	Ta funkcja pozwala całkowicie wyłączyć przesyłanie danych telemetrycznych do serwera KATA. Na przykład, jeśli używasz Kaspersky Anti Targeted Attack Platform wraz z innym rozwiązaniem, które również wykorzystuje telemetrię, możesz wyłączyć wysyłanie telemetrii dla KATA (EDR). Pozwala to zoptymalizować obciążenie serwera dla tych rozwiązań. Jeśli masz wdrożone rozwiązanie Managed Detection and Response i KATA (EDR), możesz użyć telemetrii MDR i utworzyć zadania Threat Response w KATA (EDR). Skonfiguruj ustawienia telemetrii: • **Maksymalne opóźnienie transmisji zdarzeń (s)**. Aplikacja synchronizuje się z serwerem w celu wysyłania zdarzeń po wygaśnięciu przedziału synchronizacji. Domyślnie ustawienie to 30 sekund. • **Maksymalna liczba pakietów zdarzeń**. Aplikacja synchronizuje się z serwerem, gdy bufor zostanie zapełniony zdarzeniami. Domyślnie ustawienie to 1024 zdarzenia.
Włącz ograniczanie żądań	Ta funkcja pomaga zoptymalizować obciążenie serwera. Jeśli ta funkcja jest włączona, aplikacja ogranicza przesyłanie zdarzeń. Jeśli liczba zdarzeń przekroczy skonfigurowane limity, Kaspersky Endpoint Security przestanie wysyłać zdarzenia. Skonfiguruj ustawienia telemetrii: • **Maksymalna liczba zdarzeń na godzinę**. Aplikacja analizuje strumień danych telemetrycznych i ogranicza wysyłanie zdarzeń, jeśli strumień zdarzeń przekroczy skonfigurowany limit zdarzeń na godzinę. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń po godzinie. Ustawienie domyślne to 3000 zdarzeń na godzinę. Jeżeli aplikacja jest zainstalowana na serwerze, strumień danych telemetrycznych jest większy. W przypadku serwerów zaleca się zwiększenie wartości do 60 000 zdarzeń na godzinę. • **Procent przekroczenia limitu zdarzeń**. Aplikacja sortuje zdarzenia według typu (np. zdarzenia „zmiany w rejestrze") i ogranicza transmisję zdarzeń, jeśli stosunek zdarzeń tego samego typu do całkowitej liczby zdarzeń przekroczy skonfigurowany limit w procentach. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń, gdy stosunek innych zdarzeń do łącznej liczby zdarzeń ponownie stanie się wystarczająco duży. Ustawienie domyślne to 15%.

Network Detection and Response (KATA)

Kaspersky Endpoint Security for Windows obsługuje zarządzanie komponentem Kaspersky Network Detection and Response w ramach rozwiązania Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* to rozwiązanie zaprojektowane w celu szybkiego wykrywania złożonych zagrożeń, takich jak ataki ukierunkowane, zaawansowane trwałe zagrożenia (APT), ataki zero-day i inne. Kaspersky Anti Targeted Attack Platform składa się z trzech jednostek funkcjonalnych:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Można zakupić wszystkie jednostki funkcjonalne lub poszczególne jednostki funkcjonalne osobno. Szczegółowe informacje na temat rozwiązania można znaleźć w systemie pomocy dla Kaspersky Anti Targeted Attack Platform.

Aplikacja Kaspersky Endpoint Security jest instalowana na pojedynczych komputerach w korporacyjnej infrastrukturze IT i cały czas monitoruje procesy, otwiera połączenia sieciowe i modyfikowane pliki. Informacje o zdarzeniach na komputerze (dane telemetryczne) są wysyłane na serwer Kaspersky Anti Targeted Attack Platform. W takim przypadku Kaspersky Endpoint Security wysyła również informacje do serwera Kaspersky Anti Targeted Attack Platform o zagrożeniach wykrytych przez aplikację oraz informacje o wynikach przetwarzania tych zagrożeń.

Integracja EDR (KATA) i NDR (KATA) jest konfigurowana na konsoli Kaspersky Security Center. Wbudowany agent jest następnie zarządzany przy użyciu konsoli Kaspersky Anti Targeted Attack Platform, w tym uruchamianie zadań, zarządzanie obiektami poddanymi kwarantannie, przeglądanie raportów i inne działania.

Parametry Network Detection and Response (KATA)

Parametr	Opis
Ustawienia połączenia z serwerem	**Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera węzła centralnego. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem węzła centralnego. **Certyfikat TLS serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem Central Node. Możesz uzyskać certyfikat TLS w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w Pomoc Kaspersky Anti Targeted Attack Platform). **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a serwerem Central Node. Aby korzystać z uwierzytelniania dwukierunkowego, musisz włączyć uwierzytelnianie dwukierunkowe w ustawieniach serwera Central Node, a następnie uzyskać kontener szyfrowania i ustawić hasło chroniące kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Kontener kryptograficzny można uzyskać w konsoli Kaspersky Anti Targeted Attack Platform (zobacz instrukcje w pliku Pomoc Kaspersky Anti Targeted Attack Platform). Po skonfigurowaniu ustawień węzła centralnego należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny. Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.
Adres i **Port**	Ustawienia połączeń z serwerami Kaspersky Anti Targeted Attack Platform. Aby nawiązać połączenie, wprowadź adres IP (IPv4 lub IPv6) i port serwera Central Node. Można dodać wiele adresów serwera węzła centralnego. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.
Wysyłaj żądanie synchronizacji do serwera NDR co (min)	Częstotliwość żądań synchronizacji wysyłanych do serwera. Podczas synchronizacji Kaspersky Endpoint Security wysyła informacje o zmodyfikowanych ustawieniach i zadaniach aplikacji.

Parametr	Opis
Maksymalne opóźnienie transmisji zdarzeń (s)	Aplikacja synchronizuje się z serwerem w celu wysyłania zdarzeń po wygaśnięciu przedziału synchronizacji. Domyślnie ustawienie to 30 sekund.
Włącz ograniczanie żądań	Ta funkcja pomaga zoptymalizować obciążenie serwera. Jeśli ta funkcja jest włączona, aplikacja ogranicza przesyłanie zdarzeń. Jeśli liczba zdarzeń przekroczy skonfigurowane limity, Kaspersky Endpoint Security przestanie wysyłać zdarzenia.
Maksymalna liczba zdarzeń na godzinę	Aplikacja analizuje strumień danych telemetrycznych i ogranicza wysyłanie zdarzeń, jeśli strumień zdarzeń przekroczy skonfigurowany limit zdarzeń na godzinę. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń po godzinie. Ustawienie domyślne to 3000 zdarzeń na godzinę. Jeżeli aplikacja jest zainstalowana na serwerze, strumień danych telemetrycznych jest większy. W przypadku serwerów zaleca się zwiększenie wartości do 60 000 zdarzeń na godzinę.
Procent przekroczenia limitu zdarzeń	Aplikacja sortuje zdarzenia według typu (np. zdarzenia „zmiany w rejestrze") i ogranicza transmisję zdarzeń, jeśli stosunek zdarzeń tego samego typu do całkowitej liczby zdarzeń przekroczy skonfigurowany limit w procentach. Kaspersky Endpoint Security wznawia wysyłanie zdarzeń, gdy stosunek innych zdarzeń do łącznej liczby zdarzeń ponownie stanie się wystarczająco duży. Ustawienie domyślne to 15%.

Integracja z KUMA

Kaspersky Endpoint Security for Windows obsługuje rozwiązanie Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* to rozwiązanie do zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa (SIEM) dla infrastruktury IT organizacji. Platforma KUMA umożliwia wykrywanie, analizowanie i łagodzenie zagrożeń bezpieczeństwa, zanim wyrządzą szkodę.

Ustawienia integracji KUMA

Parametr	Opis
Maksymalne opóźnienie przy wysyłaniu zdarzeń (sek.)	Aplikacja synchronizuje się z serwerem w celu wysyłania zdarzeń po wygaśnięciu przedziału synchronizacji. Domyślnie ustawienie to 30 sekund.
Połączenie z serwerami KUMA	**Limit czasu (sek)**. Maksymalny limit czasu odpowiedzi serwera KUMA. Po przekroczeniu limitu czasu Kaspersky Endpoint Security próbuje połączyć się z innym serwerem KUMA. **Certyfikat serwera**. Certyfikat TLS do nawiązania zaufanego połączenia z serwerem KUMA. Certyfikat TLS można uzyskać w konsoli Kaspersky Unified Monitoring and Analysis Platform (zobacz instrukcje w Kaspersky Unified Monitoring and Analysis Platform). Aby nawiązać zaufane połączenie, w konsoli KUMA w ustawieniach złącza tcp należy wybrać opcję tryb TLS **With verification** (patrz ustawienia złącza typu tcp w pomocy platformy Kaspersky Unified Monitoring and Analysis Platform). **Zastosuj uwierzytelnianie dwukierunkowe**. Uwierzytelnianie dwukierunkowe podczas nawiązywania bezpiecznego połączenia między Kaspersky Endpoint Security a platformą KUMA. Aby skorzystać z uwierzytelniania dwukierunkowego, w konsoli KUMA w ustawieniach złącza tcp należy wybrać opcję trybu TLS **Custom PFX** (patrz ustawienia złącza typu tcp w pomocy platformy Kaspersky Unified Monitoring and Analysis Platform). Następnie musisz uzyskać kontener szyfrowania i ustawić hasło, aby chronić kontener szyfrowania. *Kontener kryptograficzny* to archiwum PFX z certyfikatem i kluczem prywatnym. Po skonfigurowaniu ustawień platformy KUMA należy również włączyć uwierzytelnianie dwukierunkowe w ustawieniach Kaspersky Endpoint Security i załadować chroniony hasłem kontener kryptograficzny. Kontener szyfrowania musi być zabezpieczony hasłem. Nie ma możliwości dodania kontenera szyfrowania z pustym hasłem.
Serwery KUMA	Ustawienia połączeń z serwerami Kaspersky Unified Monitoring and Analysis Platform. Możesz wprowadzić adres IP (IPv4 lub IPv6). Można dodać wiele adresów serwera KUMA. Kaspersky Endpoint Security próbuje nawiązać połączenie z serwerem przy użyciu pierwszego adresu IP. Jeśli nie uda się nawiązać połączenia, Kaspersky Endpoint Security spróbuje połączyć się z serwerem przy użyciu drugiego adresu IP itd.

Szyfrowanie całego dysku

Możesz wybrać technologię szyfrowania: Kaspersky Disk Encryption lub Szyfrowanie dysków funkcją BitLocker (zwana dalej również „BitLocker").

Kaspersky Disk Encryption

Rozwiązanie Kaspersky Disk Encryption nie jest obsługiwane na komputerach opartych na architekturze ARM.

Po zaszyfrowaniu dysków twardych, przy kolejnym uruchomieniu komputera użytkownik musi przejść proces autoryzacji przy użyciu Agenta autoryzacji przed uzyskaniem dostępu do dysków twardych i załadowaniem systemu operacyjnego. Wymaga to wprowadzenia hasła do tokena lub karty inteligentnej podłączonej do komputera, bądź wpisania nazwy użytkownika i hasła konta Agenta autoryzacji utworzonego przez administratora lokalnej sieci firmowej przy użyciu zadania *Zarządzanie kontami Agenta autoryzacji*. Konta te są oparte na kontach systemu Microsoft Windows, z poziomu których użytkownik loguje się do systemu operacyjnego. Możesz także użyć technologii Single Sign-On (SSO), która umożliwia automatyczne logowanie do systemu operacyjnego przy użyciu nazwy użytkownika i hasła dla konta Agenta autoryzacji.

Autoryzacja użytkownika w Agencie autoryzacji może przebiegać na dwa sposoby:

- Poprzez wprowadzenie nazwy i hasła konta Agenta autoryzacji, utworzonego przez administratora sieci LAN przy użyciu narzędzi Kaspersky Security Center.
- Poprzez wprowadzenie hasła do tokena lub karty inteligentnej, podłączonych do komputera.

  Użycie tokena lub karty inteligentnej jest możliwe tylko wtedy, gdy dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES256. Jeśli dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES56, dodanie pliku certyfikatu elektronicznego do polecenia zostanie odrzucone.

Szyfrowanie dysków funkcją BitLocker

BitLocker to technologia szyfrowania wbudowana w systemy operacyjne Windows. Kaspersky Endpoint Security pozwala kontrolować i zarządzać funkcją Bitlocker za pomocą infrastruktury Kaspersky Next. BitLocker szyfruje woluminy logiczne. Funkcja BitLocker nie może być używana do szyfrowania dysków wymiennych. Więcej informacji na temat BitLocker można znaleźć w dokumentacji firmy Microsoft.

Podczas szyfrowania dysku program BitLocker umieszcza program rozruchowy i inne pliki pomocnicze w system partition. Ta partycja nie jest szyfrowana. System operacyjny automatycznie tworzy partycję systemową podczas instalacji systemu Windows. Jeśli dysk został całkowicie podzielony na partycje przed zainstalowaniem systemu Windows, system operacyjny nie będzie mógł utworzyć partycji systemowej. W takim przypadku po uruchomieniu szyfrowania dysku funkcją BitLocker, system operacyjny wyświetla użytkownikowi

monit o ponowne podzielenie dysku na partycje i utworzenie partycji systemowej. Po utworzeniu partycji systemowej system operacyjny uruchamia szyfrowanie BitLocker.

Funkcja BitLocker zapewnia bezpieczne przechowywanie kluczy dostępu za pomocą zaufanego modułu platformy. *Trusted Platform Module* (TPM) to mikroczip zaprojektowany do zapewnienia podstawowych funkcji związanych z bezpieczeństwem (na przykład, do przechowywania kluczy szyfrowania). Trusted Platform Module jest zazwyczaj instalowany w płycie głównej komputera i komunikuje się z wszystkimi pozostałymi komponentami systemu za pośrednictwem magistrali sprzętowej. Korzystanie z modułu TPM jest najbezpieczniejszym sposobem przechowywania kluczy dostępu funkcji BitLocker, ponieważ moduł TPM zapewnia weryfikację integralności systemu przed uruchomieniem. Nadal możesz szyfrować dyski na komputerze bez modułu TPM. W takim przypadku klucz dostępu zostanie zaszyfrowany przy użyciu hasła. Funkcja BitLocker używa następujących metod uwierzytelniania:

- TPM.
- TPM i PIN.
- Hasło.

Po zaszyfrowaniu systemowego dysku twardego użytkownik musi przejść uwierzytelnianie funkcją BitLocker, aby uruchomić system operacyjny. Po uwierzytelnieniu BitLocker umożliwia użytkownikowi zalogowanie się. Funkcja BitLocker nie obsługuje technologii pojedynczego logowania (SSO).

Po zaszyfrowaniu dysku funkcja BitLocker tworzy klucz odzyskiwania. Kaspersky Endpoint Security wysyła klucz odzyskiwania do Kaspersky Security Center, aby umożliwić przywrócenie dostępu do dysku, na przykład, jeśli użytkownik zapomniał hasło.

Jeśli użytkownik zaszyfruje dysk przy użyciu funkcji BitLocker, Kaspersky Endpoint Security wyśle klucz odzyskiwania i informacje o szyfrowaniu dysku do Kaspersky Security Center.

Jeśli używasz zasad grupy Windows, wyłącz zarządzanie funkcją BitLocker w ustawieniach zasad. Ustawienia zasad Windows mogą kolidować z ustawieniami zasad Kaspersky Endpoint Security. Podczas szyfrowania dysku mogą wystąpić błędy.

Ustawienia komponentu Kaspersky Disk Encryption

Parametr	Opis
Tryb szyfrowania	**Zaszyfruj wszystkie dyski twarde**. Jeśli ta opcja jest zaznaczona, aplikacja szyfruje wszystkie dyski twarde po zastosowaniu zasady. Jeśli na komputerze jest zainstalowanych kilka systemów operacyjnych, po szyfrowaniu będziesz mógł załadować tylko ten system operacyjny, na którym jest zainstalowana aplikacja. **Odszyfruj wszystkie dyski twarde**. Jeśli ta opcja jest zaznaczona, aplikacja odszyfrowuje wszystkie zaszyfrowane wcześniej dyski twarde po zastosowaniu zasady. **Pozostaw niezmienione**. Jeśli ten element jest zaznaczony, po zastosowaniu zasady aplikacja pozostawia dyski nienaruszone. Jeśli dysk był zaszyfrowany, pozostanie zaszyfrowany. Jeśli dysk był odszyfrowany, pozostanie odszyfrowany. Ten element jest wybrany domyślnie.
Podczas szyfrowania automatycznie utwórz konta Agenta autoryzacji dla użytkowników systemu Windows	Jeśli to pole jest zaznaczone, aplikacja tworzy konta Agenta autoryzacji w oparciu o listę kont użytkowników systemu Windows na komputerze. Domyślnie, Kaspersky Endpoint Security używa wszystkich kont lokalnych i domenowych, z którymi użytkownik logował się do systemu operacyjnego w ciągu ostatnich 30 dni.

Parametr	Opis
Ustawienia tworzenia konta Agenta autoryzacji	**Wszystkie konta na komputerze**. Wszystkie konta na komputerze, które były aktywne w dowolnym momencie. **Wszystkie konta domenowe na komputerze**. Wszystkie konta na komputerze, które należą do niektórych domen i które były aktywne w dowolnym momencie. **Wszystkie konta lokalne na komputerze**. Wszystkie konta lokalne na komputerze, które były aktywne w dowolnym momencie. **Konto usługi z hasłem jednorazowym**. Konto usługi jest niezbędne do uzyskania dostępu do komputera, na przykład, gdy użytkownik zapomni hasło. Możesz także użyć konta usługi jako konta zapasowego. Musisz wprowadzić nazwę konta (domyślnie, `ServiceAccount`). Kaspersky Endpoint Security tworzy hasło automatycznie. Hasło możesz znaleźć w konsoli Kaspersky Security Center. **Lokalny administrator**. Kaspersky Endpoint Security tworzy konto użytkownika Agenta autoryzacji dla lokalnego administratora komputera. **Menedżer komputera**. Kaspersky Endpoint Security tworzy konto użytkownika Agenta autoryzacji dla konta menadżera komputera. Możesz zobaczyć, które konto ma rolę menadżera komputera we właściwościach komputera w Active Directory. Domyślnie, rola menadżera komputera nie jest zdefiniowana, czyli nie odpowiada żadnemu kontu. **Aktywne konto**. Kaspersky Endpoint Security automatycznie tworzy konto Agenta autoryzacji dla konta, które jest aktywne w momencie szyfrowania dysku.
Automatycznie utwórz konta Agenta autoryzacji dla wszystkich użytkowników tego komputera podczas pierwszego logowania	Jeśli to pole jest zaznaczone, aplikacja sprawdza informacje o kontach użytkownika systemu Windows na komputerze przed uruchomieniem Agenta autoryzacji. Jeśli Kaspersky Endpoint Security wykryje konto użytkownika systemu Windows, które nie zawiera konta Agenta autoryzacji, aplikacja utworzy nowe konto do uzyskania dostępu do zaszyfrowanych dysków. Nowe konto Agenta autoryzacji będzie posiadało domyślne ustawienia: tylko logowanie zabezpieczone hasłem oraz zmiana hasła po pierwszej autoryzacji. Dlatego też nie musisz ręcznie dodawać kont Agenta autoryzacji przy użyciu zadania *Zarządzanie kontami Agenta autoryzacji* dla komputerów z już zaszyfrowanymi dyskami.
Zapisz nazwę użytkownika wprowadzoną w Agencie autoryzacji	Jeśli to pole jest zaznaczone, aplikacja zapisze nazwę konta Agenta autoryzacji. Przy następnej próbie zalogowania się do Agenta autoryzacji z poziomu tego samego konta nie będzie konieczne wpisanie nazwy konta.
Szyfruj tylko zajętą przestrzeń dysku (redukuje czas szyfrowania)	To pole włącza/wyłącza opcję ograniczającą obszar szyfrowania tylko do zajmowanych sektorów dysku twardego. To ograniczenie pozwala na skrócenie czasu szyfrowania. Włączenie lub wyłączenie funkcji **Szyfruj tylko zajętą przestrzeń dysku (redukuje czas szyfrowania)** po rozpoczęciu szyfrowania nie powoduje zmodyfikowania tego ustawienia, aż do odszyfrowania dysków twardych. Przed rozpoczęciem szyfrowania należy zaznaczyć lub odznaczyć to pole. Jeśli pole jest zaznaczone, zostaną zaszyfrowane tylko te obszary dysku twardego, które są zajęte przez pliki. Kaspersky Endpoint Security automatycznie szyfruje nowe dane po ich dodaniu. Jeśli pole jest odznaczone, cały dysk twardy jest szyfrowany, w tym fragmenty wcześniej usuniętych i zmodyfikowanych plików. Ta opcja jest zalecana dla nowych dysków twardych, których dane nie zostały zmodyfikowane ani usunięte. Jeśli stosujesz szyfrowanie na dysku twardym, który jest już w użyciu, zalecane jest zaszyfrowanie całego dysku twardego. Zapewni to ochronę wszystkich danych, także tych usuniętych, które potencjalnie można odzyskać. Domyślnie to pole wyboru nie jest zaznaczone.
Obsługa starszych wersji USB (niezalecane)	To pole wyboru włącza lub wyłącza funkcjonalność Legacy USB Support. *Obsługa starszych wersji USB* **to** funkcja BIOS/UEFI, która umożliwia korzystanie z urządzeń USB (takich jak token zabezpieczający) w trakcie fazy rozruchu komputera przed uruchomieniem systemu operacyjnego (tryb BIOS). Legacy USB Support nie wpływa na obsługę urządzeń USB po uruchomieniu systemu operacyjnego. Jeśli pole jest zaznaczone, obsługa urządzeń USB podczas pierwszego uruchomienia komputera będzie włączona. Jeśli funkcja Legacy USB Support jest włączona, Agent autoryzacji w trybie BIOS nie obsługuje pracy z tokenami za pośrednictwem USB. Zalecane jest użycie tej opcji tylko wtedy, gdy istnieje problem kompatybilności sprzętowej i tylko dla tych komputerów, na których wystąpił problem.
Ustawienia hasła	Ustawienia siły hasła konta Agenta autoryzacji. Podczas korzystania z technologii logowania jednokrotnego Agent autoryzacji ignoruje wymagania dotyczące siły hasła określone w Kaspersky Security Center. Możesz ustawić wymagania dotyczące siły hasła w ustawieniach systemu operacyjnego.

Parametr	Opis
Użyj technologii logowania jednokrotnego (SSO)	Technologia SSO umożliwia użycie tych samych danych uwierzytelniających konta do uzyskania dostępu do dysków twardych i do systemu operacyjnego. Jeśli pole jest zaznaczone, musisz wprowadzić dane uwierzytelniające konta w celu uzyskania dostępu do zaszyfrowanych dysków twardych i automatycznego zalogowania do systemu operacyjnego. Jeśli pole jest odznaczone, w celu uzyskania dostępu do zaszyfrowanych dysków twardych i zalogowania do systemu operacyjnego należy oddzielnie wprowadzić dane uwierzytelniające dla uzyskania dostępu do zaszyfrowanych dysków twardych oraz dane uwierzytelniające konta użytkownika systemu operacyjnego.
Zawijaj zewnętrznych dostawców poświadczeń	Kaspersky Endpoint Security obsługuje zewnętrznego dostawcę usług uwierzytelniania ADSelfService Plus. Podczas pracy z zewnętrznymi dostawcami usług uwierzytelniania Agent autoryzacji przechwytuje hasło przed załadowaniem systemu operacyjnego. Oznacza to, że użytkownik musi wprowadzić hasło tylko raz podczas logowania się do systemu Windows. Po zalogowaniu się do systemu Windows użytkownik może korzystać z możliwości zewnętrznego dostawcy usług uwierzytelniających, na przykład do uwierzytelniania w usługach korporacyjnych. Zewnętrzni dostawcy usług uwierzytelniających pozwalają także użytkownikom na samodzielne resetowanie własnego hasła. W tym przypadku Kaspersky Endpoint Security automatycznie zaktualizuje hasło dla Agenta autoryzacji. W przypadku korzystania z zewnętrznego dostawcy usług uwierzytelniających, który nie jest obsługiwany przez aplikację, można napotkać pewne ograniczenia w działaniu technologii Single Sign-On.
Pomoc	**Autoryzacja**. Tekst pomocy wyświetlany w oknie Agenta autoryzacji podczas wprowadzania poświadczeń konta. **Zmiana hasła**. Tekst pomocy wyświetlany w oknie Agenta autoryzacji podczas zmiany hasła do konta Agenta autoryzacji. **Przywracanie hasła**. Tekst pomocy wyświetlany w oknie Agenta autoryzacji podczas odzyskiwania hasła do konta Agenta autoryzacji.

Ustawiania modułu Szyfrowania dysków funkcją BitLocker

Parametr	Opis
Tryb szyfrowania	**Zaszyfruj wszystkie dyski twarde**. Jeśli ta opcja jest zaznaczona, aplikacja szyfruje wszystkie dyski twarde po zastosowaniu zasady. Jeśli na komputerze jest zainstalowanych kilka systemów operacyjnych, po szyfrowaniu będziesz mógł załadować tylko ten system operacyjny, na którym jest zainstalowana aplikacja. **Odszyfruj wszystkie dyski twarde**. Jeśli ta opcja jest zaznaczona, aplikacja odszyfrowuje wszystkie zaszyfrowane wcześniej dyski twarde po zastosowaniu zasady. **Pozostaw niezmienione**. Jeśli ten element jest zaznaczony, po zastosowaniu zasady aplikacja pozostawia dyski nienaruszone. Jeśli dysk był zaszyfrowany, pozostanie zaszyfrowany. Jeśli dysk był odszyfrowany, pozostanie odszyfrowany. Ten element jest wybrany domyślnie.
Włącz korzystanie z uwierzytelniania BitLocker wymagającego wprowadzania danych z klawiatury przed uruchomieniem na tabletach	Korzystanie z uwierzytelniania wymagającego wprowadzenia danych przed rozruchem nawet wtedy, gdy platforma nie oferuje takiej możliwości (na przykład klawiatury dotykowe na tabletach). Ekran dotykowy komputerów typu tablet nie jest dostępny w środowisku wykonawczym przed uruchomieniem systemu. Aby zakończyć uwierzytelnianie funkcji BitLocker na komputerach typu tablet, użytkownik musi, na przykład, podłączyć klawiaturę USB. Jeśli pole jest zaznaczone, użycie uwierzytelniania wymagającego wprowadzenia danych przed rozruchem jest dozwolone. Zalecane jest korzystanie z tego ustawienia tylko na urządzeniach, na których znajdują się alternatywne narzędzia do wprowadzania danych przed rozruchem, na przykład klawiatura USB będąca dodatkiem do klawiatury dotykowej. Jeśli pole jest odznaczone, szyfrowanie dysków funkcją BitLocker nie jest możliwe na tabletach.
Użyj szyfrowania sprzętowego (dla Windows 8 i nowszych)	Jeśli pole jest zaznaczone, aplikacja stosuje szyfrowanie sprzętu. Umożliwia to przyspieszenie szyfrowania i zużycie mniejszej ilości zasobów.

Parametr	Opis
Szyfruj tylko zajętą przestrzeń dysku (dla Windows 8 i nowszych)	To pole włącza/wyłącza opcję ograniczającą obszar szyfrowania tylko do zajmowanych sektorów dysku twardego. To ograniczenie pozwala na skrócenie czasu szyfrowania. Włączenie lub wyłączenie funkcji **Szyfruj tylko zajętą przestrzeń dysku (redukuje czas szyfrowania)** po rozpoczęciu szyfrowania nie powoduje zmodyfikowania tego ustawienia, aż do odszyfrowania dysków twardych. Przed rozpoczęciem szyfrowania należy zaznaczyć lub odznaczyć to pole. Jeśli pole jest zaznaczone, zostaną zaszyfrowane tylko te obszary dysku twardego, które są zajęte przez pliki. Kaspersky Endpoint Security automatycznie szyfruje nowe dane po ich dodaniu. Jeśli pole jest odznaczone, cały dysk twardy jest szyfrowany, w tym fragmenty wcześniej usuniętych i zmodyfikowanych plików. Ta opcja jest zalecana dla nowych dysków twardych, których dane nie zostały zmodyfikowane ani usunięte. Jeśli stosujesz szyfrowanie na dysku twardym, który jest już w użyciu, zalecane jest zaszyfrowanie całego dysku twardego. Zapewni to ochronę wszystkich danych, także tych usuniętych, które potencjalnie można odzyskać. Domyślnie to pole wyboru nie jest zaznaczone.
Metoda uwierzytelniania	**Tylko hasło (dla Windows 8 i nowszych)** Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security wyświetli pytanie o wprowadzenie hasła podczas próby uzyskania dostępu do zaszyfrowanego dysku. Ta opcja może zostać wybrana, gdy moduł TPM nie jest używany. **Moduł TPM (Trusted platform module)** Jeśli ta opcja jest zaznaczona, BitLocker korzysta z modułu TPM (Trusted Platform Module). *Trusted Platform Module* (TPM) to mikroczip zaprojektowany do zapewnienia podstawowych funkcji związanych z bezpieczeństwem (na przykład, do przechowywania kluczy szyfrowania). Trusted Platform Module jest zazwyczaj instalowany w płycie głównej komputera i komunikuje się z wszystkimi pozostałymi komponentami systemu za pośrednictwem magistrali sprzętowej. Dla komputerów działających pod kontrolą systemu Windows 7 lub Windows Server 2008 R2 dostępne jest tylko szyfrowanie przy użyciu modułu TPM. Jeśli moduł TPM nie jest zainstalowany, szyfrowanie funkcją BitLocker nie jest możliwe. Użycie hasła na tych komputerach nie jest obsługiwane. Urządzenie posiadające moduł Trusted Platform Module może tworzyć klucze szyfrowania, które mogą zostać odszyfrowane tylko z pomocą urządzenia. TPM szyfruje klucze szyfrowania, korzystając z własnych kluczy głównych magazynowania. Klucz główny magazynowania jest przechowywany w Trusted Platform Module. Zapewnia to dodatkowy poziom ochrony przed próbami zhakowania kluczy szyfrowania. To ustawienie jest wybrane domyślnie. Możesz ustawić dodatkową warstwę ochrony dostępu do klucza szyfrowania i zaszyfrować klucz z hasłem lub kodu PIN: • **Użyj kodu PIN dla TPM**. Jeśli to pole jest zaznaczone, użytkownik może użyć kodu PIN do uzyskania dostępu do klucza szyfrowania przechowywanego w Trusted Platform Module (TPM). Jeśli to pole jest odznaczone, użytkownicy nie mogą korzystać z kodów PIN. Aby uzyskać dostęp do klucza szyfrowania, użytkownik musi wprowadzić hasło. • **Moduł TPM (Trusted platform module) lub hasło, jeśli moduł TPM jest niedostępny**. Jeśli ta opcja jest zaznaczona, użytkownik może użyć hasła w celu uzyskania dostępu do kluczy szyfrowania, gdy moduł Trusted Platform Module (TPM) jest niedostępny. Jeśli pole wyboru zostanie odznaczone, a TPM nie jest dostępny, szyfrowanie całego dysku nie rozpocznie się. Wybraną metodę uwierzytelniania należy skonfigurować, określając wymagania dotyczące hasła lub kodu PIN: • **Minimalna długość kodu PIN (znaki)**. • **Minimalna długość hasła (znaki)**. • **Ogranicz okres ważności hasła / numeru PIN dla TPM (liczba dni)**. • **Użyj ulepszonego kodu PIN (litery i cyfry)**. *Rozszerzony kod PIN* umożliwia używanie innych znaków jako dodatku do znaków numerycznych: wielkich i małych liter alfabetu łacińskiego, znaków specjalnych i spacji.
Automatycznie odtwórz klucz odzyskiwania (liczba dni)	Umożliwia automatyczne aktualizowanie hasła w celu przywrócenia dostępu do dysku chronionego funkcją BitLocker. Jeśli to pole jest zaznaczone, musisz wybrać okres ważności hasła klucza odzyskiwania. Zapobiega to ponownemu wykorzystaniu hasła klucza odzyskiwania.

Szyfrowanie plików

Szyfrowanie plików nie jest obsługiwane na komputerach opartych na architekturze ARM.

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Możesz tworzyć listy plików według rozszerzenia lub grup rozszerzeń oraz listy folderów przechowywanych na lokalnych dyskach komputera, a także tworzyć reguły szyfrowania plików, które są tworzone przez określone aplikacje. Po zastosowaniu zasady, Kaspersky Endpoint Security zaszyfruje i odszyfruje następujące pliki:

- Pliki pojedynczo dodane do list elementów przeznaczonych do zaszyfrowania i odszyfrowania;
- Pliki przechowywane w folderach dodanych do list elementów przeznaczonych do zaszyfrowania i odszyfrowania;
- Pliki utworzone przez oddzielne aplikacje.

Szyfrowanie plików ma następujące funkcje specjalne:

- Kaspersky Endpoint Security szyfruje / deszyfruje pliki w wstępnie określonych folderach tylko dla profili lokalnego użytkownika systemu operacyjnego. Kaspersky Endpoint Security nie szyfruje / deszyfruje plików w predefiniowanych folderach profili użytkownika mobilnego, obowiązkowych profili użytkownika, tymczasowych profili użytkownika lub folderach przekierowanych.
- Kaspersky Endpoint Security nie szyfruje plików, których modyfikacja mogłaby uszkodzić system operacyjny i zainstalowane aplikacje. Na przykład, na liście wykluczeń szyfrowania znajdują się następujące pliki i foldery ze wszystkimi osadzonymi folderami:
  - %WINDIR%;
  - %PROGRAMFILES% i %PROGRAMFILES(X86)%;
  - Pliki rejestru systemu Windows.

  Lista wykluczeń z szyfrowania nie może być podglądana ani modyfikowana. Pliki i foldery znajdujące się na liście wykluczeń z szyfrowania mogą być dodawane do listy szyfrowania, ale i tak nie będą szyfrowane podczas wykonywania szyfrowania plików.

Ustawienia komponentu Szyfrowanie plików

Parametr	Opis
Tryb szyfrowania	**Pozostaw niezmienione**. Jeśli ten element jest zaznaczony, Kaspersky Endpoint Security pozostawia pliki i foldery bez zmian, nie szyfrując i nie deszyfrując ich. **Zgodnie z regułami**. Jeśli wybrano ten element, Kaspersky Endpoint Security szyfruje pliki i foldery zgodnie z regułami szyfrowania, deszyfruje pliki i foldery zgodnie z regułami deszyfrowania, a także reguluje dostęp aplikacji do zaszyfrowanych plików zgodnie z regułami aplikacji. **Odszyfruj wszystkie**. Jeśli ten element jest zaznaczony, Kaspersky Endpoint Security odszyfruje wszystkie zaszyfrowane pliki i foldery.

Parametr	Opis
Szyfrowanie	Ta zakładka wyświetla reguły szyfrowania dla plików przechowywanych na dyskach lokalnych. Możesz dodać pliki w następujący sposób: • **Wstępnie określone foldery**. Kaspersky Endpoint Security pozwala dodać następujące obszary: **Dokumenty**. Pliki w standardowym folderze *Dokumenty* systemu operacyjnego i jego podfolderach. **Ulubione**. Pliki w standardowym folderze *Ulubione* systemu operacyjnego i jego podfolderach. **Pulpit**. Pliki w standardowym folderze *Pulpit* systemu operacyjnego i jego podfolderach. **Pliki tymczasowe**. Pliki tymczasowe związane z działaniem aplikacji zainstalowanych na komputerze. Na przykład, aplikacje Microsoft Office tworzą pliki tymczasowe zawierające kopie zapasowe dokumentów. **Pliki programu Outlook**. Pliki dotyczące działania klienta poczty Outlook: pliki danych (PST), pliki danych offline (OST), pliki książki adresowej offline (OAB) oraz pliki osobistej książki adresowej (PAB). • **Folder niestandardowy**. Możesz wpisać ścieżkę dostępu do folderu. Dodając ścieżkę folderu, przestrzegaj następujących zasad: Użyj zmiennej środowiskowej (na przykład: `%FOLDER%\UserFolder\`). Możesz użyć zmiennej środowiskowej tylko raz i tylko na początku ścieżki. Nie używaj ścieżek względnych. Nie używaj znaków `*` i `?`. Nie używaj ścieżek UNC. Użyj `;` lub `,` jako separatora. • **Pliki według rozszerzenia**. Możesz wybrać grupy rozszerzeń z listy, takie jak *Archiwa* grup rozszerzeń. Możesz także ręcznie dodać rozszerzenie pliku.
Odszyfrowywanie	Ta zakładka wyświetla reguły deszyfrowania dla plików przechowywanych na dyskach lokalnych.
Reguły dla aplikacji	Zakładka wyświetla tabelę zawierającą reguły dostępu do zaszyfrowanych plików dla aplikacji oraz reguły szyfrowania dla plików, które zostały utworzone lub zmodyfikowane przez pojedyncze aplikacje.
Zaszyfrowane pakiety	Wymagania dotyczące siły hasła, jakie mają być spełniane podczas tworzenia zaszyfrowanych pakietów.

Szyfrowanie nośników wymiennych

Szyfrowanie dysków wymiennych nie jest obsługiwane na komputerach opartych na architekturze ARM.

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Kaspersky Endpoint Security obsługuje szyfrowanie plików w systemach plików FAT32 i NTFS. Jeśli dysk wymienny z nieobsługiwanym systemem plików jest podłączony do komputera, zadanie szyfrowania dla tego dysku wymiennego zakończy się błędem, a Kaspersky Endpoint Security przypisze do dysku wymiennego stan tylko do odczytu.

W celu ochrony danych na dyskach wymiennych możesz użyć następujących typów szyfrowania:

- Full Disk Encryption (FDE).

  Szyfrowanie całego dysku wymiennego, w tym systemu plików.

  Nie jest możliwy dostęp do zaszyfrowanych danych poza siecią korporacyjną. Dostęp do zaszyfrowanych danych w sieci korporacyjnej jest również niemożliwy, jeśli komputer nie jest podłączony do Kaspersky Security Center (na przykład, na komputerze gościa).

- File Level Encryption (FLE).

  Szyfrowanie tylko plików na dysku wymiennym. System plików pozostaje niezmieniony.

Szyfrowanie plików na dyskach wymiennych umożliwia dostęp do danych poza siecią korporacyjną za pomocą specjalnego trybu zwanego *trybem przenośnym*.

Podczas szyfrowania Kaspersky Endpoint Security tworzy klucz główny. Kaspersky Endpoint Security zapisuje klucz główny w następujących repozytoriach:

- Kaspersky Security Center.
- Na komputerze użytkownika.

  Klucz główny jest szyfrowany za pomocą tajnego klucza użytkownika.
- Na dysku wymiennym.

  Klucz główny jest szyfrowany za pomocą klucza publicznego Kaspersky Security Center.

Po zakończeniu szyfrowania dane na dysku wymiennym mogą być dostępne w sieci korporacyjnej tak, jakbyś używał zwykłego niezaszyfrowanego dysku wymiennego.

Uzyskiwanie dostępu do zaszyfrowanych danych

Gdy podłączony jest dysk wymienny z zaszyfrowanymi danymi, Kaspersky Endpoint Security wykonuje następujące czynności:

1. Sprawdza klucz główny w lokalnej pamięci na komputerze użytkownika.

   Jeśli klucz główny zostanie znaleziony, użytkownik uzyskuje dostęp do danych na dysku wymiennym.

   Jeśli klucz główny nie zostanie znaleziony, Kaspersky Endpoint Security wykonuje następujące działania:

   a. Wysyła zapytanie do Kaspersky Security Center.

      Po otrzymaniu zapytania, Kaspersky Security Center wysyła odpowiedź zawierającą klucz główny.

   b. Kaspersky Endpoint Security zapisuje klucz główny w lokalnej pamięci na komputerze użytkownika do późniejszych operacji na zaszyfrowanym dysku wymiennym.
2. Odszyfrowuje dane.

Specjalne funkcje szyfrowania dysku wymiennego

Szyfrowanie dysków wymiennych ma następujące funkcje specjalne:

- Zasada z predefiniowanymi ustawieniami szyfrowania dysku wymiennego zostanie utworzona dla określonej grupy zarządzanych komputerów. Dlatego też, wynik stosowania profilu Kaspersky Security Center, skonfigurowanego dla szyfrowania/deszyfrowania dysków wymiennych zależy od komputera, do którego podłączony jest dysk wymienny.
- Kaspersky Endpoint Security nie szyfruje/deszyfruje plików tylko do odczytu, które są przechowywane na nośnikach wymiennych.

- Następujące typy urządzeń są obsługiwane jako dyski wymienne:
  - Nośniki danych podłączane poprzez magistralę USB
  - Dyski twarde podłączane poprzez magistrale USB i FireWire
  - Dyski SSD podłączane poprzez magistrale USB i FireWire

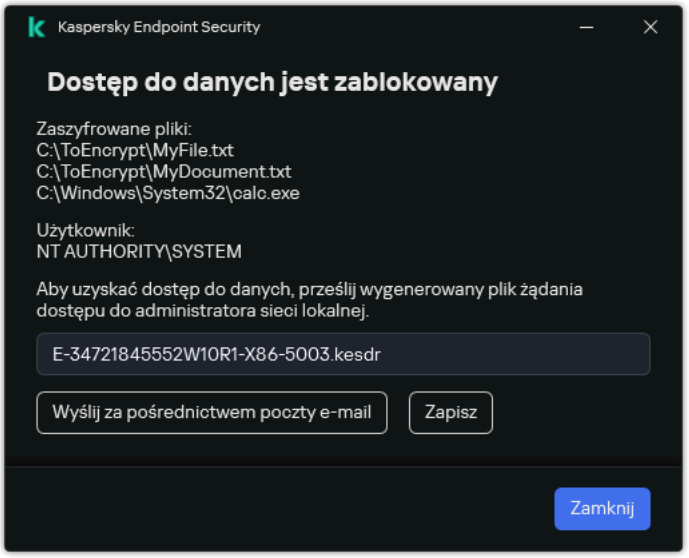
Ustawienia komponentu Szyfrowanie nośników wymiennych

Parametr	Opis
Tryb szyfrowania	**Zaszyfruj cały dysk wymienny**. Jeśli wybrano tę opcję, podczas stosowania zasady z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security szyfruje dyski wymienne sektor po sektorze, w tym ich systemy plików. **Zaszyfruj wszystkie pliki**. Jeśli wybrano tę opcję, podczas stosowania zasady z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security szyfruje wszystkie pliki przechowywane na dyskach wymiennych. Kaspersky Endpoint Security nie szyfruje ponownie plików, które zostały już zaszyfrowane. Zawartość systemu plików nośników wymiennych, łącznie ze strukturą folderów i z nazwami zaszyfrowanych plików, nie jest szyfrowana i pozostaje dostępna. **Zaszyfruj tylko nowe pliki**. Jeśli wybrano tę opcję, podczas stosowania zasady z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security szyfruje tylko te pliki, które zostały dodane lub zmodyfikowane na dyskach wymiennych po ostatnim zastosowaniu zasady Kaspersky Security Center. Ten tryb szyfrowania jest wygodny, jeśli dysk wymienny jest wykorzystywany zarówno do celów prywatnych, jak i do celów firmowych. Ten tryb szyfrowania pozwala na zachowanie wszystkich starych plików niezmienionych i zaszyfrowanie tylko tych plików, które użytkownik utworzy w trakcie pracy na komputerze z zainstalowanym Kaspersky Endpoint Security i włączoną funkcją szyfrowania. W rezultacie dostęp do prywatnych plików jest zawsze możliwy, niezależnie od tego, czy Kaspersky Endpoint Security jest zainstalowany na komputerze z włączoną funkcją szyfrowania. **Odszyfruj cały dysk wymienny**. Jeśli wybrano tę opcję, podczas stosowania zasady z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security deszyfruje wszystkie zaszyfrowane pliki przechowywane na dyskach wymiennych oraz systemy plików dysków wymiennych, jeśli zostały już wcześniej zaszyfrowane. **Pozostaw niezmienione**. Jeśli ten element jest zaznaczony, po zastosowaniu zasady aplikacja pozostawia dyski nienaruszone. Jeśli dysk był zaszyfrowany, pozostanie zaszyfrowany. Jeśli dysk był odszyfrowany, pozostanie odszyfrowany. Ten element jest wybrany domyślnie.
Tryb przenośny	Pole to włącza/wyłącza przygotowywanie dysku wymiennego, które pozwala na dostęp do plików przechowywanych na tym dysku wymiennym na komputerach poza siecią korporacyjną. Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security prosi użytkownika o podanie hasła przed zaszyfrowaniem plików na dysku wymiennym po zastosowaniu zasady. Hasło jest niezbędne do uzyskania dostępu do plików zaszyfrowanych na dysku wymiennym na komputerach poza siecią korporacyjną. Możesz skonfigurować siłę hasła. Tryb przenośny jest dostępny dla trybów **Zaszyfruj wszystkie pliki** lub **Zaszyfruj tylko nowe pliki**.
Zaszyfruj tylko używaną przestrzeń dyskową	To pole włącza / wyłącza tryb szyfrowania, w którym tylko zajmowane sektory dysku zostaną zaszyfrowane. Ten tryb jest zalecany dla nowych dysków, których dane nie zostały zmodyfikowane ani usunięte. Jeśli pole jest zaznaczone, zostaną zaszyfrowane tylko te obszary dysku, które są zajęte przez pliki. Kaspersky Endpoint Security automatycznie szyfruje nowe dane po ich dodaniu. Jeśli pole jest odznaczone, cały dysk jest szyfrowany, w tym fragmenty wcześniej usuniętych i zmodyfikowanych plików. Możliwość szyfrowania tylko zajętego miejsca jest dostępna tylko dla trybu **Zaszyfruj cały dysk wymienny**. Po uruchomieniu szyfrowania, włączenie/wyłączenie funkcji **Zaszyfruj tylko używaną przestrzeń dyskową** nie zmieni tego ustawienia. Przed rozpoczęciem szyfrowania należy zaznaczyć lub odznaczyć to pole.
Reguły niestandardowe	Ta tabela zawiera urządzenia, dla których zdefiniowano niestandardowe reguły szyfrowania. Możesz utworzyć reguły szyfrowania dla poszczególnych dysków wymiennych na następujące sposoby: • Dodaj dysk wymienny z listy zaufanych urządzeń dla Kontroli urządzeń. • Ręcznie dodaj dysk wymienny: • Według identyfikatora urządzenia (Hardware ID lub HWID) • Według modelu urządzenia: Vendor ID (VID) i Product ID (PID)

Parametr	Opis
Zezwól na szyfrowanie dysków wymiennych w trybie offline	Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security szyfruje dyski wymienne, nawet jeśli nie ma połączenia z Kaspersky Security Center. W tym przypadku dane wymagane do odszyfrowania nośnika wymiennego są przechowywane na dysku twardym komputera, do którego podłączony jest nośnik wymienny, i nie są przesyłane do Kaspersky Security Center. Jeśli pole to nie jest zaznaczone, Kaspersky Endpoint Security nie szyfruje dysków wymiennych bez połączenia z Kaspersky Security Center.
Ustawienia hasła szyfrowania / Przenośny menedżer plików	Ustawienia siły hasła dla Przenośnego menedżera plików.

Szablony (szyfrowanie danych)

Po zaszyfrowaniu danych Kaspersky Endpoint Security może ograniczyć dostęp do danych, na przykład, ze względu na zmianę infrastruktury organizacji i zmianę na Serwerze administracyjnym Kaspersky Security Center. Jeśli użytkownik nie ma dostępu do zaszyfrowanych danych, może poprosić administratora o dostęp do danych. Innymi słowy, użytkownik musi wysłać plik żądania dostępu do administratora. Użytkownik musi następnie przesłać plik odpowiedzi otrzymany od administratora do Kaspersky Endpoint Security. Kaspersky Endpoint Security pozwala poprosić administratora o dostęp do danych za pośrednictwem poczty elektronicznej (patrz rysunek poniżej).



Proszenie o dostęp do zaszyfrowanych danych

Udostępniono szablon do zgłaszania braku dostępu do zaszyfrowanych danych. Dla wygody użytkownika możesz wypełnić następujące pola:

- **Do**. Wprowadź adres e-mail grupy administratorów z uprawnieniami do funkcji szyfrowania danych.
- **Temat**. Wprowadź temat wiadomości e-mail z prośbą o dostęp do zaszyfrowanych plików. Możesz, na przykład, dodawać znaczniki, aby filtrować wiadomości.
- **Komunikat użytkownika**. W razie potrzeby zmień treść wiadomości. Możesz użyć zmiennych, aby uzyskać niezbędne dane (na przykład: zmienna `%USER_NAME%`).

Wykluczenia

Strefa zaufana jest utworzoną przez administratora listą obiektów i aplikacji, które nie są monitorowane przez Kaspersky Endpoint Security.

Administrator tworzy strefę zaufaną, biorąc pod uwagę cechy i funkcje używanych obiektów oraz zainstalowanych aplikacji. Umieszczenie obiektów i aplikacji w strefie zaufanej może być konieczne, gdy Kaspersky Endpoint Security blokuje dostęp do określonego obiektu lub aplikacji, które według Ciebie są nieszkodliwe. Administrator może także zezwolić użytkownikowi na utworzenie własnej lokalnej strefy zaufanej dla określonego komputera. W ten sposób użytkownicy mogą utworzyć swoje własne lokalne listy wykluczeń i zaufanych aplikacji jako dodatek do ogólnej strefy zaufanej w zasadzie.

Począwszy od Kaspersky Endpoint Security 12.5 for Windows, możesz dodać telemetrię EDR do strefy zaufanej. Umożliwia to optymalizację danych wysyłanych przez aplikację do serwera gromadzenia danych telemetrycznych dla rozwiązania Kaspersky Anti Targeted Attack Platform (EDR).

Począwszy od Kaspersky Endpoint Security 12.6 for Windows, wykluczenia skanowania I zaufane aplikacje są dodawane do strefy zaufanej. Predefiniowane wykluczenia ze skanowania i zaufane aplikacje pomagają szybko skonfigurować Kaspersky Endpoint Security na serwerach SQL, serwerach Microsoft Exchange i w menedżerze konfiguracji System Center Configuration Manager. Oznacza to, że nie musisz ręcznie konfigurować strefy zaufanej dla aplikacji na serwerach.

Począwszy od Kaspersky Endpoint Security 12.8 for Windows można instalować aplikację w trybie Light Agent w celu ochrony środowisk wirtualnych. Wstępnie zdefiniowane wykluczenia ze skanowania i zaufane aplikacje mogą pomóc w szybkiej konfiguracji Kaspersky Endpoint Security w środowiskach wirtualnych Citrix i VMware.

Wykluczenia ze skanowania

Wykluczenie ze skanowania to zestaw warunków, które muszą być spełnione, aby Kaspersky Endpoint Security nie skanował określonego obiektu w poszukiwaniu wirusów i innych zagrożeń. Wykluczenia ze skanowania zapewniają możliwość bezpiecznej pracy z legalnymi aplikacjami, które mogą zostać wykorzystane przez hakerów do uszkodzenia komputera lub danych. Nie posiadają one żadnych szkodliwych funkcji, ale mogą zostać wykorzystane przez cyberprzestępców. Szczegółowe informacje na temat legalnego oprogramowania, które może zostać użyte przez cyberprzestępców do uszkodzenia komputera lub danych osobistych, znajdują się na stronie internetowej Encyklopedii IT Kaspersky.

Takie aplikacje mogą być blokowane przez program Kaspersky Endpoint Security. Aby zapobiec blokowaniu tych aplikacji, możesz skonfigurować wykluczenia ze skanowania dla używanych aplikacji. W tym celu dodaj do strefy zaufanej nazwę lub maskę nazwy zgodną z klasyfikacją Encyklopedii IT Kaspersky. Na przykład, często używasz aplikacji Radmin do zdalnego zarządzania komputerami. Kaspersky Endpoint Security wykrywa ten rodzaj aktywności aplikacji jako podejrzany i może go zablokować. Aby zapobiec blokowaniu aplikacji, utwórz wykluczenie ze skanowania z nazwą lub maską nazwy z Encyklopedii IT Kaspersky.

Jeśli na komputerze jest zainstalowana aplikacja, która gromadzi informacje i wysyła je do przetworzenia, Kaspersky Endpoint Security może zaklasyfikować tę aplikację jako szkodliwe oprogramowanie. Aby tego uniknąć, możesz wykluczyć tę aplikację ze skanowania, konfigurując Kaspersky Endpoint Security w sposób opisany w dokumencie.

Wykluczenia ze skanowania mogą być używane przez następujące komponenty i zadania aplikacji, które zostały skonfigurowane przez administratora systemu:

- Wykrywanie zachowań
- Ochrona przed exploitami
- Ochrona przed włamaniami
- Ochrona plików
- Ochrona WWW
- Ochrona poczty
- Zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*

Lista zaufanych aplikacji

Lista zaufanych aplikacji jest listą aplikacji, których aktywność sieciowa i plikowa (włączając w to szkodliwą aktywność) oraz dostęp do rejestru systemowego nie są monitorowane przez Kaspersky Endpoint Security. Domyślnie program Kaspersky Endpoint Security monitoruje obiekty otwierane, uruchamiane lub zapisywane przez proces dowolnej aplikacji i kontroluje aktywność wszystkich aplikacji oraz ruch sieciowy będący wynikiem ich działania. Po dodaniu aplikacji do listy zaufanych aplikacji, Kaspersky Endpoint Security przestaje monitorować jej aktywność.

Różnica pomiędzy wykluczeniami skanowania a aplikacjami zaufanymi polega na tym, że w przypadku wykluczeń Kaspersky Endpoint Security nie skanuje plików, natomiast w przypadku aplikacji zaufanych nie kontroluje zainicjowanych procesów. Jeżeli aplikacja zaufana utworzy szkodliwy plik w folderze, który nie jest zawarty w wykluczeniach skanowania, Kaspersky Endpoint Security wykryje plik i wyeliminuje zagrożenie. Jeżeli folder zostanie dodany do wykluczeń, Kaspersky Endpoint Security pominie ten plik.

Na przykład jeżeli uważasz, że obiekty używane przez Notatnik firmy Microsoft Windows są nieszkodliwe (tzn. ufasz tej aplikacji), dodaj Notatnik firmy Microsoft Windows do listy zaufanych aplikacji, aby obiekty używane przez tę aplikację nie były monitorowane. Zwiększy to wydajność komputera, co jest szczególnie ważne przy korzystaniu z aplikacji serwerowych.

Oprócz tego pewne akcje zaklasyfikowane przez Kaspersky Endpoint Security jako podejrzane mogą być traktowane przez inne aplikacje jako nieszkodliwe. Na przykład przechwytywanie danych wprowadzanych z klawiatury jest charakterystyczne dla aplikacji, które automatycznie przełączają układ klawiatury (np. Punto Switcher). Aby korzystać z właściwości takich aplikacji i wyłączyć monitorowanie ich aktywności, dodaj je do listy zaufanych aplikacji.

Aplikacje zaufane pomagają uniknąć problemów z kompatybilnością pomiędzy Kaspersky Endpoint Security a innymi aplikacjami (na przykład: problem podwójnego skanowania ruchu sieciowego komputera osoby trzeciej przez Kaspersky Endpoint Security i przez inną aplikację antywirusową).

Należy pamiętać, że pliki wykonywalne oraz procesy zaufanych aplikacji będą nadal skanowane w poszukiwaniu wirusów i szkodliwych programów. Aplikacja może zostać całkowicie wykluczona ze skanowania wykonywanego przez program Kaspersky Endpoint Security przy użyciu wykluczeń ze skanowania.

Parametr	Opis

Typy wykrywanych obiektów

Bez względu na skonfigurowane ustawienia aplikacji, Kaspersky Endpoint Security zawsze wykrywa i blokuje wirusy, robaki i trojany. Mogą one wyrządzić znaczne szkody w komputerze.

- **Wirusy i robaki**

  Podkategoria: wirusy i robaki (Viruses_and_Worms)

  Poziom zagrożenia: wysoki

  Klasyczne wirusy i robaki wykonują akcje nieautoryzowane przez użytkownika. Mogą one tworzyć swoje kopie, które także są zdolne do powielania się.

  Klasyczny wirus

  Po przeniknięciu klasycznego wirusa do komputera, infekuje on plik, aktywuje się w nim, wykonuje szkodliwe działania i dodaje swoje kopie do innych plików.

  Klasyczny wirus rozprzestrzenia się jedynie na zasobach lokalnych komputera; nie może sam przedostać się na inne komputery. Przedostanie się takiego wirusa na inny komputer jest możliwe, jeśli doda on swoją kopię do pliku przechowywanego w folderze współdzielonym lub na nośniku CD, albo gdy użytkownik wyśle wiadomość z zainfekowanym załącznikiem.

  Kod klasycznego wirusa może przedostać się do różnych obszarów komputerów, systemów operacyjnych lub aplikacji. W zależności od środowiska wirusy dzieli się na *wirusy plikowe*, *wirusy sektora startowego*, *wirusy skryptowe* oraz *makrowirusy*.

  Wirusy mogą infekować pliki, korzystając z szerokiej gamy technik. Wirusy *Overwriting* zapisują swój kod na kodzie zainfekowanego pliku, wymazując zawartość tego pliku. Zainfekowany plik przestaje poprawnie działać oraz nie ma możliwości jego przywrócenia. Wirusy *Parasitic* modyfikują pliki, zezwalając na ich pełne lub częściowe działanie. *Companion* nie modyfikują plików, lecz tworzą ich kopie. Kiedy otwarty zostanie zainfekowany plik, uruchomiona zostanie jego kopia (czyli wirus). Istnieją również inne typy wirusów: *wirusy Link*, *wirusy plików OBJ*, *wirusy bibliotek LIB*, wirusy *infekujące kody źródłowe* oraz wiele innych.

  Worm

  Podobnie jak w przypadku klasycznego wirusa, kod robaka zostaje aktywowany i wykonuje on szkodliwe działania po przeniknięciu do komputera. Robaki noszą taką nazwę z powodu swojej zdolności do „przepełzania" z jednego komputera na inny i rozprzestrzeniania swoich kopii za pośrednictwem wielu kanałów danych bez wiedzy użytkownika.

  Główną cechą, która umożliwia rozróżnianie typów robaków, jest ich sposób rozprzestrzeniania się. Następująca tabela zawiera przegląd różnych typów robaków, klasyfikowanych zgodnie ze sposobem rozprzestrzeniania się.

  Sposoby rozprzestrzeniania się robaka

Typ	Nazwa	Opis
Email-Worm	Email-Worm	Rozprzestrzeniają się poprzez pocztę elektroniczną. Zainfekowana wiadomość zawiera załączony plik z kopią robaka lub odnośnik do pliku znajdującego się na stronie internetowej, która może być albo przechwycona przez hakerów, albo stworzona specjalnie w tym celu. Jeśli otworzysz zainfekowany plik, robak zostanie aktywowany. Po kliknięciu odsyłacza, pobraniu i otwarciu pliku, robak również rozpoczyna swoją szkodliwą działalność. Następnie zaczyna rozprzestrzeniać swoje kopie, wyszukując kolejne adresy e-mail i wysyłając na nie zainfekowane wiadomości.
IM-Worm	Robaki klientów komunikatorów internetowych	Rozprzestrzeniają się poprzez klienty komunikatorów internetowych. Z reguły robaki te za pośrednictwem listy kontaktów użytkownika wysyłają wiadomości zawierające odnośnik do pliku ze swoją kopią. Po pobraniu i otwarciu takiego pliku przez użytkownika, robak jest aktywowany.
IRC-Worm	Robaki czatu internetowego	Rozprzestrzeniają się za pośrednictwem kanału Internet Relay Chats – czyli usługi sieciowej pozwalającej na komunikowanie się w internecie w czasie rzeczywistym. Robaki te publikują w czacie internetowym pliki zawierające ich kopie lub odnośniki do pliku. Po pobraniu i otwarciu takiego pliku przez użytkownika, robak jest aktywowany.
Net-Worm	Robaki sieciowe	Rozprzestrzeniają się one w sieciach komputerowych. W przeciwieństwie do innych rodzajów robaków, typowy robak sieciowy rozprzestrzenia się bez udziału użytkownika. Skanuje on sieć lokalną w poszukiwaniu komputerów z programami zawierającymi luki. W tym celu wysyła on specjalny pakiet sieciowy (exploit) zawierający kod robaka lub część kodu. Jeśli komputer posiadający luki znajduje się w sieci, otrzyma taki pakiet sieciowy. Po przeprowadzeniu pełnej penetracji komputera, jest on aktywowany.
P2P-Worm	Robaki sieci wymiany plików	Rozprzestrzeniają się one w sieciach peer-to-peer. Aby dostać się do sieci P2P, robak kopiuje się do foldera wymiany plików, który zazwyczaj znajduje się na komputerze użytkownika. Sieć P2P wyświetli informacje o tym pliku, aby użytkownik "znalazł" zainfekowany plik w sieci, pobrał go i otworzył. Bardziej zaawansowane robaki emulują protokół sieciowy konkretnej sieci P2P: wyświetlają pozytywne wyniki wyszukiwanego obiektu i proponują pobranie swoich własnych kopii.
Worm	Inne rodzaje robaków	Inne rodzaje robaków obejmują: • Robaki rozprzestrzeniające swoje kopie w zasobach sieciowych. Przy użyciu funkcji systemu operacyjnego skanują dostępne foldery sieciowe, łączą się z komputerami w Internecie i próbują uzyskać pełen dostęp do ich dysków. W przeciwieństwie do opisanych wyżej robaków, inne typy robaków nie aktywują się automatycznie, lecz w momencie, gdy użytkownik otworzy plik zawierający kopię robaka. • Robaki, które nie rozprzestrzeniają się w żaden z powyższych sposobów (na przykład te robaki, które rozprzestrzeniają się poprzez telefony komórkowe).

- **Trojany (w tym oprogramowanie typu ransomware)**

  Podkategoria: trojany

  Poziom zagrożenia: wysoki

W przeciwieństwie do wirusów i robaków, trojany nie tworzą swoich kopii. Przenikają one do komputera, na przykład, za pośrednictwem wiadomości e-mail lub przeglądarki internetowej po otwarciu zainfekowanej strony. Trojany uruchamiają się przy udziale użytkownika. Zaczynają wykonywać szkodliwe działania zaraz po uruchomieniu.

Różne programy typu trojan zachowują się odmiennie na zainfekowanych komputerach. Głównym zadaniem trojanów jest blokowanie, modyfikowanie lub niszczenie informacji, wyłączanie komputera lub sieci. Poza tym, trojany otrzymują lub wysyłają pliki, uruchamiają je, wyświetlają wiadomości na ekranie, pobierają i instalują aplikacje, uruchamiają ponownie komputer oraz żądają połączenia ze stroną internetową.

Hakerzy często używają "zestawów" trojanów.

Typowe zachowanie trojanów opisane jest w poniższej tabeli.

Typy zachowań trojanów na zainfekowanym komputerze

Typ	Nazwa	Opis
Trojan-ArcBomb	Trojany – "archiwa-bomby"	Archiwa, które po rozpakowaniu zwiększają swój rozmiar, co zakłóca działanie komputera. Podczas próby rozpakowania takiego archiwum komputer może spowolnić swoje działanie lub całkowicie się zawiesić, a dysk twardy może zostać wypełniony „pustymi" danymi. Archiwa-bomby są szczególnie niebezpieczne dla serwerów poczty i plików. Jeśli serwer korzysta z automatycznego systemu przetwarzania informacji przychodzących, archiwum-bomba może zatrzymać jego działanie.
Backdoor	Trojany do zdalnej administracji	Uważa się, że jest to najbardziej niebezpieczny rodzaj trojanów. Dzięki swoim funkcjom są one podobne do programów służących do zdalnej administracji aplikacji zainstalowanych na komputerach. Trojany instalują się na komputerze bez wiedzy użytkownika i pozwalają hakerowi na jego zdalne zarządzanie.
Trojan	Trojany	Do trojanów zaliczają się następujące szkodliwe aplikacji: • **Klasyczne trojany**. Wykonują tylko podstawowe funkcje charakterystyczne dla trojanów: blokują, modyfikują lub niszczą informacje, wyłączają komputery lub sieci. W odróżnieniu od trojanów opisanych w tabeli, nie charakteryzują się żadnymi zaawansowanymi funkcjami. • **Wszechstronne trojany**. Posiadają zaawansowane funkcje typowe dla kilku rodzajów trojanów.
Trojan-Ransom	Trojany przeznaczone do wyłudzania pieniędzy	Jako "zakładników" biorą one informacje użytkownika, modyfikują lub blokują je, albo tak wpływają na działanie komputera, że użytkownik nie może korzystać z informacji. Cyberprzestępca żąda okupu od użytkownika, obiecując, że wyśle aplikację, która przywróci działanie komputera oraz przechowywane na nim dane.
Trojan-Clicker	Trojany klikające	Łączą się one ze stronami internetowymi albo przez wysłanie polecenia do przeglądarki albo przez zmianę adresów stron znajdujących się w plikach systemowych. Przy użyciu tych programów hakerzy przeprowadzają ataki sieciowe i zwiększają ranking stron internetowych celem zwiększenia liczby wyświetlania banerów reklamowych.
Trojan-Downloader	Trojany pobierające	Uzyskują dostęp do strony internetowej cyberprzestępcy, pobierają z niej szkodliwe aplikacje i instalują je na komputerze użytkownika. Mogą zawierać nazwę pliku szkodliwej aplikacji do pobrania lub uzyskać ją z otwartej strony internetowej.
Trojan-Dropper	Trojany droppery	Zawierają inne trojany, które instalują na dysku twardym. Hakerzy mogą użyć tego typu trojanów do następujących celów: • Instalacji szkodliwej aplikacji w sposób niezauważalny dla użytkownika: Trojan-Dropper to typ programów, które nie wyświetlają żadnych wiadomości lub wyświetlają fałszywe komunikaty informujące, na przykład, o błędzie w archiwum lub niekompatybilnej wersji systemu operacyjnego. • Ochrony innych znanych szkodliwych aplikacji przed wykryciem przez ochronę komputera: nie wszystkie programy antywirusowe są w stanie wykryć szkodliwą aplikację wewnątrz aplikacji Trojan-Dropper.
Trojan-Notifier	Trojany powiadamiające	Informują cyberprzestępcę o możliwości dostępu do zainfekowanego komputera, wysyłając do niego informacje o tym komputerze: adres IP, numer otwartego portu lub adres e-mail. Komunikują się z hakerem, na przykład, za pośrednictwem wiadomości e-mail, serwera FTP lub jego strony internetowej. Trojany typu Notifier często są wykorzystywane w zestawach złożonych z kilku trojanów. Powiadamiają one hakera, że inne trojany zostały pomyślnie zainstalowane na komputerze użytkownika.
Trojan-Proxy	Trojany proxy	Umożliwiają one hakerowi uzyskanie anonimowego dostępu do stron internetowych przy użyciu komputera użytkownika i są często używane do wysyłania spamu.
Trojan-PSW	Oprogramowanie kradnące hasła	Oprogramowanie kradnące hasła to rodzaj trojanów kradnących konta użytkownika, na przykład dane rejestracyjne oprogramowania. Takie trojany odnajdują w plikach systemowych i rejestrze poufne dane, a następnie wysyłają je do atakującego, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej. Niektóre z tych trojanów podzielone są na kategorie oddzielnych typów opisanych w tej tabeli. Należą do nich Trojany kradnące konta bankowe (Trojan-Banker), trojany kradnące informacje od użytkowników komunikatorów internetowych (Trojan-IM) oraz trojany kradnące informacje od graczy online (Trojan-GameThief).
Trojan-Spy	Trojany szpiegujące	Szpiegują one użytkownika, zbierając informacje o jego działaniach podczas pracy na komputerze. Mogą przechwytywać dane wprowadzane przez użytkownika przy użyciu klawiatury, tworzyć zrzuty ekranu lub tworzyć listę aktywnych aplikacji. Po zebraniu informacji, wysyłają je do hakera, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.
Trojan-DDoS	Ataki sieciowe przez trojany	Wysyłają one liczne żądania z komputera użytkownika na serwer zdalny. Serwer nie ma wystarczającej ilości zasobów do przetworzenia wszystkich żądań, w rezultacie przestaje działać (Denial-of-Service lub DoS). Hakerzy często infekują wiele komputerów dzięki takim programom, przez co mogą wykorzystać te komputery do jednoczesnego ataku na pojedynczy serwer. Programy DoS przeprowadzają atak z jednego komputera za wiedzą użytkownika. Programy DDoS (Distributed DoS) przeprowadzają rozproszone ataki z różnych komputerów bez wiedzy użytkownika zainfekowanego komputera.
Trojan-IM	Trojany kradnące informacje od użytkowników komunikatorów internetowych	Kradną numery kont i hasła użytkowników klientów komunikatorów internetowych. Przesyłają dane hakerowi, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.
Rootkit	Rootkity	Ukrywają inne szkodliwe aplikacje i ich aktywność, przedłużając ich obecność w systemie. Mogą również ukrywać pliki i procesy w pamięci zainfekowanego komputera lub kluczach rejestru. Rootkity mogą ukrywać wymianę danych pomiędzy aplikacjami znajdującymi się na komputerze użytkownika i innymi komputerami podłączonymi do sieci.
Trojan-SMS	Trojany wysyłające wiadomości SMS	Infekują one telefony komórkowe, wysyłając wiadomości SMS na numery o podwyższonej opłacie.

Trojan-GameThief	Trojany kradnące informacje od osób grających w sieci	Kradną dane uwierzytelniające kont osób grających w sieci, po czym wysyłają je hakerowi za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.
Trojan-Banker	Trojany kradnące konta bankowe	Kradną dane konta bankowego lub dane systemu płatności elektronicznych, po czym wysyłają je cyberprzestępcy za pośrednictwem poczty elektronicznej, serwera FTP, jego strony internetowej lub przy użyciu innych metod.
Trojan-Mailfinder	Trojany zbierające adresy e-mail	Zbierają one adresy e-mail przechowywane na komputerze i wysyłają je hakerowi, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej. Na zebrane adresy hakerzy mogą wysyłać spam.

- **Szkodliwe narzędzia**

  Podkategoria: szkodliwe narzędzia

  Poziom zagrożenia: Średni

  W odróżnieniu od innych typów szkodliwego oprogramowania, szkodliwe narzędzia nie wykonują swoich akcji zaraz po uruchomieniu. Mogą być bezpiecznie przechowywane i uruchamiane na komputerze użytkownika. Hakerzy często używają funkcji tych programów do tworzenia wirusów, robaków i trojanów oraz do przeprowadzania ataków sieciowych na serwery zdalne, łamania zabezpieczeń komputerów lub wykonywania innych szkodliwych działań.

  Różne funkcje szkodliwych narzędzi pogrupowane są według typów opisanych w poniższej tabeli.

  Funkcje szkodliwych narzędzi

Typ	Nazwa	Opis
Constructor	Konstruktory	Umożliwiają utworzenie nowych wirusów, robaków i trojanów. Niektóre konstruktory posiadają standardowy interfejs oparty na oknach, w którym użytkownik może wybrać typ szkodliwej aplikacji, jaki chce stworzyć, sposób przeciwdziałania debuggerom oraz inne funkcje.
Dos	Ataki sieciowe	Wysyłają one liczne żądania z komputera użytkownika na serwer zdalny. Serwer nie ma wystarczającej ilości zasobów do przetworzenia wszystkich żądań, w rezultacie przestaje działać (Denial-of-Service lub DoS).
Exploit	Exploity	*Exploit* jest zestawem danych lub kodem programu używającym luki aplikacji, w której jest przetwarzany, do wykonania szkodliwych działań na komputerze. Na przykład, exploit może odczytywać lub zapisywać pliki lub uzyskiwać dostęp do „zainfekowanych" stron internetowych. Różne exploity używają luk w różnych aplikacjach lub usługach sieciowych. Wyglądający jak pakiet sieciowy exploit wysyłany jest przez sieć w poszukiwaniu takich komputerów, których usługi sieciowe posiadają luki. Exploit w pliku DOC używa luk występujących w edytorach tekstu. Po otwarciu przez użytkownika zainfekowanego pliku, może on zacząć wykonywać zaprogramowane przez hakera działania. Exploit osadzony w wiadomości elektronicznej wyszukuje luki w dowolnym kliencie pocztowym. Po otwarciu przez użytkownika zainfekowanego pliku w tym programie pocztowym, wykonuje on szkodliwe działanie. Robaki Net-Worms rozprzestrzeniają się w sieci przy pomocy exploitów. Exploity Nuker są pakietami sieciowymi wyłączającymi komputery.
FileCryptor	Narzędzia szyfrujące	Szyfrują one inne szkodliwe aplikacje, aby ukryć je przed programem antywirusowym.
Flooder	Programy „zaśmiecające" sieci	Wysyłają one wiele wiadomości przez kanały sieciowe. Do tego typu narzędzi należy, na przykład, program zaśmiecający Internet Relay Chats (IRC). Wśród narzędzi typu Flooder nie ma programów "zaśmiecających" kanały używane przez programy pocztowe, komunikatory internetowe i systemy komunikacji mobilnej. Programy te wyróżnione są jako oddzielne typy opisane w tej tabeli (Email-Flooder, IM-Flooder oraz SMS-Flooder).
HackTool	Narzędzia hakerskie	Pozwalają na złamanie zabezpieczeń komputera, na którym są zainstalowane, lub na zaatakowanie innego komputera (na przykład, dodając nowe konta systemowe bez wiedzy użytkownika lub wymazując logi systemowe, aby ukryć ślady obecności w systemie operacyjnym). Ten typ narzędzi zawiera sniffery posiadające szkodliwe funkcje, jak choćby przechwytywanie haseł. Sniffery to programy umożliwiające przeglądanie ruchu sieciowego.
Hoax	Żarty (Hoaxes)	Alarmują użytkownika przy użyciu wiadomości podobnej do tej, która używana jest w przypadku wykrycia wirusa: mogą "wykryć wirusa" w nienaruszonym pliku lub powiadomić o formatowaniu dysku, które w rzeczywistości nie ma miejsca.
Spoofer	Narzędzia służące do spoofingu	Wysyłają wiadomości i żądania sieciowe z fałszywym adresem nadawcy. Hakerzy używają narzędzi do spoofingu, na przykład, aby móc podać się za prawdziwych nadawców wiadomości.
VirTool	Narzędzia do modyfikowania szkodliwych aplikacji	Umożliwiają modyfikowanie innego szkodliwego oprogramowania w celu ukrycia go przed aplikacjami antywirusowymi.
Email-Flooder	Programy „zaśmiecające" adresy e-mail	„Zaśmiecają" różne adresy e-mail poprzez wysyłanie na nie licznych wiadomości. Duża liczba wiadomości przychodzących uniemożliwia przejrzenie użytecznych wiadomości znajdujących się w skrzynce odbiorczej.
IM-Flooder	Programy „zaśmiecające" ruch wiadomościami klientów komunikatorów internetowych	Wysyłają niechciane wiadomości do użytkowników klientów komunikatorów. Duża liczba odbieranych wiadomości uniemożliwia przeczytanie użytecznych wiadomości.
SMS-Flooder	Programy „zaśmiecające" ruch wiadomościami SMS	Wysyłają one liczne wiadomości SMS na telefony komórkowe.

- **Adware**

  Podkategoria: oprogramowanie reklamujące (adware)

  Poziom zagrożenia: Średni

  Oprogramowanie Adware wyświetla informacje reklamowe użytkownikowi. Programy adware wyświetlają banery reklamowe w interfejsach innych programów i przekierowują wyszukiwanie na strony reklamowe. Niektóre z nich zbierają informacje marketingowe o użytkowniku i wysyłają je do programisty. Do gromadzonych informacji mogą należeć: nazwy stron odwiedzanych przez użytkownika lub wyszukiwana przez niego treść. W odróżnieniu od programów typu Trojan-Spy, programy adware przesyłają te informacje do twórcy za zgodą użytkownika.

- **Auto-dialery**

  Podkategoria: Legalne oprogramowanie, które może zostać wykorzystane przez przestępców do uszkodzenia komputera i prywatnych danych.

  Poziom zagrożenia: Średni

  Wiele z tych programów to nieszkodliwe oprogramowanie, z którego korzysta wielu użytkowników. Do tych programów zaliczają się: klienty IRC, auto-dialery, programy pobierające pliki, monitory aktywności systemu komputerowego, narzędzia do haseł, serwery usług FTP, HTTP i Telnet.

  Jednakże, jeśli haker uzyska dostęp do tego typu programów lub jeśli zainstaluje te programy na komputerze użytkownika, to niektóre z ich funkcji mogą zostać użyte do naruszenia ochrony.

  Aplikacje te mają różne funkcje; ich typy zostały opisane w poniższej tabeli.

Typ	Nazwa	Opis
Client-IRC	Klienty czatów internetowych	Użytkownicy instalują programy tego typu, aby móc rozmawiać z innymi w czasie rzeczywistym. Hakerzy używają ich do rozsyłania szkodliwych programów.
Downloader	Programy do pobierania	Mogą pobierać pliki ze stron internetowych w trybie ukrycia.
Monitor	Programy do monitorowania	Umożliwiają monitorowanie aktywności na komputerze, na którym są zainstalowane (sprawdzają, które aplikacje są aktywne i w jaki sposób wymieniają dane z aplikacjami zainstalowanymi na innych komputerach).
PSWTool	Programy do przywracania haseł	Umożliwiają przeglądanie i przywracanie zapomnianych haseł. Hakerzy umieszczają je na komputerze w tym samym celu, w sposób niezauważalny dla użytkownika.
RemoteAdmin	Programy do zdalnej administracji	Są używane przez administratorów systemów. Programy te pozwalają uzyskać dostęp do interfejsu zdalnego komputera w celu jego monitorowania i zarządzania. W tym właśnie celu hakerzy niezauważenie umieszczają je na komputerze użytkownika. Legalne programy do zdalnej administracji różnią się od trojanów typu backdoor do zdalnej administracji. Trojany potrafią niezależnie spenetrować system i zainstalować się; legalne programy nie potrafią tego.
Server-FTP	Serwery FTP	Działają jak serwery FTP. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu FTP.
Server-Proxy	Serwery proxy	Działają jak serwery proxy. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
Server-Telnet	Serwery Telnet	Działają jak serwery Telnet. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu Telnet.
Server-Web	Serwery sieciowe	Działają jak serwery sieciowe. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu HTTP.
RiskTool	Narzędzia wykorzystywane do pracy na lokalnym komputerze	Umożliwiają one użytkownikowi korzystanie z dodatkowych funkcji podczas jego pracy na komputerze. Narzędzia te pozwalają użytkownikowi ukryć pliki lub okna uruchomionych aplikacji i zakończyć aktywne procesy.
NetTool	Narzędzia sieciowe	Umożliwiają użytkownikowi korzystanie z dodatkowych funkcji podczas pracy z innymi komputerami w sieci. Posiadają one także możliwość ich ponownego uruchomienia, wykrywania otwartych portów oraz uruchamiania aplikacji zainstalowanych na komputerach.
Client-P2P	Klienty sieciowe P2P	Pozwalają pracować w sieciach peer-to-peer. Mogą być wykorzystywane przez hakerów do rozprzestrzeniania szkodliwego oprogramowania.
Client-SMTP	Klienty SMTP	Wysyłają wiadomości e-mail bez wiedzy użytkownika. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
WebToolbar	Paski narzędzi w przeglądarkach internetowych	Dodają one paski narzędzi w interfejsie innych aplikacji umożliwiające korzystanie z wyszukiwarek internetowych.
FraudTool	Pseudo-programy	Podają się za inne programy. Na przykład, istnieją fałszywe programy antywirusowe, które wyświetlają wiadomości o wykryciu szkodliwego oprogramowania. W rzeczywistości nie skanują ani nie leczą niczego.

- **Legalne oprogramowanie, które może zostać wykorzystane przez intruzów do uszkodzenia komputera lub prywatnych danych**

  Podkategoria: Legalne oprogramowanie, które może zostać wykorzystane przez przestępców do uszkodzenia komputera i prywatnych danych.

  Poziom zagrożenia: Średni

  Wiele z tych programów to nieszkodliwe oprogramowanie, z którego korzysta wielu użytkowników. Do tych programów zaliczają się: klienty IRC, auto-dialery, programy pobierające pliki, monitory aktywności systemu komputerowego, narzędzia do haseł, serwery usług FTP, HTTP i Telnet.

  Jednakże, jeśli haker uzyska dostęp do tego typu programów lub jeśli zainstaluje te programy na komputerze użytkownika, to niektóre z ich funkcji mogą zostać użyte do naruszenia ochrony.

  Aplikacje te mają różne funkcje; ich typy zostały opisane w poniższej tabeli.

Typ	Nazwa	Opis
Client-IRC	Klienty czatów internetowych	Użytkownicy instalują programy tego typu, aby móc rozmawiać z innymi w czasie rzeczywistym. Hakerzy używają ich do rozsyłania szkodliwych programów.

Downloader	Programy do pobierania	Mogą pobierać pliki ze stron internetowych w trybie ukrycia.
Monitor	Programy do monitorowania	Umożliwiają monitorowanie aktywności na komputerze, na którym są zainstalowane (sprawdzają, które aplikacje są aktywne i w jaki sposób wymieniają dane z aplikacjami zainstalowanymi na innych komputerach).
PSWTool	Programy do przywracania haseł	Umożliwiają przeglądanie i przywracanie zapomnianych haseł. Hakerzy umieszczają je na komputerze w tym samym celu, w sposób niezauważalny dla użytkownika.
RemoteAdmin	Programy do zdalnej administracji	Są używane przez administratorów systemów. Programy te pozwalają uzyskać dostęp do interfejsu zdalnego komputera w celu jego monitorowania i zarządzania. W tym właśnie celu hakerzy niezauważenie umieszczają je na komputerze użytkownika. Legalne programy do zdalnej administracji różnią się od trojanów typu backdoor do zdalnej administracji. Trojany potrafią niezależnie spenetrować system i zainstalować się; legalne programy nie potrafią tego.
Server-FTP	Serwery FTP	Działają jak serwery FTP. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu FTP.
Server-Proxy	Serwery proxy	Działają jak serwery proxy. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
Server-Telnet	Serwery Telnet	Działają jak serwery Telnet. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu Telnet.
Server-Web	Serwery sieciowe	Działają jak serwery sieciowe. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu HTTP.
RiskTool	Narzędzia wykorzystywane do pracy na lokalnym komputerze	Umożliwiają one użytkownikowi korzystanie z dodatkowych funkcji podczas jego pracy na komputerze. Narzędzia te pozwalają użytkownikowi ukryć pliki lub okna uruchomionych aplikacji i zakończyć aktywne procesy.
NetTool	Narzędzia sieciowe	Umożliwiają użytkownikowi korzystanie z dodatkowych funkcji podczas pracy z innymi komputerami w sieci. Posiadają one także możliwość ich ponownego uruchomienia, wykrywania otwartych portów oraz uruchamiania aplikacji zainstalowanych na komputerach.
Client-P2P	Klienty sieciowe P2P	Pozwalają pracować w sieciach peer-to-peer. Mogą być wykorzystywane przez hakerów do rozprzestrzeniania szkodliwego oprogramowania.
Client-SMTP	Klienty SMTP	Wysyłają wiadomości e-mail bez wiedzy użytkownika. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
WebToolbar	Paski narzędzi w przeglądarkach internetowych	Dodają one paski narzędzi w interfejsie innych aplikacji umożliwiające korzystanie z wyszukiwarek internetowych.
FraudTool	Pseudo-programy	Podają się za inne programy. Na przykład, istnieją fałszywe programy antywirusowe, które wyświetlają wiadomości o wykryciu szkodliwego oprogramowania. W rzeczywistości nie skanują ani nie leczą niczego.

- **Obiekty spakowane, których archiwizacja może być używana do ochrony szkodliwego kodu**

  Podkategoria: Spakowane pliki, które mogą wyrządzić szkody.

  Poziom zagrożenia: Średni.

  Plik pakowany jest za pomocą specjalnego narzędzia pakującego, które służy do pakowania złośliwego oprogramowania: wirusów, robaków i trojanów. Kaspersky Endpoint Security skanuje moduł wypakowujący znajdujący się w archiwach SFX (samorozpakowujących się).

  Aby uniemożliwić wykrycie złośliwego oprogramowania przez oprogramowanie antywirusowe, hakerzy pakują je za pomocą specjalnych programów pakujących. Eksperci firmy Kaspersky zidentyfikowali narzędzia pakujące najpopularniejsze wśród hakerów.

- **Obiekty spakowane wielokrotnie**

  Podkategoria: Spakowane pliki, które mogą wyrządzić szkody.

  Poziom zagrożenia: Średni.

  Plik pakowany jest za pomocą specjalnego narzędzia pakującego, które służy do pakowania złośliwego oprogramowania: wirusów, robaków i trojanów. Kaspersky Endpoint Security skanuje moduł wypakowujący znajdujący się w archiwach SFX (samorozpakowujących się).

  Aby uniemożliwić wykrycie złośliwego oprogramowania przez oprogramowanie antywirusowe, hakerzy pakują je za pomocą specjalnych programów pakujących. Eksperci firmy Kaspersky zidentyfikowali narzędzia pakujące najpopularniejsze wśród hakerów.

Wykluczenia

Ta tabela zawiera informacje o wykluczeniach ze skanowania.

Zalecamy określanie ścieżek względnych zamiast ścieżek bezwzględnych. Dzięki temu można wykluczać nie tylko obiekty systemu plików, ale także obiekty bezplikowe. Na przykład, `*\Program Files (x86)\Folder\Subfolder`.

Możliwe jest wykluczenie obiektów ze skanowania przy użyciu następujących metod:

- Określ ścieżkę do pliku lub folderu.
- Wprowadź sumę kontrolną obiektu.

- Użyj masek:
  - Znak `*` (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\*\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
  - Dwa występujące po sobie znaki `*` zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład maska `C:\Folder\**\*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maska musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maska `C:\**\*.txt` nie jest ważną maską.
  - Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

    W dowolnym miejscu ścieżki pliku lub folderu można używać masek. Na przykład, jeśli chcesz, aby zakres skanowania obejmował folder Pobrane dla wszystkich kont użytkowników na komputerze, należy wprowadzić maskę `C:\Users\*\Downloads\`.

    Kaspersky Endpoint Security obsługuje zmienne środowiskowe

    > Kaspersky Endpoint Security nie obsługuje zmiennej środowiskowej `%userprofile%` podczas generowania listy wykluczeń za pomocą konsoli Kaspersky Security Center. Aby zastosować wpis do wszystkich kont użytkowników, możesz użyć znaku * (na przykład: `C:\Users\*\Documents\File.exe`). Za każdym razem, gdy dodajesz nową zmienną środowiskową, musisz uruchomić aplikację ponownie.

- Wprowadź nazwę typu obiektu zgodnie z klasyfikacją Encyklopedii Kaspersky (na przykład: `Email-Worm`, `Rootkit` lub `RemoteAdmin`). Możesz użyć masek ze znakiem `?` (zastępuje dowolny pojedynczy znak) oraz znak `*` (zastępuje dowolną liczbę znaków). Na przykład, jeśli określona jest maska `Client*`, aplikacja wyklucza obiekty `Client-IRC`, `Client-P2P` i `Client-SMTP` ze skanowania.

> Kaspersky Endpoint Security ukrywa listę wykluczeń ze skanowania w interfejsie użytkownika aplikacji, jeśli konfiguracja wykluczeń ze skanowania została zablokowana przez administratora w konsoli (symbol „zamkniętej kłódki"), a wykluczenia ze skanowania lokalnego są zabronione (pole wyboru **Zezwól na korzystanie z lokalnych wykluczeń** jest odznaczone).

Zaufane aplikacje

Ta tabela wyświetla zaufane aplikacje, których aktywność nie jest monitorowana przez Kaspersky Endpoint Security w trakcie działania.

Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.

> Kaspersky Endpoint Security nie obsługuje zmiennej środowiskowej `%userprofile%` podczas generowania listy zaufanych aplikacji w konsoli Kaspersky Security Center. Aby zastosować wpis do wszystkich kont użytkowników, możesz użyć znaku * (na przykład: `C:\Users\*\Documents\File.exe`). Za każdym razem, gdy dodajesz nową zmienną środowiskową, musisz uruchomić aplikację ponownie.

Komponent Kontrola aplikacji reguluje uruchamianie każdej aplikacji niezależnie od tego, czy aplikacja znajduje się w tabeli zaufanych aplikacji.

> Kaspersky Endpoint Security ukrywa skonsolidowaną listę zaufanych aplikacji w interfejsie użytkownika aplikacji, jeśli konfiguracja zaufanych aplikacji została zablokowana przez administratora w konsoli (symbol „zamkniętej kłódki"), a lokalne zaufane aplikacje są zabronione (pole wyboru **Zezwól na korzystanie z lokalnych zaufanych aplikacji** jest odznaczone).

Przenieś wartości podczas dziedziczenia *(dostępny tylko w Kaspersky Security Center Console)*	To powoduje scalenie listy wykluczeń ze skanowania i zaufanych aplikacji w zasadach nadrzędnych i potomnych programu Kaspersky Security Center. Aby scalić listy, zasada potomna musi być skonfigurowana do dziedziczenia ustawień zasady nadrzędnej programu Kaspersky Security Center. Jeśli pole jest zaznaczone, w zasadach potomnych wyświetlane są elementy listy z zasady nadrzędnej Kaspersky Security Center. W ten sposób możesz, na przykład, utworzyć skonsolidowaną listę zaufanych aplikacji dla całej organizacji. Dziedziczone elementy listy w zasadzie potomnej nie mogą zostać usunięte ani edytowane. Elementy na liście wykluczeń ze skanowania oraz lista zaufanych aplikacji, które są scalone podczas dziedziczenia, mogą zostać usunięte i edytowane tylko w zasadzie nadrzędnej. Możesz dodawać, edytować lub usuwać elementy z list w zasadach niższego poziomu. Jeśli elementy na listach zasady potomnej i nadrzędnej pasują do siebie, te elementy są wyświetlane jak podobne elementy zasady nadrzędnej. Jeśli pole nie zostało zaznaczone, elementy z list nie są scalane podczas dziedziczenia ustawień zasad programu Kaspersky Security Center. Ta funkcja umożliwia również scalanie list w profilach zasad. Aby scalić listy, w profilu o najwyższym priorytecie należy włączyć dziedziczenie ustawień z profilu o niższym priorytecie. Aby uzyskać szczegółowe informacje na temat priorytetów profilu zasady, zapoznaj się z pomocą do Kaspersky Security Center.
Zezwól na korzystanie z lokalnych wykluczeń / Zezwól na korzystanie z lokalnych zaufanych aplikacji *(dostępny tylko w Kaspersky Security Center Console)*	*Lokalne wykluczenia i lokalne zaufane aplikacje (lokalna strefa zaufana)* – lista obiektów i aplikacji zdefiniowana przez użytkownika w Kaspersky Endpoint Security dla określonego komputera. Kaspersky Endpoint Security nie monitoruje obiektów i aplikacji z lokalnej strefy zaufanej. W ten sposób użytkownicy mogą utworzyć swoje własne lokalne listy wykluczeń i zaufanych aplikacji jako dodatek do ogólnej strefy zaufanej w zasadzie. Jeśli pole jest zaznaczone, użytkownik może utworzyć lokalną listę wykluczeń skanowania i lokalnej listy zaufanej aplikacji. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera. Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnych list wykluczeń ze skanowania i zaufanych aplikacji, wygenerowanych w zasadzie.
Telemetria EDR (KATA) / NDR (KATA) *(dostępny tylko w Kaspersky Security Center Console)*	Ta tabela zawiera informacje o wykluczeniach telemetrii EDR.
Telemetria KUMA *(dostępny tylko w Kaspersky Security Center Console)*	Lista zdarzeń, które mają zostać wysłane do Kaspersky Unified Monitoring and Analysis Platform (KUMA). Kaspersky Endpoint Security działa w następujących trybach: • **Wyślij wszystkie zdarzenia**. W tym trybie aplikacja wysyła wszystkie zdarzenia z dziennika systemu Windows, z wyjątkiem zdarzeń dodanych do reguł wykluczania. • **Wyślij tylko wybrane zdarzenia**. W tym trybie aplikacja wysyła tylko zdarzenia dodane w regułach włączania.
Magazyn zaufanych certyfikatów systemowych	Jeśli wybrano jeden z zaufanych magazynów certyfikatów systemowych, Kaspersky Endpoint Security wyklucza ze skanowania aplikacje posiadające zaufany podpis cyfrowy. Kaspersky Endpoint Security automatycznie przypisze takie aplikacje do grupy **Zaufane**. Jeśli wybrano **Nie używaj**, Kaspersky Endpoint Security skanuje aplikacje niezależnie od tego, czy posiadają podpis cyfrowy. Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera.

Ustawienia aplikacji

Możesz skonfigurować następujące ogólne ustawienia aplikacji:

- Tryb działania
- Autoochrona
- Wydajność
- Informacje debugowania
- Stan komputera po zastosowaniu ustawień

Parametr	Opis
Uruchom aplikację przy uruchomieniu komputera (zalecane)	Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security uruchamia się po załadowaniu systemu operacyjnego, chroniąc komputer w trakcie całej sesji. Jeśli opcja nie jest zaznaczona, Kaspersky Endpoint Security nie uruchamia się po załadowaniu systemu operacyjnego, dopóki użytkownik nie włączy go ręcznie. Ochrona komputera jest wyłączona, a dane użytkownika mogą być narażone na zagrożenia.
Użyj technologii zaawansowanego leczenia (wymaga znacznych zasobów komputera)	Zazwyczaj Kaspersky Endpoint Security usuwa wykryte złośliwe oprogramowanie zanim komputer zostanie zainfekowany. Technologia zaawansowanego leczenia chroni komputer przed aktywnym złośliwym oprogramowaniem (aktywną infekcją), minimalizując w ten sposób ryzyko utraty danych i rozprzestrzeniania się zagrożenia. Jeśli technologia ta jest włączona, po wykryciu szkodliwej aktywności Kaspersky Endpoint Security wyświetla powiadomienie w oknie wyskakującym. W tym komunikacie Kaspersky Endpoint Security zaoferuje użytkownikowi przeprowadzenie zaawansowanego leczenia komputera. Jeśli użytkownik wyrazi zgodę na zastosowanie tej procedury, Kaspersky Endpoint Security zneutralizuje to zagrożenie i zrestartuje komputer. Technologia zaawansowanego leczenia wykorzystuje dużą ilość zasobów komputera, co może spowolnić inne aplikacje. Jeśli aplikacja jest w trakcie wykrywania aktywnej infekcji, niektóre funkcje systemu mogą być niedostępne. Dostępność systemu operacyjnego jest przywracana, gdy Zaawansowane leczenie zostanie zakończone, a komputer zostanie uruchomiony ponownie. Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows przeznaczonego dla serwerów, Kaspersky Endpoint Security nie wyświetli komunikatu. Dlatego nie możesz wybrać działania wyleczenia aktywnego zagrożenia. Aby wyleczyć zagrożenie, musisz włączyć technologię zaawansowanego leczenia w ustawieniach aplikacji oraz natychmiast włączyć Zaawansowane leczenie w ustawieniach zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Następnie musisz uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.
Użyj Kaspersky Security Center jako serwera proxy do aktywacji *(dostępny tylko w Kaspersky Security Center Console)*	Jeśli to pole wyboru jest zaznaczone, aplikacja używa Serwera administracyjnego Kaspersky Security Center jako serwera proxy do łączenia się z serwerami aktywacji. Jest to konieczne, jeśli używasz kodu aktywacyjnego do aktywacji aplikacji w izolowanym segmencie sieci bez dostępu do Internetu. Jeśli aktywujesz aplikację za pomocą pliku klucza, dostęp do Internetu nie jest konieczny.
Włącz Autoochronę	Jeśli ta funkcjonalność jest włączona, Kaspersky Endpoint Security zapobiega zmianom lub usuwaniu procesów pamięci, plików aplikacji na dysku twardym oraz wpisów w rejestrze systemowym.
Blokuj zewnętrzne zarządzanie usługami aplikacji	Jeśli ta funkcjonalność jest włączona, Kaspersky Endpoint Security nie zezwala na zarządzanie usługami aplikacji przy użyciu aplikacji innych firm (takich jak CMD). Przy próbie zarządzania usługami aplikacji za pomocą aplikacji innych firm wyświetlane jest powiadomienie na pasku zadań Microsoft Windows, nad ikoną aplikacji (chyba, że usługa powiadomień została wyłączona przez użytkownika). Zezwalać na zewnętrzne zarządzanie usługami aplikacji można tylko na komputerach, które nie obsługują technologii AM-PPL lub na komputerach, na których wyłączono tę technologię.
Odrocz zaplanowane zadania podczas pracy na bateriach	Jeżeli to pole wyboru jest zaznaczone, tryb oszczędzania energii jest włączony podczas zasilania komputera z baterii. Kaspersky Endpoint Security odroczy zaplanowane zadania. W razie konieczności zadania skanowania i aktualizacji mogą zostać uruchomione ręcznie. Gdy tryb oszczędzania energii jest włączony, a komputer działa na bateriach, następujące zadania nie są uruchamiane, nawet jeśli zostały zaplanowane: • *Pełne skanowanie* • *Skanowanie obszarów krytycznych* • *Skanowanie niestandardowe* • *Sprawdzanie integralności aplikacji* • *Skanowanie IOC* • *Aktualizacja baz danych i modułów aplikacji* (tylko poprawki) Aplikacja pomija zaplanowane aktualizacje bazy danych tylko wtedy, gdy laptop jest zasilany z baterii, a poziom naładowania baterii wynosi poniżej 30%. We wszystkich pozostałych przypadkach Kaspersky Endpoint Security aktualizuje bazy danych zgodnie z harmonogramem, niezależnie od tego, czy laptop jest podłączony do zasilania, czy działa na zasilaniu bateryjnym, a także czy aplikacja działa w trybie oszczędzania energii.

Parametr	Opis
Udostępniaj zasoby innym aplikacjom	Zużycie zasobów komputera przez Kaspersky Endpoint Security podczas skanowania komputera może zwiększyć obciążenie podsystemów procesora i dysku twardego. Może to spowolnić działanie innych aplikacji. Aby zoptymalizować wydajność, Kaspersky Endpoint Security zapewnia *tryb przenoszenia zasobów do innych aplikacji*. W tym trybie system operacyjny może zmniejszyć priorytet wątków zadania skanowania Kaspersky Endpoint Security, gdy obciążenie procesora jest wysokie. Pozwala to na redystrybucję zasobów systemu operacyjnego do innych aplikacji. W ten sposób zadania skanowania otrzymają mniej czasu pracy procesora. W rezultacie Kaspersky Endpoint Security będzie potrzebował więcej czasu na przeskanowanie komputera. Domyślnie aplikacja udostępnia zasoby innym aplikacjom.
Ogranicz użycie procesora do zadań skanowania	Aby zoptymalizować wydajność Kaspersky Endpoint Security, możesz ograniczyć użycie procesora za pomocą zadania *Skanowanie w poszukiwaniu złośliwego oprogramowania*. Jeżeli pole wyboru jest zaznaczone, średnie obciążenie wszystkich rdzeni procesora przez zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* zbliża się do określonej wartości. Domyślnie to pole wyboru nie jest zaznaczone.
Włącz zapisywanie zrzutów pamięci	Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security zapisuje pliki zrzutu w momencie awarii. Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security nie zapisuje plików zrzutu. Aplikacja także usuwa istniejące pliki zrzutu z dysku twardego komputera.
Włącz ochronę zrzutów pamięci i plików śledzenia	Jeśli pole jest zaznaczone, dostęp do plików zrzutów pamięci jest udzielany systemowemu administratorowi i lokalnemu administratorowi, jak również użytkownikowi, który włączył zapis zrzutów pamięci. Tylko systemowi bądź lokalni administratorzy mają dostęp do plików śledzenia. Jeśli pole jest odznaczone, żaden użytkownik nie ma dostępu do plików zrzutów pamięci i plików śledzenia.
Stan komputera po zastosowaniu ustawień *(dostępny tylko w Kaspersky Security Center Console)*	Ustawienia wyświetlania stanów komputerów klienckich z zainstalowanym programem Kaspersky Endpoint Security w Web Console, gdy podczas stosowania profilu lub wykonywania zadania wystąpią błędy. Dostępne są następujące stany: *OK*, *Ostrzeżenie* i *Krytyczny*.
Zainstaluj aktualizacje bez restartu komputera	Aktualizacja aplikacji bez ponownego uruchamiania komputera pozwala zapewnić nieprzerwaną pracę serwerów. Począwszy od wersji 11.10.0 możesz aktualizować aplikację bez konieczności ponownego uruchamiania. Aby zaktualizować wcześniejszą wersję aplikacji, musisz ponownie uruchomić komputer. Od wersji 11.11.0 możesz wykonywać następujące czynności bez ponownego uruchamiania komputera: • instalacja poprawek • zmiana zestawu komponentów aplikacji • instalacja Kaspersky Endpoint Security zamiast Kaspersky Security for Windows Server Domyślna wartość parametru zależy od typu systemu operacyjnego. Jeśli aplikacja zostanie zainstalowana na stacji roboczej, opcja aktualizacji aplikacji bez ponownego uruchomienia jest wyłączona. Jeśli aplikacja zostanie zainstalowana na serwerze, opcja aktualizacji aplikacji bez ponownego uruchomienia jest włączona.
Zgodność z oprogramowaniem do zdalnej administracji *(dostępny tylko w Kaspersky Security Center Console)*	Jeśli używanie Kaspersky Endpoint Security wraz z narzędziami administracji zdalnej (RAT) powoduje problemy, możesz włączyć tryb zgodności. Problemy mogą być związane z niekompatybilnością narzędzi zdalnych RAT z funkcją Secure Desktop aplikacji. Celem tej funkcjonalności jest potwierdzanie działań, które mogą potencjalnie obniżyć poziom bezpieczeństwa komputera. Ta funkcja umożliwia aplikacji wyświetlenie okna dialogowego potwierdzenia odizolowanego od innych procesów. Ta funkcja korzysta z podwyższonych uprawnień w celu zabezpieczenia żądania. W ten sposób tylko użytkownik może potwierdzić działanie, a nie złośliwe oprogramowanie. Jeżeli opcja jest zaznaczona, zostanie włączony tryb kompatybilności RAT. Aplikacja wyświetla okno dialogowe z potwierdzeniem bez tej funkcji. Może to spowodować spadek poziom bezpieczeństwa komputera. Nie zalecamy włączania trybu zgodności, jeśli Kaspersky Endpoint Security nie powoduje problemów z narzędziami RAT użytkownika. Jeżeli opcja nie jest zaznaczona, tryb kompatybilności RAT zostanie wyłączony. Domyślnie to pole wyboru nie jest zaznaczone. Przykład: Podczas korzystania z przeglądarki w trybie RemoteApp Kaspersky Endpoint Security może nie wyświetlać okna potwierdzenia podczas odwiedzania strony internetowej z niezaufanym certyfikatem, ponieważ RemoteApp nie obsługuje funkcjonalności Bezpiecznego Pulpitu aplikacji. Może to spowodować, że przeglądarka przestanie odpowiadać. Aby przeglądarka działała poprawnie w trybie RemoteApp, należy włączyć tryb zgodności. Możesz także spróbować włączyć tryb zgodności, jeśli napotkasz problemy z funkcjonalnością Bezpiecznego Pulpitu podczas korzystania z oprogramowania innych firm.

Raporty i Kopia zapasowa

Raporty

W raportach zapisywane są informacje o działaniu każdego modułu programu Kaspersky Endpoint Security, zdarzeniach szyfrowania danych, wykonaniu każdego zadania skanowania, zadania aktualizacji oraz zadania sprawdzania integralności, a także o ogólnym działaniu aplikacji.

Raporty są przechowywane w folderze `C:\ProgramData\Kaspersky Lab\KES.14.1\Report`.

Kopia zapasowa

Kopia zapasowa przechowuje zapasowe kopie plików, które zostały usunięte lub zmodyfikowane podczas leczenia. *Kopia zapasowa* to kopia pliku utworzona przed wyleczeniem lub usunięciem pliku. Kopie zapasowe plików są przechowywane w specjalnym formacie i nie stanowią zagrożenia.

Kopie zapasowe plików są przechowywane w folderze `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

Użytkownicy należący do grupy Administratorzy mają nadane pełne uprawnienie dostępu do tego folderu. Ograniczone uprawnienia dostępu do tego folderu są nadawane użytkownikom, których konto zostało użyte do zainstalowania Kaspersky Endpoint Security.

Kaspersky Endpoint Security nie oferuje możliwości skonfigurowania uprawnień dostępu użytkownika do kopii zapasowych plików.

Kwarantanna

Kwarantanna to specjalny lokalny magazyn na komputerze. Użytkownik może poddać kwarantannie pliki, które użytkownik uznaje za niebezpieczne dla komputera. Pliki poddane kwarantannie są przechowywane w postaci zaszyfrowanej i nie zagrażają bezpieczeństwu urządzenia. Kaspersky Endpoint Security używa Kwarantanny tylko w przypadku integracji z rozwiązaniami Kaspersky Detection and Response. W innych przypadkach Kaspersky Endpoint Security umieszcza odpowiedni plik w Kopii zapasowej. Więcej informacji na temat zarządzania Kwarantanną jako częścią rozwiązań można znaleźć w pomocy dla Kaspersky Sandbox, pomocy dla Kaspersky Endpoint Detection and Response Optimum, pomocy dla Kaspersky Endpoint Detection and Response Expert, pomocy dla Kaspersky Anti Targeted Attack Platform i pomocy dla Kaspersky Endpoint Detection and Response Expert (on-premises).

Kwarantanna może być skonfigurowana tylko za pośrednictwem konsoli Web Console. Możesz także użyć konsoli Web Console do zarządzania obiektami poddanymi kwarantannie (przywróć, usuń, dodaj itd.). Możesz przywrócić obiekty lokalnie na komputerze przy użyciu wiersza polecenia.

Kaspersky Endpoint Security używa konta systemowego (SYSTEM) do poddania plików kwarantannie.

Parametr	Opis
Usuń raporty po (dniach)	Jeśli pole jest zaznaczone, maksymalny czas przechowywania raportu jest ograniczony do zdefiniowanego przedziału czasu. Domyślnie maksymalny czas przechowywania raportów wynosi 30 dni. Po tym czasie Kaspersky Endpoint Security automatycznie usuwa najstarsze wpisy z pliku raportu.
Ogranicz rozmiar pliku raportu do (MB)	Jeśli pole jest zaznaczone, maksymalny rozmiar pliku raportu jest ograniczony do zdefiniowanej wartości. Domyślnie maksymalny rozmiar pliku wynosi 1024 MB. Aby uniknąć przekroczenia maksymalnego rozmiaru pliku raportu, Kaspersky Endpoint Security automatycznie usuwa najstarsze wpisy z pliku raportu po osiągnięciu maksymalnego rozmiaru pliku raportu.
Usuń obiekty po (dniach)	Jeśli pole jest zaznaczone, maksymalny czas przechowywania pliku jest ograniczony do zdefiniowanego przedziału czasu. Domyślnie maksymalny czas przechowywania plików wynosi 30 dni. Po minięciu zdefiniowanego czasu, Kaspersky Endpoint Security usunie najstarsze pliki z Kopii zapasowej.
Ogranicz rozmiar kopii zapasowej do (MB)	Jeśli pole jest zaznaczone, maksymalny rozmiar magazynu jest ograniczony do zdefiniowanej wartości. Domyślnie wynosi on 1024 MB. Aby uniknąć przekroczenia maksymalnego rozmiaru magazynu, Kaspersky Endpoint Security automatycznie usuwa najstarsze piki z magazynu po osiągnięciu maksymalnego rozmiaru magazynu.
Ogranicz rozmiar kwarantanny	Jeśli pole jest zaznaczone, maksymalny rozmiar Kwarantanny jest ograniczony do zdefiniowanej wartości. Domyślnie wynosi on 1024 MB. Jeśli Kwarantanna osiągnie maksymalny rozmiar, Kaspersky Endpoint Security wyśle zdarzenie *Brak wystarczającej ilości miejsca w magazynie Kwarantanny* do Kaspersky Security Center i opublikuje zdarzenie w dzienniku zdarzeń Windows. W międzyczasie aplikacja przestaje poddawać nowe obiekty kwarantannie. Musisz ręcznie opróżnić Kwarantannę.
Powiadom, gdy pamięć kwarantanny osiągnie (%)	Wartość progowa Kwarantanny. Na przykład, możesz ustawić wartość progową Kwarantanny na 50%. Jeśli Kwarantanna osiągnie wartość progową, Kaspersky Endpoint Security wyśle odpowiednie zdarzenie do Kaspersky Security Center i opublikuje zdarzenie w Dzienniku zdarzeń Windows. W międzyczasie aplikacja kontynuuje poddawanie nowych obiektów kwarantannie.
Przesyłanie danych do Serwera administracyjnego *(dostępny tylko w Kaspersky Security Center)*	Kategorie zdarzeń na komputerach klienckich, których informacje muszą być wysłane do Serwera administracyjnego. Możesz wyłączyć przesyłanie niektórych danych w celu optymalizacji przestrzeni dyskowej na Serwerze administracyjnym. Aplikacja wysyła zdarzenia z następujących kategorii: • **Informacje o plikach Kwarantanny**. Listę plików poddanych kwarantannie można wyświetlić w konsoli Kaspersky Security Center, w folderze **Zaawansowane → Repozytoria → Kwarantanna**. Kaspersky Endpoint Security używa Kwarantanny tylko w przypadku integracji z rozwiązaniami Kaspersky Detection and Response. • **O plikach znajdujących się w Kopii zapasowej**. Listę plików w kopii zapasowej można wyświetlić w konsoli Kaspersky Security Center, w folderze **Zaawansowane → Repozytoria → Kopia zapasowa**. • **O nieprzetworzonych plikach**. Listę nieprzetworzonych plików można wyświetlić w konsoli Kaspersky Security Center, w folderze **Zaawansowane → Repozytoria → Aktywne zagrożenia**. • **O zainstalowanych urządzeniach**. Listę podłączonych urządzeń można wyświetlić w konsoli Kaspersky Security Center, w folderze **Zaawansowane → Repozytoria → Sprzęt**. Lista urządzeń jest dostępna również we właściwościach komputera oraz w polityce Kaspersky Endpoint Security for Windows (sekcja **Kontrola urządzeń**). • **O uruchomionych aplikacjach**. Listę plików wykonywalnych można wyświetlić w konsoli Kaspersky Security Center, w folderze **Zaawansowane → Zarządzanie aplikacjami → Pliki wykonywalne**. Lista plików wykonywalnych jest dostępna również we właściwościach komputera. • **O błędach szyfrowania pliku**. Listę błędów szyfrowania plików można wyświetlić w konsoli Kaspersky Security Center, w folderze **Zaawansowane → Ochrona i szyfrowanie danych → Zdarzenia szyfrowania**. Lista błędów jest również dostępna we właściwościach komputera. • **Raport o stanie reguł Adaptacyjnej kontroli anomalii**. Raport można wyświetlić w konsoli Kaspersky Security Center, w węźle **Serwer administracyjny**, w zakładce **Raporty**. Raport jest również dostępny we właściwościach polityki Kaspersky Endpoint Security for Windows (sekcja **Adaptacyjna kontrola anomalii**). • **Raport o wywołanych regułach Adaptacyjnej kontroli anomalii**. Raport można wyświetlić w konsoli Kaspersky Security Center, w węźle **Serwer administracyjny**, w zakładce **Raporty**. Raport jest również dostępny we właściwościach polityki Kaspersky Endpoint Security for Windows (sekcja **Adaptacyjna kontrola anomalii**). • **Informacje o łańcuchu rozprzestrzeniania się zagrożeń**. Szczegóły wykrycia można wyświetlić w Kaspersky Security Center Web Console, w sekcji **Monitorowanie → Alerty**. Informacje o łańcuchu rozwoju zagrożenia są wykorzystywane przez rozwiązania Kaspersky Endpoint Detection and Response.

Ustawienia sieci

Możliwe jest skonfigurowanie serwera proxy używanego do nawiązywania połączenia z internetem i aktualizowania antywirusowych baz danych, wybranie trybu monitorowania portu sieciowego oraz konfigurowania skanowań połączeń szyfrowanych.

Parametr	Opis
Ogranicz ruch dla połączeń taryfowych	Jeśli to pole jest zaznaczone, aplikacja ogranicza ruch sieciowy, gdy połączenie internetowe jest limitowane. Kaspersky Endpoint Security identyfikuje mobilne połączenia internetowe jako taryfowe, natomiast połączenia Wi-Fi jako nietaryfowe. Uwzględnienie kosztów połączenia działa na komputerach z systemem Windows 8 lub nowszy.
Wstrzykuj skrypt do ruchu sieciowego w celu interakcji ze stronami internetowymi	Jeśli pole jest zaznaczone, Kaspersky Endpoint Security wstrzykuje skrypt interakcji ze stronami internetowymi do ruchu sieciowego. Ten skrypt zapewnia poprawne działanie komponentu Kontrola sieci. Skrypt włącza rejestrację zdarzeń Kontroli sieci. Bez tego skryptu nie możesz włączyć monitorowanie aktywności internetowej użytkownika. Eksperci z Kaspersky zalecają wstrzyknięcie tego skryptu interakcji ze stronami internetowymi do ruchu sieciowego w celu zapewnienia poprawnego działania Kontroli sieci.
Ustawienia serwera proxy	Ustawienia serwera proxy używanego do łączenia z internetem użytkowników komputerów klienckich. Program Kaspersky Endpoint Security używa tych ustawień dla pewnych komponentów ochrony, jak również do uaktualniania baz danych i modułów aplikacji. Do automatycznej konfiguracji serwera proxy Kaspersky Endpoint Security używa protokołu WPAD (Web Proxy Auto-Discovery Protocol). Jeśli adres IP serwera proxy nie może zostać określony przy pomocy tego protokołu, aplikacja użyje adresu serwera proxy określonego w ustawieniach przeglądarki Microsoft Internet Explorer.
Nie wykorzystuj serwera proxy dla adresów lokalnych	Jeśli pole jest zaznaczone, Kaspersky Endpoint Security nie korzysta z serwera proxy przy wykonywaniu aktualizacji z foldera współdzielonego.
Ustawienia uwierzytelniania serwera proxy	Aby uwierzytelnić aplikację na serwerze proxy w celu uzyskania dostępu do Internetu, należy wprowadzić dane uwierzytelniające użytkownika. Kaspersky Endpoint Security obsługuje automatyczne uwierzytelnianie na serwerze proxy. W przypadku niepowodzenia automatycznego uwierzytelnienia aplikacja poprosi o podanie danych uwierzytelniających. **Nie używaj uwierzytelniania**. **Uwierzytelnianie NTLM**. Uwierzytelnianie NTLM przy użyciu bieżącego konta użytkownika (domyślne). **Uwierzytelnianie NTLM przy użyciu nazwy użytkownika i hasła**. Uwierzytelnianie NTLM przy użyciu ręcznie określonych danych uwierzytelniających. **Nazwa użytkownika i hasło**. Uwierzytelnianie przy użyciu ręcznie określonych danych uwierzytelniających. **Automatyczne uwierzytelnianie**. **Uwierzytelnianie Kerberos**. Uwierzytelnianie Kerberos przy użyciu bieżącego konta użytkownika. Aby mieć pewność, że uwierzytelnianie Kerberos będzie działać prawidłowo podczas korzystania z rekordów CNAME dla adresu serwera proxy, należy zarejestrować główną nazwę usługi (SPN) dla każdego rekordu CNAME. **Uwierzytelnianie Kerberos przy użyciu nazwy użytkownika i hasła**. Uwierzytelnianie Kerberos przy użyciu ręcznie określonych danych uwierzytelniających. W przypadku wyboru uwierzytelniania Kerberos, Kaspersky Endpoint Security może, w zależności od ustawień serwera proxy, wykonać uwierzytelnianie przy użyciu protokołu Kerberos lub NTLM.
Monitorowane porty	**Monitoruj wszystkie porty sieciowe**. W tym trybie monitorowania portów sieciowych składniki ochrony (Ochrona plików, Ochrona WWW i Ochrona poczty) monitorują strumienie danych przesyłane przez dowolne otwarte porty sieciowe komputera. **Monitoruj tylko wybrane porty sieciowe**. W tym trybie monitorowania portu sieciowego składniki ochrony monitorują wybrane porty komputera i aktywność sieciową wybranych aplikacji. Lista portów sieciowych używanych zazwyczaj do przesyłania wiadomości e-mail i ruchu internetowego jest konfigurowana zgodnie z zaleceniami ekspertów z Kaspersky. **Monitoruj wszystkie porty dla aplikacji z listy zalecanej przez Kaspersky**. To powoduje używanie predefiniowanej listy aplikacji, których porty sieciowe są monitorowane przez Kaspersky Endpoint Security. Na przykład, ta lista zawiera Google Chrome, Adobe Reader, Java i inne aplikacje. **Monitoruj wszystkie porty dla określonych aplikacji**. To powoduje używanie listy aplikacji, których porty sieciowe są monitorowane przez Kaspersky Endpoint Security.

Parametr	Opis
Skanowanie połączeń szyfrowanych	Kaspersky Endpoint Security skanuje zaszyfrowany ruch sieciowy przesyłany za pośrednictwem następujących protokołów: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security obsługuje następujące tryby skanowania połączenia szyfrowanego: • **Nie skanuj połączeń szyfrowanych**. Kaspersky Endpoint Security nie będzie miał dostępu do zawartości stron internetowych, których adresy zaczynają się od `https://`. • **Skanuj połączenia szyfrowane po zgłoszeniach od składników ochrony**. Kaspersky Endpoint Security będzie skanować zaszyfrowany ruch sieciowy tylko na żądanie składników: Ochrona WWW, Ochrona poczty i Kontrola sieci. • **Zawsze skanuj połączenia szyfrowane**. Kaspersky Endpoint Security będzie skanował zaszyfrowany ruch sieciowy nawet wtedy, gdy składniki ochrony są wyłączone. Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych, które zostały nawiązane przez zaufane aplikacje, dla których skanowanie ruchu sieciowego jest wyłączone. Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych z predefiniowanej listy zaufanych stron internetowych. Predefiniowana lista zaufanych stron internetowych jest tworzona przez ekspertów Kaspersky. Ta lista jest aktualizowana o antywirusowe bazy danych aplikacji. Predefiniowaną listę zaufanych stron internetowych możesz przejrzeć tylko w interfejsie Kaspersky Endpoint Security. Listy nie można przejrzeć w Kaspersky Security Center Console.
Zaufane certyfikaty główne	Lista zaufanych certyfikatów głównych. Kaspersky Endpoint Security umożliwia zainstalowanie zaufanych certyfikatów głównych na komputerach użytkowników, gdy, na przykład, musisz wdrożyć nowe centrum certyfikacji. Aplikacja umożliwia dodanie certyfikatu do specjalnego magazynu certyfikatów Kaspersky Endpoint Security. W tym przypadku certyfikat jest uznawany za zaufany tylko dla aplikacji Kaspersky Endpoint Security. Innymi słowy, użytkownik może uzyskać dostęp do strony internetowej z nowym certyfikatem w przeglądarce. Jeśli inna aplikacja spróbuje uzyskać dostęp do strony internetowej, może pojawić się błąd połączenia w wyniku problemu z certyfikatem. Aby dodać do systemowego magazynu certyfikatów, możesz użyć zasady grupy Active Directory.
Odwiedzanie domeny z niezaufanym certyfikatem	• **Zezwól**. Podczas odwiedzania domeny z niezaufanym certyfikatem, Kaspersky Endpoint Security zezwoli na połączenie sieciowe. Podczas otwierania domeny z niezaufanym certyfikatem w przeglądarce, Kaspersky Endpoint Security wyświetla stronę HTML pokazującą ostrzeżenie i powód, z jakiego odwiedzenie tej domeny nie jest zalecane. Użytkownik może kliknąć odnośnik ze strony ostrzegającej HTML, aby uzyskać dostęp do żądanego zasobu internetowego. Jeśli usługa lub aplikacja innej firmy nawiąże połączenie z domeną z niezaufanym certyfikatem, Kaspersky Endpoint Security utworzy swój własny certyfikat, aby przeskanować ruch sieciowy. Nowy certyfikat posiada stan *Niezaufane*. To jest konieczne, aby ostrzec aplikację innej firmy przed niezaufanym połączeniem, ponieważ strona HTML nie może zostać wyświetlona w tym przypadku, a połączenie może zostać nawiązane w tle. • **Zablokuj**. Podczas odwiedzania domeny z niezaufanym certyfikatem, Kaspersky Endpoint Security zablokuje połączenie sieciowe. Podczas otwierania domeny z niezaufanym certyfikatem w przeglądarce, Kaspersky Endpoint Security wyświetla stronę HTML pokazującą powód zablokowania tej domeny.
Odwiedzanie domeny z błędem skanowania połączeń szyfrowanych	• **Zablokuj**. Jeśli wystąpi błąd skanowania połączenia szyfrowanego, Kaspersky Endpoint Security zablokuje połączenie sieciowe. • **Zezwól na domenę i dodaj ją do wykluczeń**. Jeśli wystąpi błąd skanowania połączenia szyfrowanego, Kaspersky Endpoint Security doda domenę, w której wystąpił błąd, do listy domen z błędami skanowania i nie będzie monitorował szyfrowanego ruchu sieciowego, gdy ta domena będzie odwiedzana. Możesz przejrzeć listę domen z błędami skanowania połączeń szyfrowanych tylko w lokalnym interfejsie aplikacji. Aby wyczyścić zawartość listy, należy wybrać **Zablokuj**. Kaspersky Endpoint Security także generuje zdarzenie dla błędu skanowania połączenia szyfrowanego.
Blokuj połączenia SSL 2.0	Jeśli pole jest zaznaczone, aplikacja monitoruje i blokuje połączenia sieciowe nawiązane przez protokół SSL 2.0. Jeśli pole jest zaznaczone, aplikacja nie blokuje połączeń sieciowych nawiązanych przez protokół SSL 2.0. Aplikacja nie monitoruje jednak ruchu sieciowego przesyłanego za pośrednictwem tego protokołu.
Blokuj połączenia SSL 3.0	Jeśli pole jest zaznaczone, aplikacja zablokuje połączenia sieciowe nawiązane po protokole SSL 3.0. Jeśli pole jest zaznaczone, aplikacja nie blokuje połączeń sieciowych nawiązanych przez protokół SSL 3.0. Aplikacja monitoruje ruch sieciowy przesyłany za pośrednictwem tego protokołu. Wszystkie komponenty aplikacji działają bez ograniczeń.
Blokuj połączenia TLS 1.0	Jeśli pole jest zaznaczone, aplikacja zablokuje połączenia sieciowe nawiązane po protokole TLS 1.0. Jeśli pole jest zaznaczone, aplikacja nie blokuje połączeń sieciowych nawiązanych przez protokół TLS 1.0. Aplikacja monitoruje ruch sieciowy przesyłany za pośrednictwem tego protokołu. Wszystkie komponenty aplikacji działają bez ograniczeń.

Parametr	Opis
Deszyfruj szyfrowane połączenie ze stroną internetową używającą certyfikatu EV	Certyfikaty EV (Extended Validation Certificate) potwierdzają autentyczność stron internetowych i zwiększają ochronę połączenia. Przeglądarki używają ikony kłódki w paskach adresu, aby pokazać, że strona internetowa posiada certyfikat EV. W przeglądarkach pasek adresu może być częściowo lub całkowicie oznaczony na zielono. Jeśli pole jest zaznaczone, aplikacja deszyfruje i monitoruje połączenia szyfrowane ze stronami internetowymi, które używają certyfikatu EV. Jeśli pole jest odznaczone, aplikacja nie ma dostępu do zawartości ruchu sieciowego HTTPS. Z tego powodu aplikacja monitoruje ruch sieciowy HTTPS tylko w oparciu o adres strony internetowej, na przykład: `https://bing.com`. Jeśli otwierasz stronę internetową z certyfikatem EV po raz pierwszy, zaszyfrowane połączenie zostanie odszyfrowane niezależnie od tego, czy pole jest zaznaczone.
Skonfiguruj zaufane adresy	To powoduje użycie listy adresów internetowych, dla których Kaspersky Endpoint Security nie skanuje połączeń sieciowych. W tym przypadku program Kaspersky Endpoint Security nie skanuje ruchu sieciowego HTTPS zaufanych adresów internetowych, gdy komponenty Ochrona WWW, Ochrona poczty, Kontrola sieci wykonują swoją pracę. Możesz wprowadzić nazwę domeny lub adres IP. Kaspersky Endpoint Security obsługuje znak `*` do wprowadzenia maski w nazwie domeny. Kaspersky Endpoint Security nie obsługuje symbolu `*` dla adresów IP. Za pomocą maski podsieci możesz wybrać zakres adresów IP (na przykład: 198.51.100.0/24). Na przykład: • `domain.com` – wpis jest częścią następujących adresów: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Wpis nie jest częścią poddomen (na przykład: `subdomain.domain.com`). • `subdomain.domain.com` – wpis jest częścią następujących adresów: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Wpis nie jest częścią domeny `domain.com`. • `*.domain.com` – wpis jest częścią następujących adresów: `https://movies.domain.com`, `https://images.domain.com/page123`. Wpis nie jest częścią domeny `domain.com`.
Skonfiguruj zaufane aplikacje	Lista aplikacji, których aktywność nie jest monitorowana przez Kaspersky Endpoint Security w trakcie działania. Możesz wybrać typy aktywności aplikacji, których Kaspersky Endpoint Security nie będzie monitorował (na przykład, żeby nie skanował ruchu sieciowego). Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki `*` i `?`.
Do skanowania szyfrowanych połączeń w aplikacjach z własnym magazynem certyfikatów użyj *(dostępne tylko w interfejsie Kaspersky Endpoint Security)*	Jeśli to pole jest zaznaczone, aplikacja skanuje zaszyfrowany ruch sieciowy w przeglądarce Mozilla Firefox oraz w kliencie poczty Thunderbird. Dostęp do niektórych stron internetowych za pośrednictwem protokołu HTTPS może zostać zablokowany. Aby skanować ruch sieciowy w przeglądarce Mozilla Firefox i kliencie poczty Thunderbird, musisz włączyć Skanowanie połączeń szyfrowanych. Jeśli Skanowanie połączeń szyfrowanych jest wyłączone, aplikacja nie skanuje ruchu sieciowego w przeglądarce Mozilla Firefox oraz w kliencie poczty Thunderbird. Aplikacja używa certyfikatu głównego Kaspersky do odszyfrowania i analizowania zaszyfrowanego ruchu sieciowego. Możesz wybrać magazyn certyfikatów, który będzie zawierał certyfikat główny Kaspersky. • **Magazyn certyfikatów Windows (zalecane)**. Certyfikat główny Kaspersky zostanie dodany do tego magazynu podczas instalacji Kaspersky Endpoint Security. • **Własny magazyn certyfikatów**. Mozilla Firefox i Thunderbird używają swoich własnych magazynów certyfikatów. Jeśli wybrano magazyn certyfikatów aplikacji Mozilla, powinieneś ręcznie dodać certyfikat główny Kaspersky do tego magazynu z poziomu właściwości przeglądarki.

Interfejs

Możesz skonfigurować ustawienia interfejsu aplikacji.

Parametr	Opis
Interakcja z użytkownikiem *(dostępny tylko w Kaspersky Security Center Console)*	**Wyświetl uproszczony interfejs**. Na komputerze klienckim okno główne aplikacji jest niedostępne, a dostępna jest tylko ikona w obszarze powiadomień systemu Windows. W menu kontekstowym ikony użytkownik może przeprowadzić ograniczoną liczbę operacji na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetla nad ikoną aplikacji tylko powiadomienia wymagające podjęcia działania przez użytkownika. **Wyświetl interfejs użytkownika**. Na komputerze klienckim dostępne są: okno główne Kaspersky Endpoint Security oraz ikona w obszarze powiadomień systemu Windows. W menu kontekstowym ikony użytkownik może przeprowadzić operacje na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetli także powiadomienia nad ikoną aplikacji. **Ukryj sekcję Monitor aktywności aplikacji**. Na komputerze klienckim, w oknie głównym Kaspersky Endpoint Security przycisk **Monitor aktywności aplikacji** jest niedostępny. *Monitor aktywności aplikacji* to narzędzie służące do wyświetlania informacji o aktywności aplikacji na komputerze użytkownika w czasie rzeczywistym. **Nie wyświetlaj interfejsu użytkownika**. Na komputerze klienckim nie są wyświetlane żadne działania Kaspersky Endpoint Security. Ikona w obszarze powiadomień systemu Windows oraz powiadomienia nie są dostępne.
Skonfiguruj powiadomienia	Tabela z ustawieniami powiadomień o zdarzeniach o różnych poziomach istotności, które mogą wystąpić w trakcie działania modułu, zadania lub aplikacji. Kaspersky Endpoint Security wyświetla powiadomienia o tych zdarzeniach, wysyła je za pośrednictwem poczty elektronicznej lub zapisuje je w raporcie.
Skonfiguruj powiadomienia e-mail	Ustawienia serwera SMTP do dostarczania powiadomień o zdarzeniach zarejestrowanych podczas działania aplikacji. Domyślnie Kaspersky Endpoint Security używa ustawień powiadomień e-mail z Kaspersky Security Center. Bardziej szczegółowe informacje na temat ustawień powiadomień e-mail można znaleźć w pomocy do Kaspersky Security Center. Jeśli chcesz skonfigurować indywidualne powiadomienia e-mail, możesz edytować następujące ustawienia: • **Adres nadawcy**. Adres e-mail nadawcy. Nie zaleca się używania nieistniejącego adresu. • **Serwer SMTP**. Jeden lub więcej adresów serwerów e-mail Twojej organizacji (np. `mail.company.com`). Możesz wprowadzić adres IP (IPv4 lub IPv6). Aby uwierzytelnić użytkownika na serwerze SMTP, w odpowiednich polach wprowadź poświadczenia nadawcy. Aby przetestować powiadomienia e-mail, możesz wysłać wiadomość testową. • **Adres odbiorcy**. Adresy e-mail odbiorców, do których aplikacja będzie wysyłać powiadomienia. • **Tryb wysyłania**. Tryb wysyłania powiadomień e-mail. Kaspersky Endpoint Security może wysyłać wiadomości natychmiast po wystąpieniu zdarzenia; alternatywnie może działać zgodnie z wcześniej skonfigurowanym harmonogramem.
Pokaż stan aplikacji w obszarze powiadomień	Kategorie zdarzeń aplikacji, które powodują, że ikona Kaspersky Endpoint Security zmienia się w obszarze powiadomień paska zadań systemu Microsoft Windows (lub) i powoduje wyświetlanie wiadomości wyskakującej.
Powiadomienia o stanie lokalnych baz danych anty-malware	Ustawienia powiadomień o przestarzałych antywirusowych bazach danych używanych przez aplikację.
Ochrona hasłem	Jeśli przycisk przełącznika jest włączony, Kaspersky Endpoint Security pyta użytkownika o hasło, gdy użytkownik próbuje wykonać działanie, które jest w obrębie obszaru Ochrony hasłem. Obszar Ochrony hasłem obejmuje zabronione działania (takie jak wyłączenie składników ochrony) oraz konta użytkowników, do których stosowany jest obszar Ochrony hasłem. Po włączeniu Ochrony hasłem Kaspersky Endpoint Security wyświetli monit o ustawienie hasła dla konta KLAdmin.
Pomoc techniczna / Odnośniki do zasobów sieciowych *(dostępny tylko w Kaspersky Security Center Console)*	Lista odsyłaczy do zasobów sieciowych z informacjami o pomocy technicznej dla Kaspersky Endpoint Security. Dodane odnośniki będą wyświetlane w oknie **Pomoc techniczna** lokalnego interfejsu Kaspersky Endpoint Security zamiast standardowych odnośników.
Pomoc techniczna / Opis *(dostępny tylko w Kaspersky Security Center Console)*	Wiadomość, która jest wyświetlana w oknie **Pomoc techniczna** lokalnego interfejsu Kaspersky Endpoint Security.

Zarządzaj ustawieniami

Możesz zapisać bieżące ustawienia Kaspersky Endpoint Security do pliku i użyć ich do szybkiego skonfigurowania aplikacji na innym komputerze. Możesz użyć pliku konfiguracyjnego podczas zdalnej instalacji aplikacji za pośrednictwem Kaspersky Security Center z użyciem pakietu instalacyjnego. Możesz przywrócić domyślne ustawienia w dowolnym momencie.

Ustawienia zarządzania konfiguracją aplikacji są dostępne tylko w interfejsie Kaspersky Endpoint Security.

Ustawienia zarządzania konfiguracją aplikacji

Ustawienia	Opis
Importuj	Wydobywanie ustawień aplikacji z pliku w formacie CFG i ich stosowanie.
Eksportuj	Zapisywanie bieżących ustawień aplikacji do pliku w formacie CFG.
Przywracanie	W każdej chwili można przywrócić ustawienia aplikacji zalecane przez Kaspersky. Po przywróceniu ustawień, poziom ochrony wszystkich modułów zostaje ustawiony na **Zalecany**.

Aktualizowanie baz danych i modułów aplikacji

Aktualizowanie baz danych i modułów aplikacji Kaspersky Endpoint Security zapewnia aktualną ochronę Twojego komputera. Codziennie na całym świecie pojawia się duża ilość nowych wirusów i innego typu szkodliwego oprogramowania. Bazy danych Kaspersky Endpoint Security zawierają informacje o zagrożeniach i sposoby ich neutralizowania. Aby szybko wykrywać zagrożenia, zalecamy regularnie aktualizować bazy danych i moduły aplikacji.

Aktualizuje funkcje (obejmuje aktualizacje sygnatur wirusów oraz aktualizacje bazy kodu), które mogą nie być dostępne w oprogramowaniu na terytorium Stanów Zjednoczonych.

Regularne aktualizacje wymagają ważnej licencji na aplikację. Jeżeli nie ma bieżącej licencji, wówczas możliwe będzie wykonanie tylko jednej aktualizacji.

Aby możliwe było pobieranie pakietów aktualizacji z serwerów aktualizacji Kaspersky, komputer musi być podłączony do internetu. Domyślnie ustawienia połączenia internetowego są określane automatycznie. Jeśli korzystasz z serwera proxy, konieczne może być dostosowanie ustawień serwera proxy.

Uaktualnienia są pobierane po protokole HTTPS. Mogą także zostać pobrane po protokole HTTP, jeśli niemożliwe jest pobranie uaktualnień po protokole HTTPS.

Podczas procesu aktualizacji, na komputer są pobierane i instalowane następujące obiekty:

- Bazy danych programu Kaspersky Endpoint Security. Ochrona komputera jest zapewniana przy pomocy baz danych zawierających sygnatury wirusów i innych zagrożeń oraz informacje o sposobach ich neutralizacji. Moduły ochrony korzystają z tych informacji przy wyszukiwaniu i neutralizowaniu zainfekowanych plików na Twoim komputerze. Bazy danych są ciągle aktualizowane o wpisy nowych zagrożeń i metody ich zwalczania. Dlatego zalecamy regularne aktualizowanie baz danych.

  Oprócz baz danych Kaspersky Endpoint Security aktualizowane są również sterowniki sieciowe, które umożliwiają modułom aplikacji przechwytywanie ruchu sieciowego.

- Moduły aplikacji. Oprócz baz danych Kaspersky Endpoint Security można także aktualizować jej moduły. Aktualizowanie modułów aplikacji likwiduje luki w Kaspersky Endpoint Security, dodaje nowe funkcje lub poprawia te istniejące.

Podczas aktualizacji moduły i bazy danych aplikacji znajdujące się na komputerze porównywane są z tymi aktualnymi, znajdującymi się w źródle uaktualnień. Jeśli Twoje bieżące bazy danych i moduły różnią się od najnowszych wersji, na Twoim komputerze zainstalowana zostanie brakująca część uaktualnień.

Jeśli bazy danych są bardzo stare, pakiet uaktualnień może być duży, co spowoduje zwiększony ruch internetowy (kilkadziesiąt MB).

Informacje o bieżącym stanie baz danych Kaspersky Endpoint Security jest wyświetlany w oknie głównym aplikacji lub w dymku, który jest wyświetlany po najechaniu kursorem na ikonę aplikacji w obszarze powiadomień.

Informacje o wynikach aktualizacji i wszystkich zdarzeniach zaistniałych podczas wykonywania zadania aktualizacji zapisywane są w raporcie Kaspersky Endpoint Security.

Jeśli aplikacja działa w trybie Light Agent, podczas aktualizowania baz danych i modułów aplikacji należy zwrócić uwagę na pewne szczególne kwestie.

Ustawienia aktualizacji baz danych i modułów aplikacji

Parametr	Opis
Terminarz aktualizacji baz danych	**Automatycznie**. W tym trybie aplikacja sprawdza źródło uaktualnień z określoną częstotliwością w poszukiwaniu nowych pakietów aktualizacji. Częstotliwość sprawdzania w poszukiwaniu pakietu uaktualnień może wzrastać podczas epidemii wirusów, a maleć w okresach względnie spokojnych. Po wykryciu nowego pakietu aktualizacji, Kaspersky Endpoint Security pobiera go i instaluje aktualizacje na komputerze. **Ręcznie**. Ten tryb uruchamiania zadania aktualizacji umożliwia ręczne uruchomienie zadania aktualizacji. **Zgodnie z terminarzem**. W tym trybie Kaspersky Endpoint Security uruchamia zadanie aktualizacji zgodnie z ustalonym terminarzem. Jeśli wybrano ten tryb uruchamiania, zadanie aktualizacji może zostać również uruchomione ręcznie.
Uruchom pominięte zadania	Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security uruchamia pominięte zadanie, kiedy tylko będzie to możliwe. Zadanie może zostać pominięte, na przykład, jeśli komputer był wyłączony w zaplanowanym czasie uruchomienia zadania. Gdy aplikacja uzyska możliwość wykonania pominiętych zadań, uruchamia zadania losowo w określonym przedziale czasu, aby rozłożyć obciążenie na komputerze. Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security nie uruchamia pominiętych zadań. Zamiast tego uruchomi następne zadanie zgodnie z bieżącym terminarzem.

Parametr	Opis
Źródła aktualizacji	*Źródło uaktualnień* jest zasobem zawierającym uaktualnienia baz danych oraz modułów aplikacji Kaspersky Endpoint Security. Źródłami uaktualnień mogą być serwer Kaspersky Security Center, serwery aktualizacji Kaspersky i foldery lokalne lub sieciowe. Jeśli serwery aktualizacji Kaspersky są niedostępne, Kaspersky Endpoint Security może użyć alternatywnych domen w celu zaktualizowania swoich baz danych i modułów oprogramowania aplikacji. Aby uzyskać szczegółowe informacje, zapoznaj się z Bazą wiedzy na stronie działu pomocy technicznej. Domyślna lista źródeł uaktualnień zawiera serwery aktualizacji Kaspersky Security Center i Kaspersky. Do listy można dodać inne źródło uaktualnień. Źródłem uaktualnień mogą być serwery HTTP/FTP oraz foldery współdzielone. Kaspersky Endpoint Security nie obsługuje aktualizacji z serwerów HTTPS, chyba że są to serwery aktualizacji Kaspersky. Jeżeli jako aktywne ustawiono kilka źródeł uaktualnień, Kaspersky Endpoint Security będzie podejmował próby nawiązywania połączenia z każdym z nich, począwszy od góry listy; uaktualnienia zostaną pobrane z pierwszego dostępnego źródła. Domyślnie Kaspersky Endpoint Security używa serwera Kaspersky Security Center jako pierwszego źródła aktualizacji. Pomaga to oszczędzać ruch podczas aktualizacji. Jeśli zasada nie zostanie zastosowana do komputera, serwery Kaspersky zostaną wybrane jako pierwsze źródło aktualizacji w ustawieniach lokalnego zadania *Aktualizacja baz danych i modułów aplikacji*, ponieważ aplikacja może nie mieć dostępu do serwera Kaspersky Security Center. Jeśli aplikacja działa w trybie Light Agent, jako źródło aktualizacji wybierany jest folder na maszynie SVM.
Uruchamiaj aktualizacje baz danych jako	Domyślnie zadanie aktualizacji Kaspersky Endpoint Security jest uruchamiane z poziomu konta użytkownika, którego użyłeś do uruchomienia systemu operacyjnego. Jednakże program Kaspersky Endpoint Security może zostać zaktualizowany ze źródła uaktualnień, do którego użytkownik nie ma dostępu ze względu na brak wymaganych uprawnień (na przykład, z folderu współdzielonego, który zawiera pakiet uaktualnień) lub ze źródła uaktualnień, dla którego nie skonfigurowano autoryzacji na serwerze proxy. W ustawieniach aplikacji możesz wskazać użytkownika, który posiada takie uprawnienia, i skonfigurować uruchamianie zadania aktualizacji Kaspersky Endpoint Security z poziomu konta tego użytkownika.
Pobierz aktualizacje składników aplikacji	Pobieranie aktualizacji modułów aplikacji z aktualizacjami baz danych aplikacji. Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security powiadomi użytkownika o dostępnych uaktualnieniach modułów aplikacji i uwzględni te uaktualnienia w pakiecie uaktualnień podczas wykonywania zadania aktualizacji. Sposób stosowania uaktualnień modułów aplikacji jest określany przez następujące ustawienia: • **Instaluj krytyczne i zatwierdzone aktualizacje**. Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security automatycznie instaluje krytyczne uaktualnienia, a także wszystkie inne uaktualnienia modułów aplikacji po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center. • **Instaluj tylko zatwierdzone aktualizacje**. Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security instaluje je po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center. Ta opcja jest wybrana domyślnie. Jeśli to pole nie zostanie zaznaczone, Kaspersky Endpoint Security nie powiadomi użytkownika o dostępnych uaktualnieniach modułów aplikacji i nie uwzględni tych uaktualnień w pakiecie uaktualnień podczas wykonywania zadania aktualizacji. Jeśli uaktualnienia modułów aplikacji wymagają przeczytanie i zaakceptowanie warunków Umowy licencyjnej, aplikacja zainstaluje uaktualnienia po zaakceptowaniu warunków Umowy licencyjnej. Domyślnie pole to jest zaznaczone.
Kopiuj aktualizacje do folderu	Jeśli to pole wyboru jest zaznaczone, Kaspersky Endpoint Security kopiuje pakiet aktualizacji do udostępnionego folderu określonego w polu wyboru. Następnie pozostałe komputery w sieci LAN pobierają pakiet uaktualnień z tego folderu współdzielonego. Ogranicza to ruch internetowy, ponieważ pakiet uaktualnień jest pobierany jednorazowo. Domyślnie określony jest następujący folder: `C:\ProgramData\Kaspersky Lab\KES.14.1\Update distribution\`.

Parametr	Opis
Serwer proxy dla aktualizacji *(dostępne tylko w interfejsie Kaspersky Endpoint Security)*	Ustawienia serwera proxy dla dostępu użytkowników komputerów klienckich do internetu w celu przeprowadzenia aktualizacji baz danych i modułów aplikacji. Do automatycznej konfiguracji serwera proxy Kaspersky Endpoint Security używa protokołu WPAD (Web Proxy Auto-Discovery Protocol). Jeśli adres IP serwera proxy nie może zostać określony przy pomocy tego protokołu, Kaspersky Endpoint Security użyje adresu serwera proxy określonego w ustawieniach przeglądarki Microsoft Internet Explorer.
Nie wykorzystuj serwera proxy dla adresów lokalnych *(dostępne tylko w interfejsie Kaspersky Endpoint Security)*	Jeśli pole jest zaznaczone, Kaspersky Endpoint Security nie korzysta z serwera proxy przy wykonywaniu aktualizacji z foldera współdzielonego.

Dodatek 2. Grupy zaufania aplikacji

Kaspersky Endpoint Security przydziela wszystkie aplikacje, które są uruchomione na komputerze, do grup zaufania. Aplikacje są przydzielane do grup zaufania w zależności od poziomu zagrożenia, jakie stanowią dla systemu operacyjnego.

Istnieją następujące grupy zaufania:

- **Zaufane**. Ta grupa zawiera aplikacje, dla których spełniono jeden lub kilka następujących warunków:
  - Aplikacje są cyfrowo podpisane przez zaufanych producentów.
  - Aplikacje znajdują się w bazie danych zaufanych aplikacji z Kaspersky Security Network.
  - Użytkownik umieścił aplikacje w grupie *Zaufane*.

  Dla takich aplikacji nie ma zabronionych akcji.
- **Niskie ograniczenia**. Ta grupa zawiera aplikacje, dla których spełniono następujące warunki:
  - Aplikacje nie są cyfrowo podpisane przez zaufanych producentów.
  - Aplikacje nie znajdują się w bazie danych zaufanych aplikacji z Kaspersky Security Network.
  - Użytkownik umieścił aplikacje w grupie *Niskie ograniczenia*.

  Takie aplikacje mają minimalne ograniczenia dostępu do zasobów systemu operacyjnego.
- **Wysokie ograniczenia**. Ta grupa zawiera aplikacje, dla których spełniono następujące warunki:
  - Aplikacje nie są cyfrowo podpisane przez zaufanych producentów.
  - Aplikacje nie znajdują się w bazie danych zaufanych aplikacji z Kaspersky Security Network.
  - Użytkownik umieścił aplikacje w grupie *Wysokie ograniczenia*.

  Takie aplikacje mają wysokie ograniczenia dostępu do zasobów systemu operacyjnego.

- **Niezaufane**. Ta grupa zawiera aplikacje, dla których spełniono następujące warunki:
  - Aplikacje nie są cyfrowo podpisane przez zaufanych producentów.
  - Aplikacje nie znajdują się w bazie danych zaufanych aplikacji z Kaspersky Security Network.
  - Użytkownik umieścił aplikacje w grupie *Niezaufane*.

  Dla takich aplikacji wszystkie działania są zablokowane.

Dodatek 3. Rozszerzenia plików do szybkiego skanowania dysków wymiennych

com – plik wykonywalny aplikacji nie większy niż 64 KB

exe – plik wykonywalny samorozpakowującego się archiwum

sys – plik systemu Microsoft Windows

prg – dla programu dBase™, Clipper, Microsoft Visual FoxPro® lub WAVmaker

bin – plik binarny

bat – plik wsadowy

cmd – plik polecenia dla Microsoft Windows NT (podobny do pliku bat dla DOS), OS/2

dpl – skompresowana biblioteka Borland Delphi

dll – biblioteka dołączana dynamicznie

scr – ekran powitalny Microsoft Windows

cpl – moduł panelu kontrolującego Microsoft Windows

ocx – obiekt OLE Microsoft (Łączenie i osadzanie obiektów)

tsp – program działający w trybie podziału czasu

drv – sterownik urządzenia

vxd – sterownik urządzenia wirtualnego Microsoft Windows

pif – plik PIF

lnk – plik łącza Microsoft Windows

reg – plik klucza rejestru systemu Microsoft Windows

ini – plik konfiguracyjny, który zawiera dane konfiguracyjne dla Microsoft Windows, Windows NT i niektórych aplikacji

cla – plik klasy języka Java

vbs – skrypt Visual Basic®

vbe – rozszerzenie BIOS-u kart graficznych

js, jse – tekst źródłowy JavaScript

htm – dokument hipertekstowy

htt – nagłówek hipertekstowy Microsoft Windows

hta – program hipertekstowy dla Microsoft Internet Explorer®

asp – skrypt Active Server Pages

chm – skompilowany plik HTML

pht – plik HTML ze zintegrowanymi skryptami PHP

php – skrypt zintegrowany w plikach HTML

wsh – plik Microsoft Windows Script Host

wsf – skrypt Microsoft Windows

the – plik tapety pulpitu Microsoft Windows 95

hlp – plik pomocy w formacie Win Help

msg – wiadomość pocztowa Microsoft Mail

plg – wiadomość pocztowa

mbx – zapisane wiadomości e-mail Microsoft Office Outlook

doc* – dokumenty Microsoft Office Word, takie jak: doc dla dokumentów Microsoft Office Word, docx dla dokumentów Microsoft Office Word 2007 z obsługą XML oraz docm dla dokumentów Microsoft Office Word 2007 z obsługą makr

dot* – szablony dokumentów Microsoft Office Word, takie jak: dot dla szablonów dokumentów Microsoft Office Word, dotx dla szablonów dokumentów Microsoft Office Word 2007, dotm dla szablonów dokumentów Microsoft Office Word 2007 z obsługą makr

fpm – program bazodanowy, plik startowy dla Microsoft Visual FoxPro

rtf – dokument Rich Text Format

shs – fragment Windows Shell Scrap Object Handler

dwg – baza danych programu AutoCAD®

msi – pakiet Microsoft Windows Installer

otm – projekt VBA dla Microsoft Office Outlook

pdf – dokument Adobe Acrobat

swf – obiekt pakietu Shockwave® Flash

jpg, jpeg – skompresowany format graficzny

emf – plik formatu Enhanced Metafile;

ico – plik ikony obiektu

ov? – pliki wykonywalne Microsoft Office Word

xl* – pliki i dokumenty Microsoft Office Excel, takie jak: xla dla rozszerzeń dla Microsoft Office Excel, xlc dla diagramów, xlt dla szablonów dokumentów, xlsx dla skoroszytów Microsoft Office Excel 2007, xltm dla skoroszytów Microsoft Office Excel 2007 z obsługą makr, xlsb dla skoroszytów Microsoft Office Excel 2007 w formacie binarnym (nie XML), xltx dla szablonów Microsoft Office Excel 2007, xlsm dla szablonów Microsoft Office Excel 2007 z obsługą makr oraz xlam dla wtyczek Microsoft Office Excel 2007 z obsługą makr

pp* – pliki i dokumenty Microsoft Office PowerPoint®, takie jak: pps dla slajdów Microsoft Office PowerPoint, ppt dla prezentacji, pptx dla prezentacji Microsoft Office PowerPoint 2007, pptm dla prezentacji Microsoft Office PowerPoint 2007 z obsługą makr, potx dla szablonów prezentacji Microsoft Office PowerPoint 2007, potm dla szablonów prezentacji Microsoft Office PowerPoint 2007 z obsługą makr, ppsx dla pokazów slajdów Microsoft Office PowerPoint 2007, ppsm dla pokazów slajdów Microsoft Office PowerPoint 2007 z obsługą makr oraz ppam dla wtyczek Microsoft Office PowerPoint 2007 z obsługą makr

md* – pliki i dokumenty Microsoft Office Access®, takie jak: mda dla grup roboczych Microsoft Office Access oraz mdb dla baz danych

sldx – slajd Microsoft PowerPoint 2007

sldm – slajd Microsoft PowerPoint 2007 z obsługą makr

thmx – motyw Microsoft Office 2007

Dodatek 4. Typy plików dla filtra załączników modułu Ochrona poczty

Należy pamiętać, że rzeczywisty format pliku może nie odpowiadać jego rozszerzeniu.

Jeśli włączyłeś filtrowanie załączników w wiadomościach, komponent Ochrona poczty może zmieniać nazwy plików lub usuwać pliki z następującymi rozszerzeniami:

com – plik wykonywalny aplikacji nie większy niż 64 KB

exe – plik wykonywalny samorozpakowującego się archiwum

sys – plik systemu Microsoft Windows

prg – dla programu dBase™, Clipper, Microsoft Visual FoxPro® lub WAVmaker

bin – plik binarny

bat – plik wsadowy

cmd – plik polecenia dla Microsoft Windows NT (podobny do pliku bat dla DOS), OS/2

dpl – skompresowana biblioteka Borland Delphi

dll – biblioteka dołączana dynamicznie

scr – ekran powitalny Microsoft Windows

cpl – moduł panelu kontrolującego Microsoft Windows

ocx – obiekt OLE Microsoft (Łączenie i osadzanie obiektów)

tsp – program działający w trybie podziału czasu

drv – sterownik urządzenia

vxd – sterownik urządzenia wirtualnego Microsoft Windows

pif – plik PIF

lnk – plik łącza Microsoft Windows

reg – plik klucza rejestru systemu Microsoft Windows

ini – plik konfiguracyjny, który zawiera dane konfiguracyjne dla Microsoft Windows, Windows NT i niektórych aplikacji

cla – plik klasy języka Java

vbs – skrypt Visual Basic®

vbe – rozszerzenie BIOS-u kart graficznych

js, jse – tekst źródłowy JavaScript

htm – dokument hipertekstowy

htt – nagłówek hipertekstowy Microsoft Windows

hta – program hipertekstowy dla Microsoft Internet Explorer®

asp – skrypt Active Server Pages

chm – skompilowany plik HTML

pht – plik HTML ze zintegrowanymi skryptami PHP

php – skrypt zintegrowany w plikach HTML

wsh – plik Microsoft Windows Script Host

wsf – skrypt Microsoft Windows

the – plik tapety pulpitu Microsoft Windows 95

hlp – plik pomocy w formacie Win Help

msg – wiadomość pocztowa Microsoft Mail

plg – wiadomość pocztowa

mbx – zapisane wiadomości e-mail Microsoft Office Outlook

doc* – dokumenty Microsoft Office Word, takie jak: doc dla dokumentów Microsoft Office Word, docx dla dokumentów Microsoft Office Word 2007 z obsługą XML oraz docm dla dokumentów Microsoft Office Word 2007 z obsługą makr

dot* – szablony dokumentów Microsoft Office Word, takie jak: dot dla szablonów dokumentów Microsoft Office Word, dotx dla szablonów dokumentów Microsoft Office Word 2007, dotm dla szablonów dokumentów Microsoft Office Word 2007 z obsługą makr

fpm – program bazodanowy, plik startowy dla Microsoft Visual FoxPro

rtf – dokument Rich Text Format

shs – fragment Windows Shell Scrap Object Handler

dwg – baza danych programu AutoCAD®

msi – pakiet Microsoft Windows Installer

otm – projekt VBA dla Microsoft Office Outlook

pdf – dokument Adobe Acrobat

swf – obiekt pakietu Shockwave® Flash

jpg, jpeg – skompresowany format graficzny

emf – plik formatu Enhanced Metafile;

ico – plik ikony obiektu

ov? – pliki wykonywalne Microsoft Office Word

xl* – pliki i dokumenty Microsoft Office Excel, takie jak: xla dla rozszerzeń dla Microsoft Office Excel, xlc dla diagramów, xlt dla szablonów dokumentów, xlsx dla skoroszytów Microsoft Office Excel 2007, xltm dla skoroszytów Microsoft Office Excel 2007 z obsługą makr, xlsb dla skoroszytów Microsoft Office Excel 2007 w formacie binarnym (nie XML), xltx dla szablonów Microsoft Office Excel 2007, xlsm dla szablonów Microsoft Office Excel 2007 z obsługą makr oraz xlam dla wtyczek Microsoft Office Excel 2007 z obsługą makr

pp* – pliki i dokumenty Microsoft Office PowerPoint®, takie jak: pps dla slajdów Microsoft Office PowerPoint, ppt dla prezentacji, pptx dla prezentacji Microsoft Office PowerPoint 2007, pptm dla prezentacji Microsoft Office PowerPoint 2007 z obsługą makr, potx dla szablonów prezentacji Microsoft Office PowerPoint 2007, potm dla szablonów prezentacji Microsoft Office PowerPoint 2007 z obsługą makr, ppsx dla pokazów slajdów Microsoft Office PowerPoint 2007, ppsm dla pokazów slajdów Microsoft Office PowerPoint 2007 z obsługą makr oraz ppam dla wtyczek Microsoft Office PowerPoint 2007 z obsługą makr

md* – pliki i dokumenty Microsoft Office Access®, takie jak: mda dla grup roboczych Microsoft Office Access oraz mdb dla baz danych

sldx – slajd Microsoft PowerPoint 2007

sldm – slajd Microsoft PowerPoint 2007 z obsługą makr

thmx – motyw Microsoft Office 2007

Dodatek 5. Ustawienia sieci do interakcji z usługami zewnętrznymi

Kaspersky Endpoint Security i Kaspersky Security Center używają zaszyfrowanego kanału komunikacji za pośrednictwem protokołu TLS (Transport Layer Security) do pracy z zewnętrznymi usługami Kaspersky.

Kaspersky Endpoint Security używa następujących ustawień sieciowych do interakcji z usługami zewnętrznymi.

Ustawienia sieci

Adres	Opis
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protokół: `HTTPS` Port: `443`	Aktywowanie aplikacji.

Adres	Opis

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protokół: `HTTPS`
Port: `443`
	Aktualizowanie baz danych i modułów aplikacji.

`downloads.upd.kaspersky.com` Protokół: `HTTPS` Port: `443`	• Aktualizowanie baz danych i modułów aplikacji. • Weryfikacja dostępu do serwerów Kaspersky. Jeśli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja użyje publicznego DNS. Jest to konieczne, by upewnić się, że antywirusowe bazy danych są aktualizowane i że poziom bezpieczeństwa komputera jest utrzymywany. Kaspersky Endpoint Security używa poniższej listy 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 wysyłane przez aplikację mogą zawierać adresy domen i publiczny adres IP użytkownika, ponieważ aplikacja nawiązuje połączenie TCP/UDP z serwerem DNS. Te informacje są niezbędne na przykład do walidacji certyfikatu zasobu sieciowego podczas korzystania z protokołu HTTPS. Jeśli Kaspersky Endpoint Security korzysta z publicznego serwera DNS, przetwarzanie danych jest regulowane przez politykę prywatności odpowiedniej usługi. Jeśli chcesz uniemożliwić Kaspersky Endpoint Security korzystanie z publicznego serwera DNS, skontaktuj się z działem pomocy technicznej w celu uzyskania prywatnej poprawki.
`touch.kaspersky.com` Protokół: `HTTP`	• Odbieranie zaufanego czasu sprawdzania okresu ważności certyfikatu (połączenie TLS). • Ostrzeżenie o odmowie dostępu do zasobu internetowego w przeglądarce, gdy jest uruchomiona Ochrona WWW.

Adres	Opis

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Protokół: `HTTP`
Port: `80`
	Aktualizowanie baz danych i modułów aplikacji.

`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`
Protokół: `HTTPS`
Port: `443`
	Korzystanie z Kaspersky Security Network.

`ksn-a-stat-geo.kaspersky-labs.com`
`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`
Protokół: `KSN`
Port: `443`, `1443`
	Korzystanie z Kaspersky Security Network.

`click.kaspersky.com`
 	
`redirect.kaspersky.com`
Protokół: `HTTPS`
Port: `443`
	Kliknij odnośniki w interfejsie.

Ustawienia używane do szyfrowania

Adres	Opis

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protokół: `HTTP`
Port: `80`
	Infrastruktura kluczy publicznych (PKI).

Dodatek 6. Zdarzenia aplikacji

W dzienniku zdarzeń Kaspersky Security Center oraz dzienniku systemu Windows zapisywane są informacje o działaniu każdego modułu programu Kaspersky Endpoint Security, zdarzeniach szyfrowania danych, wykonaniu każdego zadania skanowania pod kątem złośliwego oprogramowania, zadania aktualizacji oraz zadania sprawdzania integralności, a także o ogólnym działaniu aplikacji.

Kaspersky Endpoint Security generuje zdarzenia następujących typów: zdarzenia ogólne i zdarzenia określone. Zdarzenia określone są tworzone tylko przez Kaspersky Endpoint Security for Windows. Zdarzenia określone posiadają prosty identyfikator, taki jak `000000cb`. Zdarzenia określone zawierają następujące wymagane parametry:

- `GNRL_EA_DESCRIPTION` to zawartość zdarzenia.
- `GNRL_EA_ID` to identyfikator usługi zdarzenia.
- `GNRL_EA_SEVERITY` to stan zdarzenia. `1` – *Informacja*, `2` – *Ostrzeżenie*, `3` – *Błąd funkcjonalny*, `4` – *Krytyczny*.
- `EVENT_TYPE_DISPLAY_NAME` to tytuł zdarzenia.
- `TASK_DISPLAY_NAME` to nazwa komponentu aplikacji, który zainicjował wystąpienie zdarzenia.

Zdarzenia ogólne mogą być tworzone przez Kaspersky Endpoint Security for Windows, a także przez inne aplikacje firmy Kaspersky (na przykład, Kaspersky Security for Windows Server). Zdarzenia ogólne zawierają bardziej złożony identyfikator, taki jak `GNRL_EV_VIRUS_FOUND`. Jako dodatek do wymaganych ustawień, zdarzenia ogólne zawierają zaawansowane ustawienia.

Długość przechowywania zdarzeń na serwerze

Krytyczny

Licencja utraciła ważność

Stan	!
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	`201`
Identyfikator zdarzenia Kaspersky Security Center	`GNRL_EV_LICENSE_EXPIRATION`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Licencja prawie utraciła ważność

Stan	!
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	`203`
Identyfikator zdarzenia Kaspersky Security Center	`000000cb`

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie odnaleziono baz danych lub są one uszkodzone

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	206
Identyfikator zdarzenia Kaspersky Security Center	000000ce
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Bazy danych są bardzo stare

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	207
Identyfikator zdarzenia Kaspersky Security Center	000000cf
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Automatyczne uruchamianie aplikacji jest wyłączone

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	209
Identyfikator zdarzenia Kaspersky Security Center	000000d1
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd aktywacji

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	229
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto aktywne zagrożenie. Należy uruchomić zaawansowane leczenie

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	231
Identyfikator zdarzenia Kaspersky Security Center	000000e7

Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Serwery KSN są niedostępne

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	2023
Identyfikator zdarzenia Kaspersky Security Center	000007e7
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Brak wystarczającej ilości miejsca w magazynie Kwarantanny

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	343
Identyfikator zdarzenia Kaspersky Security Center	00000157
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt nie został przywrócony z Kwarantanny

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	346
Identyfikator zdarzenia Kaspersky Security Center	0000015a
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt nie został usunięty z Kwarantanny

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	348
Identyfikator zdarzenia Kaspersky Security Center	0000015c
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aplikacja nawiązała połączenie ze stroną internetową z niezaufanym certyfikatem

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	57
Identyfikator zdarzenia Kaspersky Security Center	00000039

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie udało się zweryfikować połączenia szyfrowanego. Domena jest dodana do listy wykluczeń

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	`60`
Identyfikator zdarzenia Kaspersky Security Center	`0000003c`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto szkodliwy obiekt (bazy lokalne)

Stan	ⓘ
Składnik	Ochrona plików Ochrona WWW Ochrona poczty Ochrona AMSI Ochrona przed włamaniami Wykrywanie zachowań Anti-Cryptor Ochrona przed exploitami Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	`302`
Identyfikator zdarzenia Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Parametry zdarzenia	• `GNRL_EA_PARAM_1` to suma kontrolna obiektu (SHA256). • `GNRL_EA_PARAM_2` to nazwa obiektu. W przypadku wykrycia zewnętrznego szyfrowania folderów współdzielonych aplikacja wyświetli ścieżkę do pliku docelowego. • `GNRL_EA_PARAM_5` to nazwa zagrożenia zgodna z klasyfikacją Kaspersky, na przykład, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` to nazwa użytkownika sesji. • `GNRL_EA_PARAM_8` to typ zagrożenia (`typ`). • `GNRL_EA_PARAM_9` to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (`engine`). Technologia wykrywania zagrożeń (`method`). Zagrożenie wykryte przez Kaspersky Private Security Network (`blacklist`): `true` lub `false`. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto szkodliwy obiekt (KSN)

Stan	ⓘ
Składnik	Ochrona plików Ochrona WWW Ochrona poczty Ochrona AMSI Ochrona przed włamaniami Wykrywanie zachowań Anti-Cryptor Ochrona przed exploitami Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	`302`
Identyfikator zdarzenia Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Parametry zdarzenia	• `GNRL_EA_PARAM_1` to suma kontrolna obiektu (SHA256). • `GNRL_EA_PARAM_2` to nazwa obiektu. • `GNRL_EA_PARAM_5` to nazwa zagrożenia zgodna z klasyfikacją Kaspersky, na przykład, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` to nazwa użytkownika sesji. • `GNRL_EA_PARAM_8` to typ zagrożenia (`typ`). • `GNRL_EA_PARAM_9` to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (`engine`). Technologia wykrywania zagrożeń (`method`). Zagrożenie wykryte przez Kaspersky Private Security Network (`blacklist`): `true` lub `false`. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Leczenie nie jest możliwe

Stan	ⓘ
Składnik	Ochrona plików Ochrona poczty Ochrona przed włamaniami Wykrywanie zachowań Anti-Cryptor Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	`312`
Identyfikator zdarzenia Kaspersky Security Center	`GNRL_EV_OBJECT_NOTCURED`
Parametry zdarzenia	• `GNRL_EA_PARAM_1` to suma kontrolna obiektu (SHA256). • `GNRL_EA_PARAM_2` to nazwa obiektu. • `GNRL_EA_PARAM_5` to nazwa zagrożenia zgodna z klasyfikacją Kaspersky, na przykład, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` to nazwa użytkownika sesji. • `GNRL_EA_PARAM_8` to typ zagrożenia (`typ`). • `GNRL_EA_PARAM_9` to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (`engine`). Technologia wykrywania zagrożeń (`method`). Zagrożenie wykryte przez Kaspersky Private Security Network (`blacklist`): `true` lub `false`. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie można usunąć

Stan	ⓘ
Składnik	Ochrona plików Ochrona przed włamaniami Wykrywanie zachowań Anti-Cryptor Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	313
Identyfikator zdarzenia Kaspersky Security Center	00000139
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd przetwarzania

Stan	ⓘ
Składnik	Ochrona plików Ochrona WWW Ochrona poczty Ochrona przed włamaniami Ochrona AMSI Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	317
Identyfikator zdarzenia Kaspersky Security Center	0000013d
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Działanie procesu zostało zakończone

Stan	ⓘ
Składnik	Ochrona plików Ochrona przed włamaniami Wykrywanie zachowań Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	452
Identyfikator zdarzenia Kaspersky Security Center	000001c4
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie można zakończyć działania procesu

Stan	ⓘ
Składnik	Ochrona plików Ochrona przed włamaniami Wykrywanie zachowań Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	453
Identyfikator zdarzenia Kaspersky Security Center	000001c5
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Zablokowano niebezpieczny odnośnik

Stan	⚠
Składnik	Ochrona WWW
Identyfikator zdarzenia systemu Windows	362
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
Parametry zdarzenia	• GNRL_EA_PARAM_2 to ścieżka do obiektu. • GNRL_EA_PARAM_5 to nazwa obiektu zgodnie z klasyfikacją Kaspersky. • GNRL_EA_PARAM_7 to nazwa użytkownika sesji. • GNRL_EA_PARAM_8 to typ zagrożenia (typ). • GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez prywatną sieć KSN (blacklist): true Lub false.
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Otwarto szkodliwy odnośnik

Stan	⚠
Składnik	Ochrona WWW
Identyfikator zdarzenia systemu Windows	363
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_REPORTED
Parametry zdarzenia	• GNRL_EA_PARAM_2 to ścieżka do obiektu. • GNRL_EA_PARAM_5 to nazwa obiektu zgodnie z klasyfikacją Kaspersky. • GNRL_EA_PARAM_7 to nazwa użytkownika sesji. • GNRL_EA_PARAM_8 to typ zagrożenia (typ). • GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez prywatną sieć KSN (blacklist): true Lub false.
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto wcześniej otwarty niebezpieczny odnośnik

Stan	⚠
Składnik	Ochrona WWW
Identyfikator zdarzenia systemu Windows	1201
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_PASSED
Parametry zdarzenia	• GNRL_EA_PARAM_2 to ścieżka do obiektu. • GNRL_EA_PARAM_5 to nazwa obiektu zgodnie z klasyfikacją Kaspersky. • GNRL_EA_PARAM_7 to nazwa użytkownika sesji. • GNRL_EA_PARAM_8 to typ zagrożenia (typ). • GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez prywatną sieć KSN (blacklist): true Lub false.
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zablokowano akcję procesu

Stan	ⓘ
Składnik	Adaptacyjna kontrola anomalii
Identyfikator zdarzenia systemu Windows	`2200`
Identyfikator zdarzenia Kaspersky Security Center	`GNRL_EV_ADSEC_DETECT`
Parametry zdarzenia	• `GNRL_EA_PARAM_1` to nazwa reguły Adaptacyjnej kontroli anomalii. • `GNRL_EA_PARAM_2` to identyfikator reguły heurystycznej. • `GNRL_EA_PARAM_3` to nazwa użytkownika sesji. • `GNRL_EA_PARAM_4` to proces źródłowy. • `GNRL_EA_PARAM_5` to obiekt źródłowy. • `GNRL_EA_PARAM_6` to proces docelowy. • `GNRL_EA_PARAM_7` to obiekt docelowy. • `GNRL_EA_PARAM_8` to dodatkowe informacje o wykrytym obiekcie: Sumy kontrolne procesu / obiektu źródłowego oraz procesu / obiektu docelowego. Proces został zablokowany (`verdict_type`): `true` lub `false`. Identyfikator zabezpieczeń użytkownika (SID).
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Klawiatura nie została zautoryzowana

Stan	ⓘ
Składnik	Ochrona przed atakami BadUSB
Identyfikator zdarzenia systemu Windows	`2051`
Identyfikator zdarzenia Kaspersky Security Center	`00000803`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zablokowano żądanie AMSI

Stan	ⓘ
Składnik	Ochrona AMSI
Identyfikator zdarzenia systemu Windows	`2200`
Identyfikator zdarzenia Kaspersky Security Center	`00000898`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aktywność sieciowa jest zablokowana

Stan	ⓘ
Składnik	Zapora sieciowa
Identyfikator zdarzenia systemu Windows	`602`
Identyfikator zdarzenia Kaspersky Security Center	`00000329`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto atak sieciowy

Stan	ⓘ
Składnik	Ochrona sieci
Identyfikator zdarzenia systemu Windows	651
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_ATTACK_DETECTED
Parametry zdarzenia	• GNRL_EA_PARAM_1 to nazwa ataku. • GNRL_EA_PARAM_2 to protokół. • GNRL_EA_PARAM_3 to adres IP komputera pełniącego rolę źródła ataku sieciowego. Adres IP został wskazany kolejności bajtów hosta. Na przykład: 2886729929 dla 172.16.0.201. • GNRL_EA_PARAM_4 to numer portu. • GNRL_EA_PARAM_5 to adres IPv6, na przykład, 12B012B012B012B012B012B012B012B0. • GNRL_EA_PARAM_6 to adres IP komputera będącego celem ataku sieciowego. Adres IP został wskazany kolejności bajtów hosta. Na przykład: 2886729929 dla 172.16.0.201.
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zabroniono uruchomienia aplikacji

Stan	ⓘ
Składnik	Kontrola aplikacji
Identyfikator zdarzenia systemu Windows	702
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_APPLICATION_LAUNCH_DENIED
Parametry zdarzenia	• GNRL_EA_PARAM_2 to nazwa użytkownika sesji. • GNRL_EA_PARAM_3 to ręcznie utworzony identyfikator kategorii. • GNRL_EA_PARAM_4 to identyfikator kategorii aplikacji. • GNRL_EA_PARAM_5 to informacje o cyfrowym podpisie aplikacji. • GNRL_EA_PARAM_6 to nazwa pliku wykonywalnego aplikacji (na przykład: chrome.exe). • GNRL_EA_PARAM_7 to ścieżka do pliku wykonywalnego. • GNRL_EA_PARAM_8 to suma kontrolna obiektu (SHA256). • GNRL_EA_PARAM_9 to wersja aplikacji, którą użytkownik próbuje uruchomić.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zabroniony proces został uruchomiony przed Kaspersky Endpoint Security

Stan	ⓘ
Składnik	Kontrola aplikacji
Identyfikator zdarzenia systemu Windows	710
Identyfikator zdarzenia Kaspersky Security Center	000002c6
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Dostęp zabroniony (bazy lokalne)

Stan	ⓘ
Składnik	Kontrola sieci

Identyfikator zdarzenia systemu Windows	752
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Parametry zdarzenia	• GNRL_EA_PARAM_1 to adres internetowy. • GNRL_EA_PARAM_2 to nazwa użytkownika sesji. • GNRL_EA_PARAM_3 to nazwa reguły Kontroli sieci.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Dostęp zabroniony (KSN)

Stan	ⓘ
Składnik	Kontrola sieci
Identyfikator zdarzenia systemu Windows	752
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Parametry zdarzenia	• GNRL_EA_PARAM_1 to adres internetowy. • GNRL_EA_PARAM_2 to nazwa użytkownika sesji. • GNRL_EA_PARAM_3 to nazwa reguły Kontroli sieci.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Działania na urządzeniu zostały zabronione

Stan	ⓘ
Składnik	Kontrola urządzeń
Identyfikator zdarzenia systemu Windows	802
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parametry zdarzenia	• GNRL_EA_PARAM_1 to ID sprzętu (HWID). • GNRL_EA_PARAM_2 to nazwa użytkownika sesji.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Połączenie sieciowe zablokowane

Stan	ⓘ
Składnik	Kontrola urządzeń
Identyfikator zdarzenia systemu Windows	809
Identyfikator zdarzenia Kaspersky Security Center	00000329
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas aktualizacji składnika

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1011
Identyfikator zdarzenia Kaspersky Security Center	000003f3

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas dystrybucji aktualizacji składników

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1012
Identyfikator zdarzenia Kaspersky Security Center	000003f4
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Lokalny błąd aktualizacji

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1014
Identyfikator zdarzenia Kaspersky Security Center	000003f6
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Sieciowy błąd aktualizacji

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1015
Identyfikator zdarzenia Kaspersky Security Center	000003f7
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Nie można uruchomić dwóch zadań w tym samym czasie

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1017
Identyfikator zdarzenia Kaspersky Security Center	000003f9
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas weryfikacji baz danych oraz modułów aplikacji

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1018
Identyfikator zdarzenia Kaspersky Security Center	000003fa

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd współdziałania z Kaspersky Security Center

Stan	!
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1019
Identyfikator zdarzenia Kaspersky Security Center	000003fb
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie wszystkie składniki zostały zaktualizowane

Stan	!
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1021
Identyfikator zdarzenia Kaspersky Security Center	000003fd
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aktualizacja została pomyślnie zakończona, dystrybucja uaktualnień nie powiodła się

Stan	!
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1023
Identyfikator zdarzenia Kaspersky Security Center	000003ff
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wewnętrzny błąd zadania

Stan	!
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	101
Identyfikator zdarzenia Kaspersky Security Center	00000065
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Instalacja poprawki nie powiodła się

Stan	!
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	2153
Identyfikator zdarzenia Kaspersky Security Center	00000869

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wycofanie poprawki nie powiodło się

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	`2156`
Identyfikator zdarzenia Kaspersky Security Center	`0000086C`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas stosowania reguł szyfrowania / odszyfrowywania pliku

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	`904`
Identyfikator zdarzenia Kaspersky Security Center	`00000388`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas szyfrowania / odszyfrowywania pliku

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	`912`
Identyfikator zdarzenia Kaspersky Security Center	`GNRL_EV_ENCRYPTION_ERROR`
Parametry zdarzenia	• `GNRL_EA_PARAM_1` to ścieżka do pliku. • `GNRL_EA_PARAM_2` to przyczyna wystąpienia błędu. • `GNRL_EA_PARAM_3` to typ urządzenia.
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zablokowano dostęp do pliku

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	`940`
Identyfikator zdarzenia Kaspersky Security Center	`GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION`
Parametry zdarzenia	• `GNRL_EA_PARAM_1` to obiekt docelowy. • `GNRL_EA_PARAM_2` to nazwa użytkownika sesji. • `GNRL_EA_PARAM_3` to nazwa pliku wykonywalnego aplikacji (na przykład, chrome.exe), która próbuje uzyskać dostęp do pliku.
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Błąd podczas włączania trybu przenośnego

Stan	!
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	951
Identyfikator zdarzenia Kaspersky Security Center	000003b7
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas wyłączania trybu przenośnego

Stan	!
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	953
Identyfikator zdarzenia Kaspersky Security Center	000003b9
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas tworzenia zaszyfrowanego pakietu

Stan	!
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	931
Identyfikator zdarzenia Kaspersky Security Center	000003a3
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas szyfrowania/odszyfrowywania urządzenia

Stan	!
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1305
Identyfikator zdarzenia Kaspersky Security Center	00000519
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie można wczytać modułu szyfrującego

Stan	!
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1311
Identyfikator zdarzenia Kaspersky Security Center	0000051f
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zadanie zarządzające kontami Agenta autoryzacji zostało zakończone z błędem

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1340
Identyfikator zdarzenia Kaspersky Security Center	0000053c
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zasada nie może zostać zastosowana

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	1312
Identyfikator zdarzenia Kaspersky Security Center	00000520
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aktualizacja FDE zakończyła się niepowodzeniem

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1342
Identyfikator zdarzenia Kaspersky Security Center	0000053e
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Cofanie aktualizacji FDE zakończyło się niepowodzeniem (aby dowiedzieć się więcej, przejdź do systemu pomocy online Kaspersky Endpoint Security)

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1344
Identyfikator zdarzenia Kaspersky Security Center	00000540
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Serwer Kaspersky Anti Targeted Attack Platform jest niedostępny

Stan	ⓘ
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2100
Identyfikator zdarzenia Kaspersky Security Center	00000834
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Usunięcie obiektu nie powiodło się

Stan	!
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2252
Identyfikator zdarzenia Kaspersky Security Center	000008cc
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt nie został poddany kwarantannie (Sandbox)

Stan	!
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2603
Identyfikator zdarzenia Kaspersky Security Center	00000a2b
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wystąpił błąd wewnętrzny

Stan	!
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2607
Identyfikator zdarzenia Kaspersky Security Center	00000a2f
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy certyfikat serwera Sandbox

Stan	!
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2613
Identyfikator zdarzenia Kaspersky Security Center	00000a35
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Węzeł Sandbox jest niedostępny

Stan	!
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2614
Identyfikator zdarzenia Kaspersky Security Center	00000a36
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie udało się przetworzyć obiektu w Sandbox

Stan	!
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2617
Identyfikator zdarzenia Kaspersky Security Center	00000a39
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Przekroczono maksymalne obciążenie Sandbox

Stan	!
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2618
Identyfikator zdarzenia Kaspersky Security Center	00000a3a
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Znaleziono przerwanie IOC

Stan	!
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2651
Identyfikator zdarzenia Kaspersky Security Center	00000a5b
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd weryfikacji licencji Sandbox

Stan	!
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2620
Identyfikator zdarzenia Kaspersky Security Center	00000a3c
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Użytkownikowi nie udało się wysłać zadania skanowania do środowiska Sandbox

Stan	!
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2623
Identyfikator zdarzenia Kaspersky Security Center	00000a3e
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas tworzenia zadania Sandbox

Stan	ⓘ
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2621
Identyfikator zdarzenia Kaspersky Security Center	00000a3d
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zablokowano uruchamianie obiektu

Stan	ⓘ
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2553
Identyfikator zdarzenia Kaspersky Security Center	000009f9
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zablokowano uruchamianie procesu

Stan	ⓘ
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2551
Identyfikator zdarzenia Kaspersky Security Center	000009f7
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zablokowano wykonywanie skryptu

Stan	ⓘ
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2559
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt nie został poddany kwarantannie (Endpoint Detection and Response)

Stan	ⓘ
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2556
Identyfikator zdarzenia Kaspersky Security Center	000009fc
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Uruchamianie procesów nie jest zablokowane

Stan	ⓘ
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2561
Identyfikator zdarzenia Kaspersky Security Center	00000a01
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt nie jest zablokowany

Stan	ⓘ
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2562
Identyfikator zdarzenia Kaspersky Security Center	00000a02
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykonywanie skryptów nie jest zablokowane

Stan	ⓘ
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2563
Identyfikator zdarzenia Kaspersky Security Center	00000a03
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas zmiany składników aplikacji

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	1401
Identyfikator zdarzenia Kaspersky Security Center	00000579
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

W systemie istnieją wzorce możliwego ataku siłowego

Stan	ⓘ
Składnik	Kontrola dziennika
Identyfikator zdarzenia systemu Windows	2800
Identyfikator zdarzenia Kaspersky Security Center	00000af0
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

W systemie istnieją wzorce możliwego nadużycia dziennika zdarzeń systemu Windows

Stan	!
Składnik	Kontrola dziennika
Identyfikator zdarzenia systemu Windows	`2801`
Identyfikator zdarzenia Kaspersky Security Center	`00000af1`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto nietypowe działania w imieniu nowej zainstalowanej usługi

Stan	!
Składnik	Kontrola dziennika
Identyfikator zdarzenia systemu Windows	`2802`
Identyfikator zdarzenia Kaspersky Security Center	`00000af2`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto nietypowe logowanie wykorzystujące jawne dane uwierzytelniające

Stan	!
Składnik	Kontrola dziennika
Identyfikator zdarzenia systemu Windows	`2803`
Identyfikator zdarzenia Kaspersky Security Center	`00000af3`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

W systemie istnieją wzorce możliwego ataku Kerberos PAC (MS14-068)

Stan	!
Składnik	Kontrola dziennika
Identyfikator zdarzenia systemu Windows	`2804`
Identyfikator zdarzenia Kaspersky Security Center	`00000af4`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Podejrzane zmiany wykryte w uprzywilejowanej wbudowanej grupie Administratorzy

Stan	!
Składnik	Kontrola dziennika
Identyfikator zdarzenia systemu Windows	`2805`
Identyfikator zdarzenia Kaspersky Security Center	`00000af5`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Podczas sesji logowania do sieci wykryto nietypową aktywność

Stan	!
Składnik	Kontrola dziennika
Identyfikator zdarzenia systemu Windows	2806
Identyfikator zdarzenia Kaspersky Security Center	00000af6
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wyzwolono regułę kontroli dziennika

Stan	!
Składnik	Kontrola dziennika
Identyfikator zdarzenia systemu Windows	2807
Identyfikator zdarzenia Kaspersky Security Center	00000af7
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zdarzenie nietypowe występuje zbyt często. Uruchomiono agregację zdarzeń

Stan	!
Składnik	Kontrola dziennika
Identyfikator zdarzenia systemu Windows	2808
Identyfikator zdarzenia Kaspersky Security Center	00000af8
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Raport o nietypowym zdarzeniu dla okresu agregacji

Stan	!
Składnik	Kontrola dziennika
Identyfikator zdarzenia systemu Windows	2809
Identyfikator zdarzenia Kaspersky Security Center	00000af9
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas nawiązywania połączenia z serwerem EDR Expert

Stan	!
Składnik	Endpoint Detection and Response Expert (on-premises)
Identyfikator zdarzenia systemu Windows	2850
Identyfikator zdarzenia Kaspersky Security Center	00000b22
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy certyfikat serwera EDR Expert

Stan	!
Składnik	Endpoint Detection and Response Expert (on-premises)
Identyfikator zdarzenia systemu Windows	2851
Identyfikator zdarzenia Kaspersky Security Center	00000b23
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy certyfikat agenta na serwerze EDR Expert

Stan	!
Składnik	Endpoint Detection and Response Expert (on-premises)
Identyfikator zdarzenia systemu Windows	2852
Identyfikator zdarzenia Kaspersky Security Center	00000b24
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas nawiązywania połączenia z serwerem odpowiedzi EDR Expert

Stan	!
Składnik	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identyfikator zdarzenia systemu Windows	2858
Identyfikator zdarzenia Kaspersky Security Center	00000b22
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy certyfikat serwera odpowiedzi EDR Expert

Stan	!
Składnik	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identyfikator zdarzenia systemu Windows	2859
Identyfikator zdarzenia Kaspersky Security Center	00000b23
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy certyfikat agenta na serwerze odpowiedzi EDR Expert

Stan	!
Składnik	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identyfikator zdarzenia systemu Windows	2860
Identyfikator zdarzenia Kaspersky Security Center	00000b24

Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd połączenia z serwerem gromadzenia danych telemetrycznych EDR Expert

Stan	ⓘ
Składnik	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identyfikator zdarzenia systemu Windows	`2854`
Identyfikator zdarzenia Kaspersky Security Center	`00000b22`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy certyfikat serwera gromadzenia danych telemetrycznych EDR Expert

Stan	ⓘ
Składnik	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identyfikator zdarzenia systemu Windows	`2855`
Identyfikator zdarzenia Kaspersky Security Center	`00000b23`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy certyfikat agenta na serwerze gromadzenia danych telemetrycznych EDR Expert

Stan	ⓘ
Składnik	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identyfikator zdarzenia systemu Windows	`2856`
Identyfikator zdarzenia Kaspersky Security Center	`00000b24`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas nawiązywania połączenia z serwerem NDR

Stan	ⓘ
Składnik	Network Detection and Response (KATA)
Identyfikator zdarzenia systemu Windows	`3080`
Identyfikator zdarzenia Kaspersky Security Center	`00000c08`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy certyfikat serwera NDR

Stan	ⓘ
Składnik	Network Detection and Response (KATA)
Identyfikator zdarzenia systemu Windows	`3081`

Identyfikator zdarzenia Kaspersky Security Center	00000c09
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy certyfikat agenta na serwerze NDR

Stan	ⓘ
Składnik	Network Detection and Response (KATA)
Identyfikator zdarzenia systemu Windows	3082
Identyfikator zdarzenia Kaspersky Security Center	00000c0a
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Twoje urządzenie jest połączone z niezaufanym serwerem administracyjnym. Skontaktuj się z administratorem

Stan	ⓘ
Składnik	Ochrona połączenia z Serwerem administracyjnym
Identyfikator zdarzenia systemu Windows	3301
Identyfikator zdarzenia Kaspersky Security Center	00000ce5
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto zmianę pliku lub folderu

Stan	ⓘ / ⚠ / ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2950
Identyfikator zdarzenia Kaspersky Security Center	00000b86
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu*.

Obiekt zbyt często ulega zmianom. Rozpoczęto agregację zdarzeń

Stan	ⓘ / ⚠ / ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2955
Identyfikator zdarzenia Kaspersky Security Center	00000b8b
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Raport o modyfikacji obiektu dla okresu agregacji

Stan	ⓘ / ⚠ / ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2956
Identyfikator zdarzenia Kaspersky Security Center	00000b8c
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Zakres monitorowania obejmuje nieprawidłowe obiekty

Stan	ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2953
Identyfikator zdarzenia Kaspersky Security Center	00000b89
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zmiana rejestru została wykryta

Stan	ⓘ / ⚠ / ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2951
Identyfikator zdarzenia Kaspersky Security Center	00000b87
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Wykryto podłączenie/odłączenie urządzenia

Stan	ⓘ / ⚠ / ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2952
Identyfikator zdarzenia Kaspersky Security Center	00000b88
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Zakres monitorowania obejmuje nieprawidłowe obiekty

Stan	/ /
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2903
Identyfikator zdarzenia Kaspersky Security Center	00000b89
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Zbyt wiele prób wykonania zabronionych operacji na obiekcie. Rozpoczęto agregację zdarzeń

Stan	
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2963
Identyfikator zdarzenia Kaspersky Security Center	00000b93
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Operacja z plikami objętymi zakresem monitorowania została zablokowana

Stan	
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2959
Identyfikator zdarzenia Kaspersky Security Center	00000b8f
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Zablokowano modyfikację rejestru

Stan	
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2960
Identyfikator zdarzenia Kaspersky Security Center	00000b90
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Błąd przetwarzania

Stan	ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2954
Identyfikator zdarzenia Kaspersky Security Center	00000b8a
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Monitor integralności systemu: wyzwalanie reguły wyłączone dla kont użytkowników bez pasującego identyfikatora zabezpieczeń (SID)

Stan	ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2964
Identyfikator zdarzenia Kaspersky Security Center	00000b94
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Kontrola aplikacji: wyzwalanie reguły wyłączone dla kont użytkowników bez pasującego identyfikatora zabezpieczeń (SID)

Stan	ⓘ
Składnik	Kontrola aplikacji
Identyfikator zdarzenia systemu Windows	711
Identyfikator zdarzenia Kaspersky Security Center	000002c7
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Kontrola urządzeń: wyzwalanie reguły wyłączone dla kont użytkowników bez pasującego identyfikatora zabezpieczeń (SID)

Stan	ⓘ
Składnik	Kontrola urządzeń
Identyfikator zdarzenia systemu Windows	810
Identyfikator zdarzenia Kaspersky Security Center	0000032a
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Kontrola sieci: wyzwalanie reguły wyłączone dla kont użytkowników bez pasującego identyfikatora zabezpieczeń (SID)

Stan	ⓘ
Składnik	Kontrola sieci
Identyfikator zdarzenia systemu Windows	757
Identyfikator zdarzenia Kaspersky Security Center	000002f5
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Adaptacyjna kontrola anomalii: wyzwalanie reguły wyłączone dla kont użytkowników bez pasującego identyfikatora zabezpieczeń (SID)

Stan	ⓘ
Składnik	Adaptacyjna kontrola anomalii
Identyfikator zdarzenia systemu Windows	504
Identyfikator zdarzenia Kaspersky Security Center	000001f8
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Kontrola dziennika: wyzwalanie reguły wyłączone dla kont użytkowników bez pasującego identyfikatora zabezpieczeń (SID)

Stan	ⓘ
Składnik	Kontrola dziennika
Identyfikator zdarzenia systemu Windows	2810
Identyfikator zdarzenia Kaspersky Security Center	00000afa
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie można połączyć się z serwerem integracji przez ponad 6 godzin. Sprawdź stan serwera integracji i ustawienia sieciowe

Stan	ⓘ
Składnik	Light Agent
Identyfikator zdarzenia systemu Windows	3103
Identyfikator zdarzenia Kaspersky Security Center	00000c1f
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

SVM jest niedostępny

Stan	ⓘ
Składnik	Light Agent
Identyfikator zdarzenia systemu Windows	3151
Identyfikator zdarzenia Kaspersky Security Center	00000c4f
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto złośliwy obiekt. Zaawansowana dezynfekcja powinna zostać uruchomiona na szablonie maszyny wirtualnej

Stan	ⓘ
Składnik	Light Agent
Identyfikator zdarzenia systemu Windows	3182
Identyfikator zdarzenia Kaspersky Security Center	00000c6e

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Połączenie sieciowe nawiązane przy użyciu przestarzałego protokołu zostało zablokowane

Stan	ⓘ
Składnik	Ochrona
Identyfikator zdarzenia systemu Windows	75
Identyfikator zdarzenia Kaspersky Security Center	0000004b
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd połączenia z serwerem KUMA

Stan	ⓘ
Składnik	Integracja KUMA
Identyfikator zdarzenia systemu Windows	2854
Identyfikator zdarzenia Kaspersky Security Center	00000b26
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy certyfikat serwera KUMA

Stan	ⓘ
Składnik	Integracja KUMA
Identyfikator zdarzenia systemu Windows	2855
Identyfikator zdarzenia Kaspersky Security Center	00000b27
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy certyfikat agenta na serwerze KUMA

Stan	ⓘ
Składnik	Integracja KUMA
Identyfikator zdarzenia systemu Windows	2856
Identyfikator zdarzenia Kaspersky Security Center	00000b28
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd funkcjonalny

Zadanie nie może zostać wykonane

Stan	!
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	212
Identyfikator zdarzenia Kaspersky Security Center	000000d4
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowe ustawienia zadania. Ustawienia nie zostały zastosowane

Stan	!
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	707
Identyfikator zdarzenia Kaspersky Security Center	000002c3
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Ostrzeżenie

Aplikacja uległa awarii podczas poprzedniej sesji

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	237
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Licencja wkrótce utraci ważność

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	204
Identyfikator zdarzenia Kaspersky Security Center	000000cc
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Bazy danych są nieaktualne

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	208
Identyfikator zdarzenia Kaspersky Security Center	000000d0

Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Automatyczna aktualizacja jest wyłączona

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	210
Identyfikator zdarzenia Kaspersky Security Center	000000d2
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Autoochrona jest wyłączona

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	211
Identyfikator zdarzenia Kaspersky Security Center	000000d3
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Składniki ochrony są wyłączone

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	214
Identyfikator zdarzenia Kaspersky Security Center	000000d6
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Komputer działa w trybie awaryjnym

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	215
Identyfikator zdarzenia Kaspersky Security Center	000000d7
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Istnieją nieprzetworzone pliki

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	216
Identyfikator zdarzenia Kaspersky Security Center	000000d8

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zasady grupy zostały zastosowane

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	219
Identyfikator zdarzenia Kaspersky Security Center	000000db
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zadanie zostało zatrzymane

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	222
Identyfikator zdarzenia Kaspersky Security Center	000000de
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

W calu zakończenia aktualizacji zamknij aplikację, a następnie otwórz ponownie

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	224
Identyfikator zdarzenia Kaspersky Security Center	0000057b
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wymagane jest ponowne uruchomienie komputera

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	225
Identyfikator zdarzenia Kaspersky Security Center	000000e1
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Licencja uprawnia do korzystania ze składników, które nie są zainstalowane

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	226
Identyfikator zdarzenia Kaspersky Security Center	000000e2

Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Uruchomiono zaawansowane leczenie

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	232
Identyfikator zdarzenia Kaspersky Security Center	000000e8
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zakończono zaawansowane leczenie

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	233
Identyfikator zdarzenia Kaspersky Security Center	000000e9
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nieprawidłowy klucz zapasowy

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	230
Identyfikator zdarzenia Kaspersky Security Center	000000e6
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Subskrypcja wkrótce utraci ważność

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	240
Identyfikator zdarzenia Kaspersky Security Center	000000f0
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zablokowano

Stan	⚠
Składnik	Wykrywanie zachowań Anti-Cryptor Ochrona przed exploitami Ochrona WWW
Identyfikator zdarzenia systemu Windows	331

Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
Parametry zdarzenia	• GNRL_EA_PARAM_1 to suma kontrolna obiektu (SHA256). • GNRL_EA_PARAM_2 to nazwa obiektu. W przypadku wykrycia zewnętrznego szyfrowania folderów współdzielonych aplikacja wyświetli ścieżkę do pliku docelowego. • GNRL_EA_PARAM_5 to nazwa zagrożenia zgodna z klasyfikacją Kaspersky, na przykład, EICAR-Test-File. • GNRL_EA_PARAM_7 to nazwa użytkownika sesji. • GNRL_EA_PARAM_8 to typ zagrożenia (typ). • GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez Kaspersky Private Security Network (blacklist): true lub false. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Ustawienia systemu operacyjnego nie pozwalają na kontrolowanie dostępu do sieci Wi-Fi

Stan	⚠
Składnik	Kontrola urządzeń
Identyfikator zdarzenia systemu Windows	249
Identyfikator zdarzenia Kaspersky Security Center	000000f9
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Obiekt nie został przywrócony z kopii zapasowej

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	336
Identyfikator zdarzenia Kaspersky Security Center	00000150
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wykryto podejrzaną aktywność sieciową

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	2001
Identyfikator zdarzenia Kaspersky Security Center	000007d1
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Przerwano zaszyfrowane połączenie

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	250
Identyfikator zdarzenia Kaspersky Security Center	000007d3
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Uczestnictwo w KSN jest wyłączone

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	2021
Identyfikator zdarzenia Kaspersky Security Center	000007e5
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Przetwarzanie pewnych funkcji systemu operacyjnego jest wyłączone

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	245
Identyfikator zdarzenia Kaspersky Security Center	000000f5
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Magazyn Kwarantanny jest prawie przepełniony

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	344
Identyfikator zdarzenia Kaspersky Security Center	00000158
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Połączenie sieciowe zablokowane

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	809
Identyfikator zdarzenia Kaspersky Security Center	00000abe
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie można utworzyć kopii zapasowej

Stan	⚠
Składnik	Ochrona plików Ochrona poczty Ochrona przed włamaniami Ochrona AMSI Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	`314`
Identyfikator zdarzenia Kaspersky Security Center	`GNRL_EV_OBJECT_REPORTED`
Parametry zdarzenia	• `GNRL_EA_PARAM_1` to suma kontrolna obiektu (SHA256). • `GNRL_EA_PARAM_2` to nazwa obiektu. • `GNRL_EA_PARAM_5` to nazwa zagrożenia zgodna z klasyfikacją Kaspersky, na przykład, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` to nazwa użytkownika sesji. • `GNRL_EA_PARAM_8` to typ zagrożenia (`typ`). • `GNRL_EA_PARAM_9` to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (`engine`). Technologia wykrywania zagrożeń (`method`). Zagrożenie wykryte przez Kaspersky Private Security Network (`blacklist`): `true` lub `false`. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Stan	⚠
Składnik	Ochrona plików Wykrywanie zachowań Anti-Cryptor Ochrona przed włamaniami Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	`310`
Identyfikator zdarzenia Kaspersky Security Center	`00000136`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt zaszyfrowany

Stan	⚠
Składnik	Ochrona przed włamaniami
Identyfikator zdarzenia systemu Windows	`320`
Identyfikator zdarzenia Kaspersky Security Center	`00000140`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Obiekt uszkodzony

Stan	⚠
Składnik	Ochrona plików Ochrona WWW Ochrona poczty Ochrona AMSI Ochrona przed włamaniami Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	`321`
Identyfikator zdarzenia Kaspersky Security Center	`00000141`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wykryto legalne oprogramowanie, które może zostać wykorzystane przez intruzów do uszkodzenia komputera lub prywatnych danych (bazy lokalne)

Stan	⚠
Składnik	Ochrona plików Ochrona WWW Ochrona poczty Ochrona przed włamaniami Ochrona AMSI Wykrywanie zachowań Anti-Cryptor Anti-Cryptor Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	`303`
Identyfikator zdarzenia Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Parametry zdarzenia	• `GNRL_EA_PARAM_1` to suma kontrolna obiektu (SHA256). • `GNRL_EA_PARAM_2` to nazwa obiektu. • `GNRL_EA_PARAM_5` to nazwa zagrożenia zgodna z klasyfikacją Kaspersky, na przykład, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` to nazwa użytkownika sesji. • `GNRL_EA_PARAM_8` to typ zagrożenia (`typ`).
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto legalne oprogramowanie, które może zostać wykorzystane przez intruzów do uszkodzenia komputera lub prywatnych danych (KSN)

Stan	⚠
Składnik	Ochrona plików Ochrona WWW Ochrona poczty Ochrona przed włamaniami Ochrona AMSI Wykrywanie zachowań Anti-Cryptor Anti-Cryptor Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	`303`

Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_BY_KSN
Parametry zdarzenia	• GNRL_EA_PARAM_1 to suma kontrolna obiektu (SHA256). • GNRL_EA_PARAM_2 to nazwa obiektu. • GNRL_EA_PARAM_5 to nazwa zagrożenia zgodna z klasyfikacją Kaspersky, na przykład, EICAR-Test-File. • GNRL_EA_PARAM_7 to nazwa użytkownika sesji. • GNRL_EA_PARAM_8 to typ zagrożenia (typ).
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt usunięty

Stan	⚠
Składnik	Ochrona plików Ochrona poczty Ochrona przed włamaniami Ochrona przed exploitami Wykrywanie zachowań Anti-Cryptor Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	307
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_OBJECT_DELETED
Parametry zdarzenia	• GNRL_EA_PARAM_1 to suma kontrolna obiektu (SHA256). • GNRL_EA_PARAM_2 to nazwa obiektu. • GNRL_EA_PARAM_5 to nazwa zagrożenia zgodna z klasyfikacją Kaspersky, na przykład, EICAR-Test-File. • GNRL_EA_PARAM_7 to nazwa użytkownika sesji. • GNRL_EA_PARAM_8 to typ zagrożenia (typ). • GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez Kaspersky Private Security Network (blacklist): true lub false. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt wyleczony

Stan	⚠
Składnik	Ochrona plików Ochrona poczty Ochrona przed włamaniami Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	306

Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_OBJECT_CURED
Parametry zdarzenia	• GNRL_EA_PARAM_1 to suma kontrolna obiektu (SHA256). • GNRL_EA_PARAM_2 to nazwa obiektu. • GNRL_EA_PARAM_5 to nazwa zagrożenia zgodna z klasyfikacją Kaspersky, na przykład, EICAR-Test-File. • GNRL_EA_PARAM_7 to nazwa użytkownika sesji. • GNRL_EA_PARAM_8 to typ zagrożenia (typ). • GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez Kaspersky Private Security Network (blacklist): true lub false. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt zostanie wyleczony po ponownym uruchomieniu

Stan	⚠
Składnik	Ochrona przed włamaniami Ochrona plików Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	324
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Obiekt zostanie usunięty po ponownym uruchomieniu

Stan	⚠
Składnik	Wykrywanie zachowań Anti-Cryptor Ochrona przed exploitami Ochrona przed włamaniami Ochrona plików Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	323
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Obiekt usunięty zgodnie z ustawieniami

Stan	⚠
Składnik	Ochrona poczty
Identyfikator zdarzenia systemu Windows	342
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Zakończono wycofywanie

Stan	⚠
Składnik	Ochrona plików Wykrywanie zachowań Anti-Cryptor Ochrona przed exploitami Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	`455`
Identyfikator zdarzenia Kaspersky Security Center	`000001c7`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Pobranie obiektu zostało zablokowane

Stan	⚠
Składnik	Ochrona WWW
Identyfikator zdarzenia systemu Windows	`341`
Identyfikator zdarzenia Kaspersky Security Center	`GNRL_EV_OBJECT_BLOCKED`
Parametry zdarzenia	• `GNRL_EA_PARAM_1` to suma kontrolna obiektu (SHA256). • `GNRL_EA_PARAM_2` to nazwa obiektu. • `GNRL_EA_PARAM_5` to nazwa zagrożenia zgodna z klasyfikacją Kaspersky, na przykład, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` to nazwa użytkownika sesji. • `GNRL_EA_PARAM_8` to typ zagrożenia (`typ`). • `GNRL_EA_PARAM_9` to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (`engine`). Technologia wykrywania zagrożeń (`method`). Zagrożenie wykryte przez Kaspersky Private Security Network (`blacklist`): `true` lub `false`. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd autoryzacji klawiatury

Stan	⚠
Składnik	Ochrona przed atakami BadUSB
Identyfikator zdarzenia systemu Windows	`2052`
Identyfikator zdarzenia Kaspersky Security Center	`00000804`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wynik skanowania obiektu został wysłany do zewnętrznej aplikacji

Stan	⚠
Składnik	Ochrona AMSI
Identyfikator zdarzenia systemu Windows	`1512`

Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
Parametry zdarzenia	• GNRL_EA_PARAM_1 to suma kontrolna obiektu (SHA256). • GNRL_EA_PARAM_2 to nazwa obiektu. • GNRL_EA_PARAM_5 to nazwa zagrożenia zgodna z klasyfikacją Kaspersky, na przykład, EICAR-Test-File. • GNRL_EA_PARAM_7 to nazwa użytkownika sesji. • GNRL_EA_PARAM_8 to typ zagrożenia (typ). • GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez Kaspersky Private Security Network (blacklist): true lub false. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Ustawienia zadania zostały pomyślnie zastosowane

Stan	⚠
Składnik	Kontrola aplikacji
Identyfikator zdarzenia systemu Windows	708
Identyfikator zdarzenia Kaspersky Security Center	000002c4
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Ostrzeżenie o niechcianej zawartości (bazy lokalne)

Stan	⚠
Składnik	Kontrola sieci
Identyfikator zdarzenia systemu Windows	708
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parametry zdarzenia	• GNRL_EA_PARAM_1 to adres internetowy. • GNRL_EA_PARAM_2 to nazwa użytkownika sesji. • GNRL_EA_PARAM_3 to nazwa reguły Kontroli sieci.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Ostrzeżenie o niechcianej zawartości (KSN)

Stan	⚠
Składnik	Kontrola sieci
Identyfikator zdarzenia systemu Windows	708
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parametry zdarzenia	• GNRL_EA_PARAM_1 to adres internetowy. • GNRL_EA_PARAM_2 to nazwa użytkownika sesji. • GNRL_EA_PARAM_3 to nazwa reguły Kontroli sieci.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Uzyskano dostęp do niechcianej zawartości po wyświetleniu ostrzeżenia

Stan	⚠
Składnik	Kontrola sieci
Identyfikator zdarzenia systemu Windows	754
Identyfikator zdarzenia Kaspersky Security Center	000002f2
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Aktywowano tymczasowy dostęp do urządzenia

Stan	⚠
Składnik	Kontrola urządzeń
Identyfikator zdarzenia systemu Windows	803
Identyfikator zdarzenia Kaspersky Security Center	000002f2
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Operacja została anulowana przez użytkownika

Stan	⚠
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1016
Identyfikator zdarzenia Kaspersky Security Center	000003f8
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Użytkownik zrezygnował z zasady szyfrowania

Stan	⚠
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1306
Identyfikator zdarzenia Kaspersky Security Center	0000051a
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Przerwano stosowanie reguł szyfrowania / odszyfrowywania pliku

Stan	⚠
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	903
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Przerwano szyfrowanie / odszyfrowywanie pliku

Stan	⚠
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	914
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Przerwano szyfrowanie / odszyfrowywanie urządzenia

Stan	⚠
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1303
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Nie udało się zainstalować lub zaktualizować sterowników Kaspersky Disk Encryption w obrazie WinRE

Stan	⚠
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1345
Identyfikator zdarzenia Kaspersky Security Center	00000541
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Sprawdzanie sygnatury modułu zakończyło się niepowodzeniem

Stan	⚠
Składnik	Sprawdzanie integralności systemu
Identyfikator zdarzenia systemu Windows	2002
Identyfikator zdarzenia Kaspersky Security Center	000007d2
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Uruchomienie aplikacji zostało zablokowane

Stan	⚠
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2105
Identyfikator zdarzenia Kaspersky Security Center	00000839
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Otwarcie dokumentu zostało zablokowane

Stan	⚠
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2106
Identyfikator zdarzenia Kaspersky Security Center	0000083a
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Proces został zakończony przez administratora serwera Kaspersky Anti Targeted Attack Platform

Stan	⚠
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2112
Identyfikator zdarzenia Kaspersky Security Center	00000840
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aplikacja została zakończona przez administratora serwera Kaspersky Anti Targeted Attack Platform

Stan	⚠
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2113
Identyfikator zdarzenia Kaspersky Security Center	00000841
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Plik lub strumień został usunięty przez administratora serwera Kaspersky Anti Targeted Attack Platform

Stan	⚠
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2111
Identyfikator zdarzenia Kaspersky Security Center	0000083f
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Plik został przywrócony z kwarantanny z serwera Kaspersky Anti Targeted Attack Platform przez administratora

Stan	⚠
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2110
Identyfikator zdarzenia Kaspersky Security Center	0000083e
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Plik został przeniesiony do kwarantanny na serwer Kaspersky Anti Targeted Attack Platform przez administratora

Stan	⚠
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2109
Identyfikator zdarzenia Kaspersky Security Center	0000083d
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aktywność sieciowa aplikacji firm trzecich została zablokowana

Stan	⚠
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2107
Identyfikator zdarzenia Kaspersky Security Center	0000083b
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aktywność sieciowa aplikacji firm trzecich została odblokowana

Stan	⚠
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2108
Identyfikator zdarzenia Kaspersky Security Center	0000083c
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt zostanie usunięty po ponownym uruchomieniu (Sandbox)

Stan	⚠
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2605
Identyfikator zdarzenia Kaspersky Security Center	00000a2d
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Całkowity rozmiar zadań skanowania przekroczył limit

Stan	⚠
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2612
Identyfikator zdarzenia Kaspersky Security Center	00000a34
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Dozwolone uruchamianie obiektu, zdarzenie zarejestrowane

Stan	⚠
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2553
Identyfikator zdarzenia Kaspersky Security Center	000009fa
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Dozwolone uruchamianie procesu, zdarzenie zarejestrowane

Stan	⚠
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2554
Identyfikator zdarzenia Kaspersky Security Center	000009f8
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt zostanie usunięty po ponownym uruchomieniu (Endpoint Detection and Response)

Stan	⚠
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2558
Identyfikator zdarzenia Kaspersky Security Center	000009fe
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Izolacja od sieci

Stan	⚠
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2700
Identyfikator zdarzenia Kaspersky Security Center	00000a8c
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zakończenie izolacji od sieci

Stan	⚠
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2701
Identyfikator zdarzenia Kaspersky Security Center	00000a8d
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

W celu zakończenia zadania wymagane jest ponowne uruchomienie

Stan	⚠
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	225
Identyfikator zdarzenia Kaspersky Security Center	0000057b
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wiadomość do administratora dotycząca zablokowania uruchomienia aplikacji

Stan	⚠
Składnik	Kontrola aplikacji
Identyfikator zdarzenia systemu Windows	503
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_AC_USER_REQUEST
Parametry zdarzenia	• GNRL_EA_DESCRIPTION to wiadomość do użytkownika. • GNRL_EA_PARAM_2 to nazwa użytkownika sesji. • GNRL_EA_PARAM_6 to nazwa pliku wykonywalnego aplikacji (na przykład: chrome.exe). • GNRL_EA_PARAM_7 to ścieżka do pliku wykonywalnego. • GNRL_EA_PARAM_8 to suma kontrolna obiektu (SHA256). • GNRL_EA_PARAM_9 to wersja aplikacji, którą użytkownik próbuje uruchomić.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wiadomość do administratora dotycząca zablokowania dostępu do urządzenia

Stan	⚠
Składnik	Kontrola urządzeń
Identyfikator zdarzenia systemu Windows	804
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_DC_USER_REQUEST
Parametry zdarzenia	• c_er_descr to wiadomość do użytkownika. • GNRL_EA_PARAM_1 to ID sprzętu (HWID). • GNRL_EA_PARAM_2 to nazwa użytkownika sesji.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wiadomość do administratora dotycząca zablokowania dostępu do strony internetowej

Stan	⚠
Składnik	Kontrola sieci
Identyfikator zdarzenia systemu Windows	755
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_WC_USER_REQUEST
Parametry zdarzenia	• GNRL_EA_DESCRIPTION to wiadomość do użytkownika. • GNRL_EA_PARAM_1 to adres internetowy. • GNRL_EA_PARAM_2 to nazwa użytkownika sesji.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Połączenie z urządzeniem jest zablokowane

Stan	⚠
Składnik	Kontrola urządzeń
Identyfikator zdarzenia systemu Windows	807
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parametry zdarzenia	• GNRL_EA_PARAM_1 to ID sprzętu (HWID). • GNRL_EA_PARAM_2 to nazwa użytkownika sesji.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wiadomość do administratora dotycząca zablokowania aktywności aplikacji

Stan	⚠
Składnik	Monitor integralności plików
Identyfikator zdarzenia systemu Windows	2901
Identyfikator zdarzenia Kaspersky Security Center	00000b55
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Stan	⚠
Składnik	Monitor integralności plików
Identyfikator zdarzenia systemu Windows	2900
Identyfikator zdarzenia Kaspersky Security Center	00000b54
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Stan	⚠
Składnik	Adaptacyjna kontrola anomalii
Identyfikator zdarzenia systemu Windows	503
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_ADSEC_USER_REQUEST
Parametry zdarzenia	• GNRL_EA_DESCRIPTION to wiadomość do użytkownika. • GNRL_EA_PARAM_1 to nazwa reguły Adaptacyjnej kontroli anomalii. • GNRL_EA_PARAM_2 to identyfikator reguły heurystycznej. • GNRL_EA_PARAM_3 to nazwa użytkownika sesji. • GNRL_EA_PARAM_4 to proces źródłowy. • GNRL_EA_PARAM_5 to obiekt źródłowy. • GNRL_EA_PARAM_6 to proces docelowy. • GNRL_EA_PARAM_7 to obiekt docelowy. • GNRL_EA_PARAM_8 to dodatkowe informacje o wykrytym obiekcie: Sumy kontrolne procesu / obiektu źródłowego oraz procesu / obiektu docelowego. Proces został zablokowany (verdict_type): true lub false. Identyfikator zabezpieczeń użytkownika (SID).
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Uruchamianie aplikacji klienckiej usługi chmury jest blokowane

Stan	⚠
Składnik	Cloud Discovery
Identyfikator zdarzenia systemu Windows	2212
Identyfikator zdarzenia Kaspersky Security Center	000008a4
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Dostęp do usługi chmury jest zablokowany

Stan	⚠
Składnik	Cloud Discovery
Identyfikator zdarzenia systemu Windows	2213
Identyfikator zdarzenia Kaspersky Security Center	000008a5
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto zmianę pliku lub folderu

Stan	ⓘ / ⚠ / ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2950
Identyfikator zdarzenia Kaspersky Security Center	00000b86
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu*.

Obiekt zbyt często ulega zmianom. Rozpoczęto agregację zdarzeń

Stan	ⓘ / ⚠ / ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2955
Identyfikator zdarzenia Kaspersky Security Center	00000b8b
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Raport o modyfikacji obiektu dla okresu agregacji

Stan	ⓘ / ⚠ / ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2956
Identyfikator zdarzenia Kaspersky Security Center	00000b8c
Dziennik zdarzeń systemu Windows (domyślnie)	–

Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Zmiana rejestru została wykryta

Stan	ⓘ / ⚠ / ⓔ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2951
Identyfikator zdarzenia Kaspersky Security Center	00000b87
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Wykryto podłączenie/odłączenie urządzenia

Stan	ⓘ / ⚠ / ⓔ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2952
Identyfikator zdarzenia Kaspersky Security Center	00000b88
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Zakres monitorowania obejmuje nieprawidłowe obiekty

Stan	ⓘ / ⚠ / ⓔ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2903
Identyfikator zdarzenia Kaspersky Security Center	00000b89
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Niedozwolona operacja była dozwolona w trybie testowym

Stan	⚠
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2961
Identyfikator zdarzenia Kaspersky Security Center	00000b91
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie można połączyć się z serwerem integracji przez ponad 30 minut. Sprawdź stan serwera integracji i ustawienia sieciowe

Stan	⚠
Składnik	Light Agent
Identyfikator zdarzenia systemu Windows	3102
Identyfikator zdarzenia Kaspersky Security Center	00000c1e
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie można połączyć się z serwerem integracji. Sprawdź stan serwera integracji i ustawienia sieciowe

Stan	⚠
Składnik	Light Agent
Identyfikator zdarzenia systemu Windows	3101
Identyfikator zdarzenia Kaspersky Security Center	00000c1d
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Szablon maszyny wirtualnej wymaga aktualizacji

Stan	⚠
Składnik	Light Agent
Identyfikator zdarzenia systemu Windows	3181
Identyfikator zdarzenia Kaspersky Security Center	00000c6d
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Licencja Standard została zakończona. Aplikacja działa z licencją Enterprise

Stan	⚠
Składnik	Light Agent
Identyfikator zdarzenia systemu Windows	3171
Identyfikator zdarzenia Kaspersky Security Center	00000c64
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wiadomość informacyjna

Aplikacja uruchomiona

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	235
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Aplikacja zatrzymana

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	236
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Autoochrona ograniczyła dostęp do tego chronionego zasobu

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	213
Identyfikator zdarzenia Kaspersky Security Center	000000d5
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Raport został wyczyszczony

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	217
Identyfikator zdarzenia Kaspersky Security Center	000000d9
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zasady grupy zostały wyłączone

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	220

Identyfikator zdarzenia Kaspersky Security Center	000000dc
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Ustawienia aplikacji zostały zmienione

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	218
Identyfikator zdarzenia Kaspersky Security Center	000000da
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Zadanie zostało uruchomione

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	221
Identyfikator zdarzenia Kaspersky Security Center	000000dd
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zadanie zakończone

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	223
Identyfikator zdarzenia Kaspersky Security Center	000000df
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wszystkie składniki aplikacji określone w tej licencji zostały zainstalowane i działają w normalnym trybie

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	227
Identyfikator zdarzenia Kaspersky Security Center	000000e3
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Ustawienia subskrypcji uległy zmianie

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	238

Identyfikator zdarzenia Kaspersky Security Center	000000ee
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Subskrypcja została odnowiona

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	239
Identyfikator zdarzenia Kaspersky Security Center	000000ef
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt został przywrócony z Kopii zapasowej

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	335
Identyfikator zdarzenia Kaspersky Security Center	0000014f
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wprowadzenie nazwy użytkownika i hasła

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	2000
Identyfikator zdarzenia Kaspersky Security Center	000007d0
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Uczestnictwo w KSN jest włączone

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	2020
Identyfikator zdarzenia Kaspersky Security Center	000007e4
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Serwery KSN są dostępne

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	2022

Identyfikator zdarzenia Kaspersky Security Center	000007e6
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aplikacja działa i przetwarza dane zgodnie z odpowiednimi przepisami i korzysta z odpowiedniej infrastruktury

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	2024
Identyfikator zdarzenia Kaspersky Security Center	000007e8
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt został przywrócony z Kwarantanny

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	345
Identyfikator zdarzenia Kaspersky Security Center	00000159
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt został usunięty z Kwarantanny

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	347
Identyfikator zdarzenia Kaspersky Security Center	0000015b
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Utworzono kopię zapasową obiektu

Stan	ⓘ
Składnik	Ochrona plików Ochrona poczty Wykrywanie zachowań Anti-Cryptor Ochrona przed włamaniami Sandbox Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	308
Identyfikator zdarzenia Kaspersky Security Center	00000134
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nadpisany przy użyciu wcześniej wyleczonej kopii

Stan	ⓘ
Składnik	Ochrona plików Ochrona przed włamaniami Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	327
Identyfikator zdarzenia Kaspersky Security Center	00000147
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wykryto archiwum zabezpieczone hasłem

Stan	ⓘ
Składnik	Ochrona plików Ochrona WWW Ochrona poczty Ochrona AMSI Ochrona przed włamaniami Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	322
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_PASSWD_ARCHIVE_FOUND
Parametry zdarzenia	• GNRL_EA_PARAM_2 to nazwa obiektu. • GNRL_EA_PARAM_3 to data utworzenia obiektu (opcjonalne). • GNRL_EA_PARAM_7 to nazwa użytkownika sesji. • GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine ?). Technologia wykrywania zagrożeń (method ?). Zagrożenie wykryte przez prywatną sieć KSN (denylist): true lub false.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Informacje o wykrytym obiekcie

Stan	ⓘ
Składnik	Ochrona plików Ochrona WWW Ochrona poczty Ochrona AMSI Ochrona przed włamaniami Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	332
Identyfikator zdarzenia Kaspersky Security Center	0000014c
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt znajduje się na liście zezwolonych programu Kaspersky Private Security Network

Stan	ⓘ
Składnik	Ochrona plików Ochrona WWW Ochrona poczty Ochrona AMSI Ochrona przed włamaniami Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	340

Identyfikator zdarzenia Kaspersky Security Center	00000154
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zmieniono nazwę obiektu

Stan	ⓘ
Składnik	Ochrona poczty Ochrona przed exploitami Wykrywanie zachowań Anti-Cryptor Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	329
Identyfikator zdarzenia Kaspersky Security Center	00000149
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt przetworzony

Stan	ⓘ
Składnik	Ochrona przed włamaniami Ochrona plików Ochrona WWW Ochrona poczty Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	301
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Obiekt został pominięty

Stan	ⓘ
Składnik	Ochrona przed włamaniami Ochrona plików Ochrona AMSI Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	315
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wykryto archiwum

Stan	ⓘ
Składnik	Ochrona przed włamaniami Ochrona plików Ochrona WWW Ochrona poczty Ochrona AMSI Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	318

Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wykryto obiekt spakowany

Stan	ⓘ
Składnik	Ochrona przed włamaniami Ochrona plików Ochrona WWW Ochrona poczty Ochrona AMSI Skanowanie w poszukiwaniu złośliwego oprogramowania
Identyfikator zdarzenia systemu Windows	319
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Odnośnik przetworzony

Stan	ⓘ
Składnik	Ochrona WWW
Identyfikator zdarzenia systemu Windows	361
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Zezwolono na uruchomienie aplikacji

Stan	ⓘ
Składnik	Kontrola aplikacji
Identyfikator zdarzenia systemu Windows	701
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wybrano źródło aktualizacji

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1001
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wybrano serwer proxy

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1002
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Link znajduje się na liście zezwolonych programu Kaspersky Private Security Network

Stan	ⓘ
Składnik	Ochrona WWW
Identyfikator zdarzenia systemu Windows	370
Identyfikator zdarzenia Kaspersky Security Center	00000172
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aplikacja została umieszczona w grupie zaufanych

Stan	ⓘ
Składnik	Ochrona przed włamaniami
Identyfikator zdarzenia systemu Windows	401
Identyfikator zdarzenia Kaspersky Security Center	00000191
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aplikacja została umieszczona w grupie z ograniczeniami

Stan	ⓘ
Składnik	Ochrona przed włamaniami
Identyfikator zdarzenia systemu Windows	402
Identyfikator zdarzenia Kaspersky Security Center	00000192
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Ochrona przed włamaniami została wywołana

Stan	ⓘ
Składnik	Ochrona przed włamaniami
Identyfikator zdarzenia systemu Windows	403
Identyfikator zdarzenia Kaspersky Security Center	00000193
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Przywrócono plik

Stan	ⓘ
Składnik	Wykrywanie zachowań Anti-Cryptor Ochrona przed exploitami Ochrona przed włamaniami
Identyfikator zdarzenia systemu Windows	`457`
Identyfikator zdarzenia Kaspersky Security Center	`000001c9`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Przywrócono wartość rejestru

Stan	ⓘ
Składnik	Wykrywanie zachowań Ochrona przed exploitami
Identyfikator zdarzenia systemu Windows	`458`
Identyfikator zdarzenia Kaspersky Security Center	`000001ca`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Usunięto wartość rejestru

Stan	ⓘ
Składnik	Wykrywanie zachowań Ochrona przed exploitami
Identyfikator zdarzenia systemu Windows	`459`
Identyfikator zdarzenia Kaspersky Security Center	`000001cb`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Pominięto akcję procesu

Stan	ⓘ
Składnik	Adaptacyjna kontrola anomalii
Identyfikator zdarzenia systemu Windows	`2201`
Identyfikator zdarzenia Kaspersky Security Center	`GNRL_EV_ADSEC_DETECT`
Parametry zdarzenia	• `GNRL_EA_PARAM_1` to nazwa reguły Adaptacyjnej kontroli anomalii. • `GNRL_EA_PARAM_2` to identyfikator reguły heurystycznej. • `GNRL_EA_PARAM_3` to nazwa użytkownika sesji. • `GNRL_EA_PARAM_4` to proces źródłowy. • `GNRL_EA_PARAM_5` to obiekt źródłowy. • `GNRL_EA_PARAM_6` to proces docelowy. • `GNRL_EA_PARAM_7` to obiekt docelowy. • `GNRL_EA_PARAM_8` to dodatkowe informacje o wykrytym obiekcie: Sumy kontrolne procesu / obiektu źródłowego oraz procesu / obiektu docelowego. Proces został zablokowany (`verdict_type`): `true` lub `false`. Identyfikator zabezpieczeń użytkownika (SID).
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Klawiatura zautoryzowana

Stan	ⓘ
Składnik	Ochrona przed atakami BadUSB
Identyfikator zdarzenia systemu Windows	2050
Identyfikator zdarzenia Kaspersky Security Center	00000802
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aktywność sieciowa jest dozwolona

Stan	ⓘ
Składnik	Zapora sieciowa
Identyfikator zdarzenia systemu Windows	601
Identyfikator zdarzenia Kaspersky Security Center	00000259
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Zabroniono uruchomienia aplikacji w trybie testowym

Stan	ⓘ
Składnik	Kontrola aplikacji
Identyfikator zdarzenia systemu Windows	703
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Parametry zdarzenia	• GNRL_EA_PARAM_2 to nazwa użytkownika sesji. • GNRL_EA_PARAM_3 to ręcznie utworzony identyfikator kategorii. • GNRL_EA_PARAM_4 to identyfikator zabezpieczeń konta (SID). • GNRL_EA_PARAM_5 to informacje o cyfrowym podpisie aplikacji. • GNRL_EA_PARAM_6 to nazwa pliku wykonywalnego aplikacji (na przykład: chrome.exe). • GNRL_EA_PARAM_7 to ścieżka do pliku wykonywalnego. • GNRL_EA_PARAM_8 to suma kontrolna obiektu (SHA256). • GNRL_EA_PARAM_9 to wersja aplikacji, którą użytkownik próbuje uruchomić.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zezwolono na uruchomienie aplikacji w trybie testowym

Stan	ⓘ
Składnik	Kontrola aplikacji
Identyfikator zdarzenia systemu Windows	704
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Parametry zdarzenia	• GNRL_EA_PARAM_2 to nazwa użytkownika sesji. • GNRL_EA_PARAM_3 to ręcznie utworzony identyfikator kategorii. • GNRL_EA_PARAM_4 to identyfikator zabezpieczeń konta (SID). • GNRL_EA_PARAM_5 to informacje o cyfrowym podpisie aplikacji.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Strona, która jest dozwolona została otwarta

Stan	
Składnik	Kontrola sieci
Identyfikator zdarzenia systemu Windows	751
Identyfikator zdarzenia Kaspersky Security Center	000002f4
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Działania na urządzeniu zostały dozwolone

Stan	
Składnik	Kontrola urządzeń
Identyfikator zdarzenia systemu Windows	801
Identyfikator zdarzenia Kaspersky Security Center	00000321
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Operacja na pliku została wykonana

Stan	
Składnik	Kontrola urządzeń
Identyfikator zdarzenia systemu Windows	808
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_USB_FILE_OPERATION
Parametry zdarzenia	• GNRL_EA_PARAM_1 to operacja na pliku (zapis lub usuwanie). • GNRL_EA_PARAM_2 to ścieżka do pliku. • GNRL_EA_PARAM_3 to nazwa urządzenia. • GNRL_EA_PARAM_4 to nazwa użytkownika sesji. • GNRL_EA_PARAM_5 to ID sprzętu (HWID).
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Brak dostępnych aktualizacji

Stan	
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1020
Identyfikator zdarzenia Kaspersky Security Center	000003fc
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Zadanie dystrybucji uaktualnień zostało pomyślnie zakończone

Stan	
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1022
Identyfikator zdarzenia Kaspersky Security Center	000003fe

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Pobieranie plików

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1003
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Plik został pobrany

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1004
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Plik został zainstalowany

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1005
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Plik został uaktualniony

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1006
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Plik został przywrócony z powodu błędu aktualizacji

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1007
Identyfikator zdarzenia Kaspersky Security Center	–

Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Aktualizacja plików

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1008
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Dystrybucja uaktualnień

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1009
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Przywracanie plików

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1010
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Tworzenie listy plików do pobrania

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	1013
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Pobieranie poprawek

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	2150
Identyfikator zdarzenia Kaspersky Security Center	–

Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Instalowanie poprawki

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	2151
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Poprawka zainstalowana

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	2152
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wycofywanie poprawki

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	2154
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Poprawka wycofana

Stan	ⓘ
Składnik	Aktualizacja
Identyfikator zdarzenia systemu Windows	2155
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Uruchomiono stosowanie reguł szyfrowania / odszyfrowywania pliku

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	901
Identyfikator zdarzenia Kaspersky Security Center	00000385

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zakończono stosowanie reguł szyfrowania / odszyfrowywania pliku

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	902
Identyfikator zdarzenia Kaspersky Security Center	00000386
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wznowiono stosowanie reguł szyfrowania / odszyfrowywania pliku

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	905
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Uruchomiono szyfrowanie / odszyfrowywanie pliku

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	910
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Zakończono szyfrowanie / odszyfrowywanie pliku

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	911
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Plik nie został zaszyfrowany, ponieważ jest wykluczony

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	913
Identyfikator zdarzenia Kaspersky Security Center	–

Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Włączono tryb przenośny

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	950
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wyłączono tryb przenośny

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	952
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Uruchomiono szyfrowanie / odszyfrowywanie urządzenia

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1301
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Zakończono szyfrowanie / odszyfrowywanie urządzenia

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1302
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wznowiono szyfrowanie / odszyfrowywanie urządzenia

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1304
Identyfikator zdarzenia Kaspersky Security Center	–

Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Urządzenie nie jest zaszyfrowane

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1307
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Proces szyfrowania / odszyfrowywania urządzenia został przełączony do trybu aktywnego

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1308
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Proces szyfrowania / odszyfrowywania urządzenia został przełączony do trybu pasywnego

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1309
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Wczytano moduł szyfrujący

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1310
Identyfikator zdarzenia Kaspersky Security Center	0000051e
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Utworzono nowe konto Agenta autoryzacji

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1330
Identyfikator zdarzenia Kaspersky Security Center	00000532

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Usunięto konto Agenta autoryzacji

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1331
Identyfikator zdarzenia Kaspersky Security Center	00000533
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Zmieniono hasło konta Agenta autoryzacji

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1332
Identyfikator zdarzenia Kaspersky Security Center	00000534
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Pomyślne logowanie Agenta autoryzacji

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1333
Identyfikator zdarzenia Kaspersky Security Center	00000535
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Nieudana próba logowania Agenta autoryzacji

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1334
Identyfikator zdarzenia Kaspersky Security Center	00000536
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Dostęp do dysku twardego uzyskany przy użyciu procedury dostępu do zaszyfrowanych urządzeń

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1335
Identyfikator zdarzenia Kaspersky Security Center	00000537

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Próba dostępu do dysku twardego przy użyciu procedury dostępu do zaszyfrowanych urządzeń nie powiodła się

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1336
Identyfikator zdarzenia Kaspersky Security Center	00000538
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Konto nie zostało dodane. To konto już istnieje

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1337
Identyfikator zdarzenia Kaspersky Security Center	00000539
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Konto nie zostało zmodyfikowane. To konto nie istnieje

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1338
Identyfikator zdarzenia Kaspersky Security Center	0000053a
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Konto nie zostało usunięte. To konto nie istnieje

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1339
Identyfikator zdarzenia Kaspersky Security Center	0000053b
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Aktualizacja FDE zakończyła się powodzeniem

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	1341
Identyfikator zdarzenia Kaspersky Security Center	0000053d

Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Cofanie aktualizacji FDE zakończyło się powodzeniem

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	`1343`
Identyfikator zdarzenia Kaspersky Security Center	`0000053f`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nie udało się odinstalować sterowników Kaspersky Disk Encryption w obrazie WinRE

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	`1346`
Identyfikator zdarzenia Kaspersky Security Center	`00000542`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Klucz odzyskiwania funkcji BitLocker został zmieniony

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	`1370`
Identyfikator zdarzenia Kaspersky Security Center	`0000055a`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Hasło funkcji BitLocker / PIN zostało zmienione

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	`1371`
Identyfikator zdarzenia Kaspersky Security Center	`0000055b`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Klucz odzyskiwania funkcji BitLocker został zapisany na dysku wymiennym

Stan	ⓘ
Składnik	Szyfrowanie danych
Identyfikator zdarzenia systemu Windows	`1372`
Identyfikator zdarzenia Kaspersky Security Center	`0000055c`

Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Przetwarzanie zadań z serwera Kaspersky Anti Targeted Attack Platform jest nieaktywne

Stan	ⓘ
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2103
Identyfikator zdarzenia Kaspersky Security Center	00000837
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Składnik Endpoint Sensor nawiązał połączenie z serwerem

Stan	ⓘ
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2101
Identyfikator zdarzenia Kaspersky Security Center	00000835
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Połączenie z serwerem Kaspersky Anti Targeted Attack Platform zostało przywrócone

Stan	ⓘ
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2102
Identyfikator zdarzenia Kaspersky Security Center	00000836
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zadania z serwera Kaspersky Anti Targeted Attack Platform są przetwarzane

Stan	ⓘ
Składnik	Endpoint Sensor
Identyfikator zdarzenia systemu Windows	2104
Identyfikator zdarzenia Kaspersky Security Center	00000838
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt usunięty

Stan	ⓘ
Składnik	Wyczyść dane
Identyfikator zdarzenia systemu Windows	2251
Identyfikator zdarzenia Kaspersky Security Center	000008cb

Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Statystyki zadania czyszczenia

Stan	
Składnik	Endpoint Detection and Response Expert (on-premises)
Identyfikator zdarzenia systemu Windows	2853
Identyfikator zdarzenia Kaspersky Security Center	00000b25
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Stan	
Składnik	Wyczyść dane
Identyfikator zdarzenia systemu Windows	2253
Identyfikator zdarzenia Kaspersky Security Center	000008cd
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt poddano kwarantannie (Sandbox)

Stan	
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2602
Identyfikator zdarzenia Kaspersky Security Center	00000a2a
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt został usunięty (Sandbox)

Stan	
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2604
Identyfikator zdarzenia Kaspersky Security Center	00000a2c
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Uruchomiono skanowanie IOC

Stan	
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2652
Identyfikator zdarzenia Kaspersky Security Center	00000a5c
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zakończono skanowanie IOC

Stan	ⓘ
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2653
Identyfikator zdarzenia Kaspersky Security Center	00000a5d
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt poddano kwarantannie (Endpoint Detection and Response)

Stan	ⓘ
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2555
Identyfikator zdarzenia Kaspersky Security Center	000009fb
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Obiekt został usunięty (Endpoint Detection and Response)

Stan	ⓘ
Składnik	Endpoint Detection and Response
Identyfikator zdarzenia systemu Windows	2557
Identyfikator zdarzenia Kaspersky Security Center	000009fd
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Składniki aplikacji zostały pomyślnie zmienione

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	1402
Identyfikator zdarzenia Kaspersky Security Center	0000057a
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Stan	ⓘ
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2606
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Stan	ⓘ
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2609
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Stan	ⓘ
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2610
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Stan	ⓘ
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2616
Identyfikator zdarzenia Kaspersky Security Center	–
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	–

Serwer administracyjny, z którym połączone jest Twoje urządzenie, jest ustawiony jako zaufany

Stan	ⓘ
Składnik	Ochrona połączenia z Serwerem administracyjnym
Identyfikator zdarzenia systemu Windows	3300
Identyfikator zdarzenia Kaspersky Security Center	00000ce4
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Twoje urządzenie jest połączone z nowym zaufanym Serwerem administracyjnym

Stan	ⓘ
Składnik	Ochrona połączenia z Serwerem administracyjnym
Identyfikator zdarzenia systemu Windows	3302
Identyfikator zdarzenia Kaspersky Security Center	00000ce6
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Serwer administracyjny, z którym połączone jest Twoje urządzenie, nie jest już ustawiony jako zaufany

Stan	ⓘ
Składnik	Ochrona połączenia z Serwerem administracyjnym
Identyfikator zdarzenia systemu Windows	3303

Identyfikator zdarzenia Kaspersky Security Center	00000ce7
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Asynchroniczne wykrywanie Sandbox

Stan	ⓘ
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2619
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_APP_INCIDENT_OCCURED
Parametry zdarzenia	• GNRL_EA_PARAM_1 są parametrami składników Sandbox. • GNRL_EA_PARAM_2 to ścieżka do obiektu. • GNRL_EA_PARAM_3 to identyfikator incydentu. • GNRL_EA_PARAM_4 to suma kontrolna obiektu (SHA256).
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zadanie skanowania zostało pomyślnie wysłane do Sandbox przez użytkownika

Stan	ⓘ
Składnik	Sandbox
Identyfikator zdarzenia systemu Windows	2622
Identyfikator zdarzenia Kaspersky Security Center	00000a3e
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Urządzenie jest podłączone

Stan	ⓘ
Składnik	Kontrola urządzeń
Identyfikator zdarzenia systemu Windows	805
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUGGED
Parametry zdarzenia	• GNRL_EA_PARAM_1 to ID sprzętu (HWID). • GNRL_EA_PARAM_2 to nazwa użytkownika sesji.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Urządzenie jest odłączone

Stan	ⓘ
Składnik	Kontrola urządzeń
Identyfikator zdarzenia systemu Windows	806
Identyfikator zdarzenia Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
Parametry zdarzenia	• GNRL_EA_PARAM_1 to ID sprzętu (HWID). • GNRL_EA_PARAM_2 to nazwa użytkownika sesji.
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Błąd podczas usuwania poprzedniej wersji aplikacji

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	246
Identyfikator zdarzenia Kaspersky Security Center	000000f6
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Pomyślne połączenie z serwerem EDR Expert

Stan	ⓘ
Składnik	Endpoint Detection and Response Expert (on-premises)
Identyfikator zdarzenia systemu Windows	2853
Identyfikator zdarzenia Kaspersky Security Center	00000b25
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nawiązano połączenie z serwerem odpowiedzi EDR Expert

Stan	ⓘ
Składnik	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identyfikator zdarzenia systemu Windows	2853
Identyfikator zdarzenia Kaspersky Security Center	00000b25
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Nawiązano połączenie z serwerem gromadzenia danych telemetrycznych EDR Expert

Stan	ⓘ
Składnik	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Identyfikator zdarzenia systemu Windows	2857
Identyfikator zdarzenia Kaspersky Security Center	00000b26
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Pomyślne połączenie z serwerem NDR

Stan	ⓘ
Składnik	Network Detection and Response (KATA)
Identyfikator zdarzenia systemu Windows	3083
Identyfikator zdarzenia Kaspersky Security Center	00000c0b

Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Uruchamianie aplikacji klienckiej usługi chmury jest dozwolone

Stan	ⓘ
Składnik	Cloud Discovery
Identyfikator zdarzenia systemu Windows	`2210`
Identyfikator zdarzenia Kaspersky Security Center	`000008a2`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Dostęp do usługi chmury jest dozwolony

Stan	ⓘ
Składnik	Cloud Discovery
Identyfikator zdarzenia systemu Windows	`2211`
Identyfikator zdarzenia Kaspersky Security Center	`000008a3`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Dostęp do obszaru chronionego

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	`2004`
Identyfikator zdarzenia Kaspersky Security Center	`000007d4`
Dziennik zdarzeń systemu Windows (domyślnie)	✓
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Wykryto zmianę pliku lub folderu

Stan	ⓘ / ⚠ / ⓘ
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	`2950`
Identyfikator zdarzenia Kaspersky Security Center	`00000b86`
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Obiekt zbyt często ulega zmianom. Rozpoczęto agregację zdarzeń

Stan	/ /
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2955
Identyfikator zdarzenia Kaspersky Security Center	00000b8b
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Raport o modyfikacji obiektu dla okresu agregacji

Stan	/ /
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2956
Identyfikator zdarzenia Kaspersky Security Center	00000b8c
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Zmiana rejestru została wykryta

Stan	/ /
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2951
Identyfikator zdarzenia Kaspersky Security Center	00000b87
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Wykryto podłączenie/odłączenie urządzenia

Stan	/ /
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2952
Identyfikator zdarzenia Kaspersky Security Center	00000b88
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Zakres monitorowania obejmuje nieprawidłowe obiekty

Stan	/ /
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2903
Identyfikator zdarzenia Kaspersky Security Center	00000b89
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Utworzono stan wyjściowy

Stan	
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2957
Identyfikator zdarzenia Kaspersky Security Center	00000b8d
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Zaktualizowano stan wyjściowy

Stan	
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2958
Identyfikator zdarzenia Kaspersky Security Center	00000b8e
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Operacja jest wykonywana przez zaufanego użytkownika

Stan	
Składnik	Monitor integralności systemu
Identyfikator zdarzenia systemu Windows	2962
Identyfikator zdarzenia Kaspersky Security Center	00000b92
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Aby skonfigurować okres przechowywania dla tego zdarzenia, przejdź do sekcji **Konfiguracja zdarzenia** polityki i ustaw okres przechowywania dla ogólnego zdarzenia Monitora integralności systemu – *Wykryto zmianę pliku lub folderu.*

Połączono z SVM

Stan	
Składnik	Light Agent

Identyfikator zdarzenia systemu Windows	3152
Identyfikator zdarzenia Kaspersky Security Center	00000c50
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Utworzono nowe hasło tymczasowe

Stan	ⓘ
Składnik	Audyt systemu
Identyfikator zdarzenia systemu Windows	265
Identyfikator zdarzenia Kaspersky Security Center	00000109
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Połączono z serwerem integracji

Stan	ⓘ
Składnik	Light Agent
Identyfikator zdarzenia systemu Windows	3105
Identyfikator zdarzenia Kaspersky Security Center	00000c21
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Przywracanie połączenia z serwerem integracji

Stan	ⓘ
Składnik	Light Agent
Identyfikator zdarzenia systemu Windows	3104
Identyfikator zdarzenia Kaspersky Security Center	00000c20
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Pomyślne połączenie z serwerem KUMA

Stan	ⓘ
Składnik	Integracja KUMA
Identyfikator zdarzenia systemu Windows	2857
Identyfikator zdarzenia Kaspersky Security Center	00000b29
Dziennik zdarzeń systemu Windows (domyślnie)	–
Dziennik zdarzeń Kaspersky Security Center (domyślnie)	✓

Dodatek 7. Obsługiwane rozszerzenia plików dla Zapobiegania wykonywaniu

Kaspersky Endpoint Security obsługuje zapobieganie otwierania plików formatu office w pewnych aplikacjach. Informacje o obsługiwanych rozszerzeniach plików i aplikacji znajdują się w następującej tabeli.

Obsługiwane rozszerzenia plików dla Zapobiegania wykonywaniu

Nazwa aplikacji	Plik wykonywalny	Rozszerzenie pliku
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm

Nazwa aplikacji	Plik wykonywalny	Rozszerzenie pliku
Adobe Acrobat	acrord32.exe	pdf
Foxit PDF Reader	FoxitReader.exe	
STDU Viewer	STDUViewerApp.exe	
Microsoft Edge	MicrosoftEdge.exe	
Google Chrome	chrome.exe	
Mozilla Firefox	firefox.exe	
Yandex Browser	browser.exe	
Tor Browser	tor.exe	

Dodatek 8. Obsługiwane interpretery skryptów do usługi Zapobiegania wykonywaniu

Zapobieganie wykonywaniu obsługuje następujące interpretory skryptów:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe

- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Zapobieganie wykonywaniu obsługuje pracę z aplikacjami Java w środowisku uruchomieniowym Java (procesy java.exe i javaw.exe).

Dodatek 9. Obszar skanowania IOC w rejestrze (RegistryItem)

Jeśli dodasz typ danych **Rejestr Windowsa - RegistryItem** do obszaru skanowania IOC, Kaspersky Endpoint Security przeskanuje następujące klucze rejestru:

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders
```

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Dodatek 10. Wymagania pliku IOC

Podczas tworzenia zadań Skanowanie IOC rozważ następujące ograniczenia i wymagania pliku IOC:

- Aplikacja obsługuje pliki IOC z rozszerzeniami IOC i XML w otwartym standardzie OpenIOC w wersjach 1.0 i 1.1 dla opisania wskaźników naruszeń bezpieczeństwa.
- Po przesłaniu plików IOC możesz ręcznie edytować pliki we wbudowanym edytorze bezpośrednio we właściwościach zadania. Kaspersky Endpoint Security obsługuje edycję plików IOC zgodnych ze standardem OpenIOC 1.1. Nie można modyfikować zawartości plików IOC zgodnych z wersją OpenIOC 1.0.
- Jeśli podczas tworzenia zadania *Skanowanie IOC* w wierszu polecenia przesłałeś pliki IOC, z których niektóre nie są obsługiwane, gdy zadanie jest uruchomione, aplikacja używa tylko obsługiwanych plików IOC. Jeśli podczas tworzenia zadania *Skanowanie IOC* w wierszu polecenia wszystkie pliki IOC, które przesyłasz, okażą się nieobsługiwane, zadanie wciąż może być uruchomione, ale nie wykryje żadnych wskaźników naruszeń bezpieczeństwa. Nie jest możliwe przesłanie nieobsługiwanych plików IOC przy użyciu konsoli Web Console lub Cloud Console.

- Błędy semantyczne i nieobsługiwane warunki IOC i znaczniki w plikach IOC nie powodują błędu wykonania zadania. W takich sekcjach plików IOC aplikacja nie wykrywa dopasowania.
- Identyfikatory wszystkich plików IOC używane w pojedynczym zadaniu Skanowanie IOC muszą być unikatowe. Jeśli istnieją pliki IOC z takim samym identyfikatorem, mogą wpłynąć na wyniki wykonania zadania.
- Rozmiar pojedynczego pliku IOC nie może przekraczać 2 MB. Używanie większych plików spowoduje zakończenie zadania Skanowanie IOC z błędem. Całkowity rozmiar wszystkich plików dodanych do zbioru IOC nie może przekroczyć 10 MB. Jeżeli łączny rozmiar wszystkich plików przekracza 10 MB, należy podzielić kolekcję IOC i utworzyć kilka zadań *Skanowanie IOC*.
- Zalecane jest utworzenie jednego pliku IOC na zagrożenie. To ułatwia analizowanie wyników zadania *Skanowanie IOC*.

Plik, który możesz pobrać, klikając poniższy odnośnik, zawiera tabelę z pełną listą warunków IOC standardu OpenIOC.

POBIERZ PLIK IOC_TERMS.XLSX

Funkcje i ograniczenia obsługi aplikacji dla standardu OpenIOC są wyświetlone w poniższej tabeli.

Funkcje i ograniczenia obsługi OpenIOC w wersji 1.0 i 1.1.

Obsługiwane warunki	OpenIOC 1.0:
	
	`is`
	`isnot` (jako wyjątek z zestawu)
	`contains`
	`containsnot` (jako wyjątek z zestawu)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	W przypadku parametrów Email/* obsługiwane są tylko warunki `contains` i `is`. Prawidłowe działanie Retrospektywnego skanowania IOC podczas korzystania z warunku `is`, wymaga określenia adresów e-mail w plikach IOC w następującym formacie: `"name@example.org" <SMTP:name@example.org>`. Podczas normalnego uruchamiania zadania *Skanowanie IOC* wystarczy zwykle określić adres e-mail w następującym formacie: `name@example.org`.

Obsługiwane atrybuty warunku	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Obsługiwane operatory	`AND` `OR`
Obsługiwane typy danych	`"date"`: data (stosowane warunki: `is`, `greater-than`, `less-than`) `"int"`: liczba całkowita (stosowane warunki: `is`, `greater-than`, `less-than`) `"string"`: ciąg znaków (stosowane warunki: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: czas trwania w sekundach (stosowane warunki: `is`, `greater-than`, `less-than`)

Funkcje interpretacji typu danych	Typy danych `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` i `"base64Binary"` są interpretowane jako ciąg znaków.
	
	Aplikacja obsługuje interpretację ustawienia `Content` dla typów danych `int` i `date`, gdy jest ona ustawiona w postaci przedziałów czasu:
	
	OpenIOC 1.0:
	Przy użyciu operatora `TO` w polu `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Przy użyciu warunków `greater-than` i `less-than`
	Przy użyciu operatora `TO` w polu `Content`
	Aplikacja obsługuje interpretację typów danych `date` i `duration`, jeśli wskaźniki są ustawione w formacie `ISO 8601, Zulu time zone, UTC`.

Dodatek 11. Interfejs API dla usługi reagowania na zagrożenia EDR

W Kaspersky Endpoint Security 12.9 for Windows wprowadzono obsługę działań reagowania na zagrożenia EDR (EDR responses) za pomocą Kaspersky Security Center OpenAPI. Oznacza to, że można wywołać metody OpenAPI w celu zautomatyzowania reakcji na zagrożenie EDR przy użyciu języka Python. Metody te można wywołać po ich zintegrowaniu z rozwiązaniami SIEM. *Kaspersky Unified Monitoring and Analysis Platform* to rozwiązanie SIEM firmy Kaspersky, które obsługuje interfejs OpenAPI reagowania na zagrożenia EDR od wersji 3.4.1. Przykładowe skrypty można znaleźć w dokumentacji KUMA.

Aby wykonać działania w ramach reagowania na zagrożenia EDR, należy utworzyć żądanie i wysłać je za pomocą interfejsu KSC Open API (`AddIncident`). Po przetworzeniu żądania w konsoli Kaspersky Security Center tworzone jest specjalne zadanie.

Aby tworzyć zadania podczas reagowania na zagrożenia EDR, należy nawiązać połączenie w tle między Serwerem administracyjnym a Kaspersky Security Center Web Console. Usługa połączenia w tle jest dostępna w Kaspersky Security Center dla systemu Windows w wersji 14.2 lub nowszej oraz w wersji w Kaspersky Security Center Linux 15.2 lub nowszej. Inne konsole, w tym konsole rozwiązań Kaspersky Detection and Response, nie są obsługiwane.

W przypadku odpowiedzi na zagrożenia EDR konieczne jest określenie podstawowych parametrów żądania, na przykład w formacie JSON:

- `task` jest typem zadania (patrz poniżej).
- `targetHost` jest identyfikatorem komputera, na którym ma zostać uruchomiony skrypt. Wymagany argument. Skrypt pobiera ten argument ze zdarzenia.
- `responseEventIncidentArea` jest nazwą aplikacji, która uruchomiła skrypt (na przykład `KUMA`). Ten parametr jest dodawany do nazwy tworzonego zadania.

Aby skonfigurować usługę rozpoznawania zagrożeń EDR, należy określić ustawienia zadania w formacie JSON w parametrze `"KLINCDT_BODY": json.dumps(data)`. W rezultacie aplikacja tworzy `[Response][KUMA] <task type> - <Date> <Time> - <ID>` w konsoli Kaspersky Security Center.

Łączenie z OpenAPI Kaspersky Security Center

Aplikacja tworzy specjalne zadania w konsoli Kaspersky Security Center w ramach reakcji na zagrożenia EDR. Utworzenie tych zadań wymaga nawiązania połączenia między komputerem a Kaspersky Security Center. W tym celu należy określić w żądaniu parametry połączenia Kaspersky Security Center.

W Kaspersky XDR w wersji 2.1 zmieniono metodę autoryzacji żądań. Kaspersky XDR wykorzystuje tokeny PAT zamiast uwierzytelniania za pomocą nazwy użytkownika i hasła. Z tego powodu nie jest możliwe uruchamianie skryptów w Kaspersky XDR. Więcej informacji na temat autoryzacji żądań można znaleźć w pomocy dla Kaspersky XDR.

Parametry połączenia Kaspersky Security Center

Parametr	Typ	Opis
`kscHost`	`string`	Adres serwera administracyjnego Kaspersky Security Center. Parametr wymagany.
`kscPort`	`int`	Port połączenia z Serwerem administracyjnym. Parametr wymagany.
`kscCert`	`string`	Ścieżka do pliku certyfikatu umożliwiającego połączenie z Serwerem administracyjnym Kaspersky Security Center. Parametr jest domyślnie ustawiony na `False`.
`kscUser`	`string`	Nazwa konta użytkownika. Parametr wymagany.
`kscPassword`	`string`	Hasło do konta użytkownika. Parametr wymagany.

Na przykład

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

Dane konta użytkownika nie są chronione, dlatego należy utworzyć osobne konto użytkownika, które będzie używane wyłącznie do wykonywania tych czynności.

Uzyskaj plik – getFile

Ustawienia zadania Uzyskaj plik

Parametr	Typ	Opis
md5hash	string	Skrót MD5 pliku, który chcesz uzyskać.
sha256hash	string	Skrót SHA256 pliku, który chcesz uzyskać.
path	string	Ścieżka do pliku, który chcesz uzyskać.

Na przykład

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Usuń plik – deleteFile

Ustawienia zadania Usuń plik

Parametr	Typ	Opis
md5hash	string	Skrót MD5 pliku, który chcesz usunąć.
sha256hash	string	Skrót SHA256 pliku, który chcesz usunąć.
path	string	Ścieżka do pliku, który chcesz usunąć.
searchInSubfolders?	boolean	Znajdź w podfolderach plik, który chcesz usunąć.

Na przykład

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

Przenieś plik do Kwarantanny – quarantineFile

Ustawienia zadania Przenieś plik do Kwarantanny

Parametr	Typ	Opis
`md5hash`	`string`	Skrót MD5 pliku, który chcesz poddać kwarantannie.
`sha256hash`	`string`	Skrót SHA256 pliku, który chcesz poddać kwarantannie.
`path`	`string`	Ścieżka do pliku, który chcesz poddać kwarantannie.

Na przykład

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Skanowanie IOC – iocScan

Ustawienia zadania Skanowanie IOC

Parametr	Typ	Opis
`ioc`	`string`	Ścieżka do archiwum ZIP zawierającego plik IOC, którego chcesz użyć do skanowania.
`isolateHost`	`boolean`	W przypadku wykrycia oznak zagrożenia należy odizolować komputer od sieci, aby zapobiec jego rozprzestrzenianiu.
`scanCriticalAreas`	`boolean`	Uruchom zadanie *Skanowanie obszarów krytycznych* po wykryciu oznak zagrożenia.
`quarantineObject`	`boolean`	Usuń szkodliwy obiekt po wykryciu oznak zagrożenia. Przed usunięciem obiektu Kaspersky Endpoint Security utworzy kopię zapasową w przypadku, gdy obiekt musi zostać przywrócony w późniejszym czasie. Kaspersky Endpoint Security przeniesie kopię zapasową do Kwarantanny.

Na przykład

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

Rozpocznij proces – startProcess

Ustawienia zadania Rozpocznij proces

Parametr	Typ	Opis
executablePath	string	Ścieżka do pliku wykonywalnego używanego do uruchomienia procesu.
arguments?	string	Dodatkowe argumenty wiersza poleceń służące do uruchomienia procesu.
workingFolder?	string	Ścieżka do folderu roboczego procesu.

Na przykład

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

Zakończ proces – terminateProcess

Ustawienia zadania Zakończ proces

Parametr	Typ	Opis
md5hash	string	Skrót MD5 pliku, którego proces chcesz zakończyć.
sha256hash	string	Skrót SHA256 pliku, którego proces chcesz zakończyć.
path	string	Ścieżka do pliku, który chcesz usunąć.
caseSensitive	boolean	Rozróżnianie wielkości liter podczas wyszukiwania pliku.

Na przykład

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Izolacja sieci komputerowej — isolateHost

Ustawienia izolacji sieci komputerowej

Parametr	Typ	Opis
`action`	`string`	Tryb działania izolacji od sieci.

Na przykład

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Zapobieganie wykonywaniu — preventExecution

Ustawienia zapobiegania wykonywania

Parametr	Typ	Opis
`hash`	`string`	Skrót MD5 pliku, którego uruchomieniu chcesz zapobiec.
`path`	`string`	Ścieżka do pliku, którego uruchomieniu chcesz zapobiec.
`caseSensitive`	`boolean`	Rozróżnianie wielkości liter podczas wyszukiwania pliku.

Na przykład

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Skanowanie w poszukiwaniu złośliwego oprogramowania – onDemandScan

Ustawienia zadania Skanowanie w poszukiwaniu złośliwego oprogramowania

Parametr	Typ	Opis
`path`	`string`	Rozdzielona spacjami lista plików i folderów do celów skanowania niestandardowego.
`recursive`	`boolean`	Tryb skanowania cyklicznego.

Parametr	Typ	Opis
type	number	Obszar skanowania.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Na przykład

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

Dodatek 12. Konta użytkowników w regułach składników aplikacji

Aby skonfigurować niektóre składniki aplikacji, musisz dodać reguły. Na przykład w przypadku Kontroli sieci należy dodać zasadę z listą adresów internetowych, które aplikacja ma blokować. W regułach składników aplikacji możesz także skonfigurować harmonogram dla składników lub wybrać użytkowników, do których aplikacja ma zastosować regułę.

Reguły należy dodać, aby skonfigurować następujące składniki aplikacji:

- Kontrola aplikacji.
- Kontrola sieci.
- Kontrola urządzeń.
- Kontrola dziennika.
- Adaptacyjna kontrola anomalii.
- Monitor integralności systemu.

Począwszy od wersji Kaspersky Endpoint Security for Windows 12.5 można wybierać użytkowników nie tylko z Active Directory, ale także z listy użytkowników w Kaspersky Security Center. Możesz także ręcznie wprowadzić dane lokalnego konta użytkownika. Oznacza to, że możesz dodawać użytkowników w następujący sposób:

- Active Directory (zalecane)
- Lista użytkowników w Kaspersky Security Center
- Lokalne konto użytkownika

Aby móc poprawnie stosować wszystkie metody wyboru użytkownika, należy zaktualizować aplikację Kaspersky Endpoint Security oraz wtyczkę zarządzającą do wersji 12.5 lub nowszej.

Kaspersky zaleca używanie lokalnych kont użytkowników tylko w szczególnych przypadkach, gdy nie jest możliwe korzystanie z kont użytkowników domeny. Szczegółowe informacje na temat zagrożeń bezpieczeństwa związanych z korzystaniem z kont lokalnych można znaleźć w Bazie wiedzy Microsoft. Użytkownik ponosi pełną odpowiedzialność za bezpieczeństwo komputera, jeśli używane są lokalne konta użytkowników; w szczególności obejmuje to odpowiedzialność za kontrolowanie i ograniczanie dostępu do ustawień Kaspersky Endpoint Security.

Aplikacja wykorzystuje identyfikator SID (identyfikator zabezpieczeń) użytkownika do identyfikacji użytkowników. Podczas korzystania z kont użytkowników z usługi Active Directory lub z listy użytkowników Kaspersky Security Center aplikacja określa identyfikator SID na serwerze administracyjnym. Oznacza to, że aplikacja nie obciąża komputera dodatkowym obciążeniem w celu identyfikacji użytkownika. Jeśli do zasady aplikacji dodano więcej niż 1000 lokalnych kont użytkowników, aplikacje kontaktują się z kontrolerem domeny w celu zidentyfikowania użytkownika. Oznacza to zwiększone obciążenie komputera. Aby zoptymalizować wpływ na wydajność komputera, zalecamy korzystanie z kont użytkowników z Active Directory lub listy użytkowników Kaspersky Security Center.

Aplikacja wykorzystuje nazwy NetBIOS do identyfikacji ręcznie dodanych kont użytkowników w formatach `<username>` i `<hostname>\<username>`. Nazwa NetBIOS może mieć długość do 16 bajtów (15 znaków). Jeśli nazwa komputera ma więcej niż 15 znaków, aplikacja nie zidentyfikuje użytkownika. Następnie aplikacja wyłączy regułę i wygeneruje błąd, na przykład: *Kontrola sieci: wyzwalanie reguły wyłączone dla kont użytkowników bez pasującego identyfikatora zabezpieczeń (SID).* Aby reguła zadziałała, musisz ręcznie skrócić nazwę komputera. Konta użytkowników można dodawać z Active Directory lub Kaspersky Security Center. W tym przypadku aplikacja automatycznie skraca nazwę komputera.

Kaspersky Endpoint Security obsługuje również wbudowanych użytkowników i grupy (takie jak grupa „Wszystkie") w regułach. Ze względu na sposób ustalania identyfikatora SID użytkownika aplikacja pozwala na korzystanie wyłącznie z wbudowanych kont użytkowników dodanych z usługi Active Directory lub listy użytkowników w Kaspersky Security Center. Reguły, w których wbudowane konto użytkownika jest dodawane lokalnie, nie działają.

Informacje prawne

Przekazywanie danych

W tej sekcji znajdują się informacje o danych, które aplikacja Kaspersky Endpoint Security może przechowywać na urządzeniu i automatycznie przesyłać do Kaspersky podczas działania.

Kaspersky chroni otrzymywane informacje zgodnie z wymogami wynikającymi z przepisów prawa oraz zasadami obowiązującymi w Kaspersky. Dane są przesyłane za pośrednictwem zaszyfrowanych kanałów komunikacji.

Przekazywanie danych zgodnie z Umową licencyjną

Jeśli do aktywacji Kaspersky Endpoint Security zostanie użyty kod aktywacyjny, użytkownik zgadza się okresowo automatycznie wysyłać do Kaspersky następujące informacje w celu weryfikacji prawidłowego korzystania z aplikacji:

- Typ, wersję i lokalizację Kaspersky Endpoint Security;
- Wersje zainstalowanych aktualizacji dla Kaspersky Endpoint Security;
- Identyfikator komputera i identyfikator konkretnej instalacji Kaspersky Endpoint Security na komputerze;
- Numer seryjny i identyfikator aktywnego klucza;
- Typ, wersję i szybkość transmisji bitów systemu operacyjnego oraz nazwę środowiska wirtualnego (jeśli Kaspersky Endpoint Security jest zainstalowany w środowisku wirtualnym);
- unikalny identyfikator żądania usług Rightholder;
- Identyfikatory składników Kaspersky Endpoint Security, które są aktywne podczas przesyłania informacji.

Kaspersky może również wykorzystywać te informacje do generowania statystyk dotyczących rozpowszechniania i użytkowania oprogramowania Kaspersky.

Korzystając z kodu aktywacyjnego, zgadzasz się na automatyczne przesyłanie danych wymienionych powyżej. Jeśli nie zgadzasz się na przesłanie tych informacji do Kaspersky, powinieneś użyć pliku klucza do aktywacji Kaspersky Endpoint Security.

Akceptując warunki Umowy licencyjnej, wyrażasz zgodę na automatyczne przesyłanie następujących informacji:

- Podczas aktualizacji wersji Kaspersky Endpoint Security:
  - Wersji Kaspersky Endpoint Security;
  - ID programu Kaspersky Endpoint Security;
  - Aktywnego klucza;

- Unikatowego numeru ID uruchomienia zadania aktualizacji;
- Unikatowego numeru ID instalacji Kaspersky Endpoint Security.

- Podczas klikania następujących odnośników w interfejsie Kaspersky Endpoint Security:
  - Wersji Kaspersky Endpoint Security;
  - Wersji systemu operacyjnego;
  - Daty aktywacji Kaspersky Endpoint Security;
  - Daty wygaśnięcia licencji;
  - Daty utworzenia klucza;
  - Daty instalacji Kaspersky Endpoint Security;
  - ID programu Kaspersky Endpoint Security;
  - ID wykrytej luki w systemie operacyjnym;
  - ID ostatniej aktualizacji zainstalowanej dla Kaspersky Endpoint Security;
  - Sumy kontrolnej wykrytego pliku z zagrożeniem oraz nazwy tego zagrożenia zgodnej z klasyfikacją Kaspersky;
  - Kategorii błędu aktywacji Kaspersky Endpoint Security;
  - Kodu błędu aktywacji Kaspersky Endpoint Security;
  - Liczby dni pozostałych do wygaśnięcia klucza;
  - Liczby dni, jaka minęła od dodania klucza;
  - Liczby dni, jaka minęła od wygaśnięcia licencji;
  - Liczby komputerów, na których zastosowana jest bieżąca licencja;
  - Aktywnego klucza;
  - Okresu ważności licencji Kaspersky Endpoint Security;
  - Bieżącego stanu licencji;
  - Typu bieżącej licencji;
  - Typu aplikacji;
  - Unikatowego numeru ID uruchomienia zadania aktualizacji;
  - Unikatowego numeru ID instalacji Kaspersky Endpoint Security na komputerze;
  - Języka interfejsu Kaspersky Endpoint Security.

Kaspersky chroni otrzymywane informacje zgodnie z wymogami wynikającymi z przepisów prawa oraz zasadami obowiązującymi w Kaspersky. Dane są przesyłane za pośrednictwem zaszyfrowanych kanałów komunikacji.

Przeczytaj Umowę licencyjną i odwiedź stronę internetową Kaspersky, aby dowiedzieć się więcej o otrzymywaniu, przetwarzaniu, przechowywaniu i niszczeniu przez Kaspersky informacji dotyczących korzystania z aplikacji po zaakceptowaniu Umowy licencyjnej i Oświadczenia Kaspersky Security Network. Pliki license.txt i ksn_<ID języka>.txt zawierają treść Umowy licencyjnej i Oświadczenia Kaspersky Security Network i można je znaleźć w pakiecie dystrybucyjnym aplikacji.

Przekazywanie danych podczas korzystania z Kaspersky Security Network

Zestaw danych, jaki Kaspersky Endpoint Security wysyła do Kaspersky, zależy od typu licencji i ustawień korzystania z Kaspersky Security Network.

Korzystanie z KSN zgodnie z licencją na więcej niż 4 komputerach

Akceptując Oświadczenie Kaspersky Security Network, wyrażasz zgodę na automatyczne przesyłanie następujących informacji:

- informacje o aktualizacjach konfiguracji KSN: identyfikator aktywnej konfiguracji, identyfikator otrzymanej konfiguracji, kod błędu dla aktualizacji konfiguracji;
- informacje o plikach i adresach URL wymagających skanowania: sumy kontrolne skanowanych plików (MD5, SHA2-256, SHA1) i wzorce plików (MD5), rozmiar wzorca, typ wykrytego zagrożenia i jego nazwę według klasyfikacji Posiadacza Praw, identyfikator dla antywirusowych baz danych, adres URL, którego reputacja jest sprawdzana, a także adres URL strony odsyłającej, identyfikator protokołu połączenia oraz numer używanego portu;
- ID zadania skanowania, które wykryło zagrożenie;
- informacje o używanych certyfikatach cyfrowych, wymagane do zweryfikowania ich autentyczności: sumy kontrolne (SHA256) certyfikatu użytego do podpisania przeskanowanego obiektu oraz klucz publiczny certyfikatu;
- identyfikator komponentu Oprogramowania przeprowadzającego skanowanie;
- identyfikatory antywirusowych baz danych i zapisów w tych antywirusowych bazach danych;
- informacje o aktywności Oprogramowania na Komputerze: podpisany nagłówek biletu z usługi aktywacji (identyfikator regionalnego centrum aktywacji, suma kontrolna kodu aktywacyjnego, suma kontrolna biletu, data utworzenia biletu, unikatowy identyfikator biletu, wersja biletu, stan licencji, data i godzina rozpoczęcia/zakończenia okresu ważności biletu, unikatowy identyfikator licencji, wersja licencji), identyfikator certyfikatu, użytego do podpisania nagłówka biletu, suma kontrolna (MD5) pliku klucza;
- informacje o Oprogramowaniu Posiadacza praw: pełna wersja, typ, wersja protokołu użytego do nawiązania połączenia z usługami Kaspersky.

Korzystanie z KSN zgodnie z licencją na 5 lub więcej komputerach

Akceptując Oświadczenie Kaspersky Security Network, wyrażasz zgodę na automatyczne przesyłanie następujących informacji:

Jeśli pole **Kaspersky Security Network** jest zaznaczone, a pole **Włącz rozszerzony tryb KSN** jest odznaczone, aplikacja przesyła następujące informacje:

- informacje o aktualizacjach konfiguracji KSN: identyfikator aktywnej konfiguracji, identyfikator otrzymanej konfiguracji, kod błędu dla aktualizacji konfiguracji;
- informacje o plikach i adresach URL wymagających skanowania: sumy kontrolne skanowanych plików (MD5, SHA2-256, SHA1) i wzorce plików (MD5), rozmiar wzorca, typ wykrytego zagrożenia i jego nazwę według klasyfikacji Posiadacza Praw, identyfikator dla antywirusowych baz danych, adres URL, którego reputacja jest sprawdzana, a także adres URL strony odsyłającej, identyfikator protokołu połączenia oraz numer używanego portu;
- ID zadania skanowania, które wykryło zagrożenie;
- informacje o używanych certyfikatach cyfrowych, wymagane do zweryfikowania ich autentyczności: sumy kontrolne (SHA256) certyfikatu użytego do podpisania przeskanowanego obiektu oraz klucz publiczny certyfikatu;
- identyfikator komponentu Oprogramowania przeprowadzającego skanowanie;
- identyfikatory antywirusowych baz danych i zapisów w tych antywirusowych bazach danych;
- informacje o aktywności Oprogramowania na Komputerze: podpisany nagłówek biletu z usługi aktywacji (identyfikator regionalnego centrum aktywacji, suma kontrolna kodu aktywacyjnego, suma kontrolna biletu, data utworzenia biletu, unikatowy identyfikator biletu, wersja biletu, stan licencji, data i godzina rozpoczęcia/zakończenia okresu ważności biletu, unikatowy identyfikator licencji, wersja licencji), identyfikator certyfikatu, użytego do podpisania nagłówka biletu, suma kontrolna (MD5) pliku klucza;
- informacje o Oprogramowaniu Posiadacza praw: pełna wersja, typ, wersja protokołu użytego do nawiązania połączenia z usługami Kaspersky.

Jeśli pole **Włącz rozszerzony tryb KSN** jest zaznaczone wraz z polem **Kaspersky Security Network**, oprócz powyższych informacji aplikacja przesyła także następujące informacje:

- informacje o wynikach kategoryzacji żądanych zasobów internetowych, które zawierają przetwarzane adresy URL i IP hosta, wersję komponentu Oprogramowania, który przeprowadził kategoryzację, metodę kategoryzacji i zestaw kategorii zdefiniowany dla zasobu internetowego;
- informacje o oprogramowaniu zainstalowanym na Komputerze: nazwy aplikacji i producentów oprogramowania, klucze rejestru i ich wartości, informacje o plikach zainstalowanych komponentów oprogramowania (sumy kontrolne (MD5, SHA2-256, SHA1), nazwa, ścieżka do pliku na Komputerze, rozmiar, wersja i podpis cyfrowy);
- informacje o stanie antywirusowej ochrony Komputera: wersje i znaczniki czasu publikacji używanych antywirusowych baz danych, identyfikator zadania i identyfikator Oprogramowania, które przeprowadza skanowanie;

- informacje o plikach pobieranych przez Użytkownika Końcowego: adresy URL i IP pobrań i stron pobierania, identyfikator protokołu pobierania i numer portu połączenia, status złośliwości lub braku złośliwości adresu URL, atrybuty, rozmiar i sumy kontrolne plików (MD5, SHA2-256, SHA1), informacje o procesie, który pobrał plik (sumy kontrolne (MD5, SHA2-256, SHA1), datę i czas utworzenia/zbudowania, stan automatycznego uruchamiania, atrybuty, nazwy programów pakujących, informacje o sygnaturach, znacznik, identyfikator formatu i entropię pliku wykonywalnego), nazwę pliku i jego ścieżkę na Komputerze, podpis cyfrowy pliku i znacznik czasu jego utworzenia, adres URL miejsca wykrycia, numer skryptu na podejrzanej lub szkodliwej stronie, informacje o wygenerowanych żądaniach HTTP i odpowiedzi na nie;

- informacje o uruchomionych aplikacjach i ich modułach: dane o procesach działających w systemie (identyfikator procesu (PID), nazwę procesu, informacje o koncie, z którego proces został uruchomiony, aplikację i polecenie, które uruchomiły proces, znacznik zaufanego programu lub procesu, pełną ścieżkę plików procesu i ich sum kontrolnych (MD5, SHA2-256, SHA1) oraz uruchamianie wiersza polecenia, poziom integralności procesu, opis produktu, do którego należy proces (nazwę produktu i informacje o wydawcy), używane certyfikaty cyfrowe i informacje niezbędne do zweryfikowania ich autentyczności lub informacje o braku podpisu cyfrowego pliku), a także informacje o modułach załadowanych do procesów (ich nazwy, rozmiary, typy, daty utworzenia, atrybuty, sumy kontrolne (MD5, SHA2-256, SHA1), ścieżki na Komputerze), informacje o nagłówku pliku PE, nazwy programów pakujących (jeśli plik był spakowany);

- informacje o wszystkich potencjalnie szkodliwych obiektach i aktywnościach: nazwa wykrytego obiektu i pełna ścieżka dostępu do obiektu na komputerze, sumy kontrolne przetworzonych plików (MD5, SHA2-256, SHA1), data i godzina wykrycia, nazwy i rozmiary zainfekowanych plików i ścieżki dostępu do tych plików, kod szablonu ścieżki dostępu, flaga pliku wykonywalnego, wskaźnik określający, czy obiekt znajduje się w kontenerze, nazwy narzędzi pakujących (jeśli plik został spakowany), kod typu pliku, ID formatu pliku, lista działań wykonanych przez szkodliwe oprogramowanie oraz decyzja podjęta przez oprogramowanie i reakcja użytkownika, identyfikatory antywirusowych baz danych oraz wpisy w tych antywirusowych bazach danych, które zostały użyte do podjęcia decyzji, wskaźnik potencjalnie szkodliwego obiektu, nazwa wykrytego zagrożenia zgodna z klasyfikacją Posiadacza praw, poziom zagrożenia, stan wykrycia i metoda wykrycia, powód włączenia do analizowanego kontekstu i numer sekwencyjny pliku w kontekście, sumy kontrolne (MD5, SHA2-256, SHA1), nazwa i atrybuty pliku wykonywalnego aplikacji, poprzez którą przesłana została zainfekowana wiadomość lub odnośnik, zdepersonalizowane adresy IP (IPv4 i IPv6) hosta zablokowanego obiektu, entropia pliku, wskaźnik automatycznego uruchomienia pliku, godzina pierwszego wykrycia pliku w systemie, liczba uruchomień pliku od ostatniego wysłania statystyk, informacje o nazwie, sumy kontrolne (MD5, SHA2-256, SHA1) oraz rozmiar klienta poczty, poprzez którego otrzymano szkodliwy obiekt, ID zadania oprogramowania, które przeprowadziło skanowanie, wskaźnik pokazujący, czy podpis lub reputacja pliku zostały sprawdzone, wynik przetworzenia pliku, suma kontrolna (MD5) wzorca zebranego dla obiektu, rozmiar wzorca w bajtach i specyfikacje techniczne zastosowanych technologii wykrywania;

- informacje o skanowanych obiektach: przypisaną grupę zaufania, do której i/lub z której plik został umieszczony, powód, dla którego plik umieszczono w danej kategorii, identyfikator kategorii, informacje o źródle kategorii i wersji bazy danych kategorii, znacznik certyfikatu zaufania pliku, nazwę dostawcy pliku, wersję pliku, nazwę i wersję aplikacji, do której należy plik;

- informacje o wykrytych lukach w zabezpieczeniach: identyfikator luki w bazie danych luk, klasę zagrożenia luki;

- informacje o emulacji pliku wykonywalnego: rozmiar pliku i jego sumy kontrolne (MD5, SHA2-256, SHA1), wersję komponentu emulatora, głębokość emulacji, tablicę właściwości bloków logicznych i funkcji w obrębie bloków logicznych uzyskanych podczas emulacji oraz dane z nagłówków PE pliku wykonywalnego;

- adresy IP atakującego komputera (IPv4 i IPv6), numer portu na Komputerze będącym celem ataku sieciowego, identyfikator protokołu pakietu IP zawierającego atak, cel ataku (nazwę organizacji, stronę internetową), znacznik reakcji na atak, wagę ataku, poziom zaufania;

- informacje o atakach powiązanych ze sfałszowanymi zasobami sieciowymi, adresy DNS i IP (IPv4 i IPv6) odwiedzonych stron internetowych;

- adresy DNS i IP (IPv4 lub IPv6) zażądanego zasobu sieciowego, informacje o pliku i kliencie sieci Web uzyskujących dostęp do zasobu sieciowego, nazwę, rozmiar i sumy kontrolne (MD5, SHA2-256, SHA1) pliku, pełną ścieżkę do pliku oraz kod szablonu ścieżki, wynik weryfikacji jego podpisu cyfrowego i jego stan w KSN;

- informacje o wycofaniu szkodliwych działań: dane dotyczące pliku, którego aktywność została wycofana (nazwa pliku, pełna ścieżka dostępu do pliku, jego rozmiar i sumy kontrolne (MD5, SHA2-256, SHA1)), dane dotyczące pomyślnych i niepomyślnych działań mających na celu usunięcie, zmianę nazwy i skopiowanie plików oraz przywrócenie wartości w rejestrze (nazwy kluczy rejestru i ich wartości) oraz informacje o plikach systemowych zmodyfikowanych przez szkodliwe oprogramowanie, przed i po wycofaniu działań;

- informacje o wyłączeniach ustawionych dla komponentu Adaptacyjna kontrola anomalii: identyfikator i stan reguły, która została wyzwolona, czynność wykonywaną przez Oprogramowanie podczas wyzwalania reguły, rodzaj konta użytkownika, w ramach którego proces lub wątek wykonuje podejrzaną aktywność, informacje o procesie, który był przedmiotem podejrzanej aktywności (identyfikator skryptu lub nazwa pliku procesu, pełna ścieżka do pliku procesu, kod szablonu ścieżki, sumy kontrolne (MD5, SHA2-256, SHA1) pliku procesu); informacje o obiekcie, który wykonał podejrzane aktywności, jak również o obiekcie, który był przedmiotem podejrzanych aktywności (nazwa klucza rejestru lub nazwa pliku, pełna ścieżka do pliku, kod szablonu ścieżki oraz sumy kontrolne (MD5, SHA2-256, SHA1) pliku);

- informacje o załadowanych modułach oprogramowania: nazwa, rozmiar i sumy kontrolne (MD5, SHA2-256, SHA1) pliku modułu, pełna ścieżka dostępu do niego oraz kod szablonu ścieżki dostępu, ustawienia podpisu cyfrowego pliku modułu, data i godzina utworzenia podpisu, nazwa podmiotu i organizacji, która podpisała plik modułu, ID procesu, w którym moduł został załadowany, nazwa dostawcy modułu oraz numer sekwencyjny modułu w kolejce ładowania;

- informacje o jakości interakcji Oprogramowania z usługami KSN: datę i godzinę rozpoczęcia i zakończenia okresu, w którym generowane były statystyki, informacje o jakości żądań i połączeniu z każdą z wykorzystywanych usług KSN (identyfikator usługi KSN, liczba udanych żądań, liczba żądań z odpowiedziami z pamięci podręcznej, liczba nieudanych żądań (problemy sieciowe, wyłączenie KSN w ustawieniach Oprogramowania, nieprawidłowe przekierowanie), rozłożenie w czasie udanych żądań, rozkład w czasie anulowanych żądań, rozkład w czasie żądań z przekroczonym limitem czasu, liczbę połączeń do KSN pobranych z pamięci podręcznej, liczbę udanych połączeń do KSN, liczbę nieudanych połączeń do KSN, liczbę udanych transakcji, liczbę nieudanych transakcji, rozkład w czasie udanych połączeń do KSN, rozkład w czasie nieudanych połączeń do KSN, rozkład w czasie udanych transakcji, rozkład w czasie nieudanych transakcji);

- informacje na temat danych w pamięci procesów w przypadku usunięcia potencjalnie złośliwego obiektu: elementy hierarchii obiektów systemu (ObjectManager), dane w pamięci UEFI BIOS oraz nazwy kluczy rejestru i ich wartości;

- informacje o zdarzeniach w dziennikach systemowych: znacznik czasu zdarzenia, nazwa dziennika, w którym znaleziono zdarzenie, typ i kategoria zdarzenia oraz nazwa źródła zdarzenia i opis zdarzenia;

- informacje o połączeniach sieciowych: wersja i sumy kontrolne (MD5, SHA2-256, SHA1) pliku, z którego uruchomiono proces, który otworzył port, ścieżka do pliku procesu i jego podpis cyfrowy, lokalne i zdalne adresy IP, numery lokalnych i zdalnych portów połączeń, stan połączenia oraz znacznik czasu otwarcia portu;

- informacje o dacie instalacji i aktywacji Oprogramowania na Komputerze: ID partnera, który sprzedał licencję, numer seryjny licencji, podpisany nagłówek zgłoszenia z usługi aktywacji (ID regionalnego centrum aktywacji, suma kontrolna kodu aktywacyjnego, suma kontrolna zgłoszenia, data utworzenia zgłoszenia, unikatowy ID zgłoszenia, wersja zgłoszenia, stan licencji, data i godzina rozpoczęcia/zakończenia zgłoszenia, unikatowy ID licencji, wersja licencji), ID certyfikatu użytego do podpisania nagłówka zgłoszenia, suma kontrolna (MD5) pliku klucza, unikatowy ID instalacji Oprogramowania na Komputerze, typ i ID aplikacji, która jest aktualizowana, ID zadania aktualizacji;

- informacje o zestawie wszystkich zainstalowanych aktualizacji oraz zestawie ostatnio zainstalowanych/usuniętych aktualizacji, typ zdarzenia, które spowodowało przesłanie informacji o aktualizacji, czas od instalacji ostatniej aktualizacji oraz informacje o wszelkich aktualnie zainstalowanych antywirusowych bazach danych;

- informacje o działaniu oprogramowania na komputerze: dane dotyczące użycia procesora, dane dotyczące użycia pamięci (Bajty prywatne, Pula niestronicowana, Pula stronicowana), liczba aktywnych wątków w procesie oprogramowania i oczekujące wątki, a także czas działania oprogramowania przed wystąpieniem błędu;

- liczbę zrzutów oprogramowania i zrzutów systemu (BSOD - niebieski ekran śmierci) od momentu zainstalowania Oprogramowania oraz od momentu ostatniej aktualizacji, identyfikator i wersję modułu Oprogramowania, który uległ awarii, stos pamięci w procesie Oprogramowania oraz informacje o antywirusowych bazach danych w momencie awarii;

- dane na temat zrzutu systemu (BSOD - niebieski ekran śmierci): znacznik wskazujący wystąpienie niebieskiego ekranu na Komputerze, nazwę sterownika, którzy spowodował wystąpienie niebieskiego ekranu, adres i stos pamięci w sterowniku, znacznik wskazujący czas trwania sesji systemu operacyjnego przed wystąpieniem niebieskiego ekranu, stos pamięci sterownika, który uległ awarii, typ przechowywanego zrzutu pamięci, znacznik sesji systemu operacyjnego informujący o trwaniu jego sesji przez ponad 10 minut przed wystąpieniem niebieskiego ekranu, unikatowy identyfikator zrzutu oraz znacznik czasu niebieskiego ekranu;

- informacje o błędach lub problemach z wydajnością, które wystąpiły podczas pracy komponentów Oprogramowania: identyfikator stanu Oprogramowania, typ błędu, kod i przyczynę oraz czas wystąpienia błędu, identyfikatory komponentu, modułu i procesu produktu, w którym wystąpił błąd, identyfikator zadania lub kategorii aktualizacji, w której wystąpił błąd, rejestry sterowników wykorzystywanych przez Oprogramowanie (kod błędu, nazwa modułu, nazwa pliku źródłowego oraz linia, w której wystąpił błąd);

- informacje o aktualizacjach antywirusowych baz danych i składników Oprogramowania: nazwę, datę i godzinę indeksowania plików pobranych podczas ostatniej aktualizacji i pobieranych podczas bieżącej aktualizacji;

- informacje o nieprawidłowym zakończeniu działania Oprogramowania: znacznik czasu utworzenia zrzutu, jego typ, typ zdarzenia, które spowodowało nieprawidłowe zakończenie działania Oprogramowania (nieoczekiwanego wyłączenia zasilania, awarii aplikacji innej firmy) oraz datę i czas nieoczekiwanego wyłączenia zasilania;

- informacje o kompatybilności sterowników Oprogramowania ze sprzętem i Oprogramowaniem: informacje o właściwościach systemu operacyjnego ograniczających funkcjonalność komponentów Oprogramowania (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), typ zainstalowanego Oprogramowania do pobrania (UEFI, BIOS), identyfikator modułu Trusted Platform Module (TPM), wersję specyfikacji TPM, informacje o procesorze zainstalowanym w Komputerze, tryb pracy i parametry Code Integrity i Device Guard, tryb pracy sterowników i powód korzystania z aktualnego trybu, wersję sterowników Oprogramowania, stan obsługi wirtualizacji oprogramowania i sprzętu Komputera;

- informacje o aplikacjach innych firm, które spowodowały błąd: ich nazwy, wersje i lokalizacje, kod błędu i informacje o błędzie z dziennika systemowego aplikacji, adres błędu i stos pamięci aplikacji innej firmy, znacznik wskazujący wystąpienie błędu w komponencie Oprogramowania, czas działania aplikacji innej firmy przed wystąpieniem błędu, sumy kontrolne (MD5, SHA2-256, SHA1) obrazu procesu aplikacji, w którym wystąpił błąd, ścieżkę obrazu procesu aplikacji i kod szablonu ścieżki, informację z dziennika systemowego z opisem błędu powiązanego z aplikacją, informacje o module aplikacji, w którym wystąpił błąd (identyfikator wyjątku, adres pamięci związany z awarią jako przesunięcie w module aplikacji, nazwę i wersję modułu, identyfikator awarii aplikacji we wtyczce Posiadacza Praw i stos pamięci z awarii, a także czas trwania sesji aplikacji przed awarią);

- wersję komponentu aktualizującego Oprogramowania, liczbę awarii komponentu aktualizującego w czasie trwania zadań aktualizacji przez łączny czas działania komponentu, identyfikator typu zadania aktualizacji, liczbę nieudanych prób ukończenia zadań aktualizacji przez komponent aktualizujący;

- informacje o działaniu komponentów monitorujących system Oprogramowania: pełne wersje komponentów, datę i godzinę uruchomienia komponentów, kod zdarzenia, które przepełniło kolejkę zdarzeń i liczbę takich zdarzeń, całkowitą liczbę zdarzeń przepełnienia kolejki, informacje o pliku procesu inicjatora zdarzenia (nazwę pliku i jego ścieżkę na Komputerze, kod szablonu ścieżki pliku, sumy kontrolne (MD5, SHA2-256, SHA1) procesu związanego z plikiem, wersję pliku), identyfikator przechwycenia zdarzenia, pełną wersję filtra przechwytującego, identyfikator typu przechwyconego zdarzenia, wielkość kolejki zdarzeń i liczbę zdarzeń pomiędzy pierwszym zdarzeniem w kolejce a bieżącym zdarzeniem, liczbę zaległych zdarzeń w kolejce, informacje o pliku procesu inicjatora bieżącego zdarzenia (nazwę pliku i jego ścieżkę na Komputerze, kod szablonu ścieżki pliku, sumy kontrolne (MD5, SHA2-256, SHA1) procesu związanego z plikiem), czas trwania przetwarzania zdarzenia, maksymalny czas przetwarzania zdarzenia, prawdopodobieństwo wysłania statystyk, informacje o zdarzeniach w systemie operacyjnym, dla których przekroczony został limit czasu przetwarzania (datę i czas zdarzenia, liczbę powtórzeń inicjalizacji antywirusowych baz danych, datę i godzinę ostatniej powtórzonej inicjalizacji antywirusowych baz danych po ich aktualizacji, czas opóźnienia przetwarzania zdarzeń dla każdego komponentu monitorującego system, liczbę zdarzeń oczekujących w kolejce, liczbę przetwarzanych zdarzeń, liczbę opóźnionych zdarzeń bieżącego typu, całkowity czas opóźnienia dla zdarzeń bieżącego typu, całkowity czas opóźnienia dla wszystkich zdarzeń);

- informacje z narzędzia śledzenia zdarzeń Windows (Event Tracing for Windows, ETW) w przypadku problemów z wydajnością Oprogramowania, dostawców zdarzeń SysConfig / SysConfigEx / WinSATAssessment firmy Microsoft: informacje o Komputerze (model, producent, rozmiary obudowy, wersję), informacje o metrykach wydajności systemu Windows (oceny WinSAT, indeks wydajności systemu Windows), nazwę domeny, informacje o procesorach fizycznych i logicznych (liczbę procesorów fizycznych i logicznych, producenta, model, poziom taktowania procesora, liczbę rdzeni, częstotliwość zegara, CPUID, charakterystykę pamięci podręcznej, charakterystykę procesora logicznego, wskaźniki obsługiwanych trybów i instrukcji), informacje o modułach RAM (typ, współczynnik kształtu, producenta, model, pojemność, ziarnistość alokacji pamięci), informacje o interfejsach sieciowych (adresy IP i MAC, nazwę, opis, konfigurację interfejsów sieciowych, podział liczby i wielkości pakietów sieciowych według typu, prędkość wymiany danych w sieci, podział liczby błędów sieciowych według typu), konfigurację kontrolera IDE, adresy IP serwerów DNS, informacje o karcie graficznej (model, opis, producenta, kompatybilność, pojemność pamięci wideo, uprawnienia ekranu, liczbę bitów na piksel, wersję BIOS), informacje o urządzeniach typu plug-and-play (nazwę, opis, identyfikator urządzenia [PnP, ACPI], informacje o dyskach i urządzeniach pamięci masowej (liczbę dysków lub napędów flash, producenta, model, pojemność dysku, liczbę cylindrów, liczbę ścieżek na cylinder, liczbę sektorów na ścieżkę, pojemność sektora, charakterystykę pamięci podręcznej, liczbę sekwencyjną, liczbę partycji, konfigurację kontrolera SCSI), informacje o dyskach logicznych (numer sekwencyjny, pojemność partycji, pojemność wolumenu, literę wolumenu, typ partycji, typ systemu plików, liczbę klastrów, wielkość klastra, liczbę sektorów na klaster, liczbę pustych i zajętych klastrów, literę woluminu rozruchowego, adres przesunięcia partycji w stosunku do początku dysku), informacje o BIOS-ie płyty głównej (producenta, datę publikacji, wersję), informacje o płycie głównej (producenta, model, typ), informacje o pamięci fizycznej (współdzielonej i wolnej pojemności), informacje o usługach systemu operacyjnego (nazwę, opis, stan, znacznik, informacje o procesach [nazwę i PID]), parametry zużycia energii dla Komputera, konfigurację kontrolera przerwań, ścieżkę do folderów systemu Windows (Windows i System32), informacje o systemie operacyjnym (wersję, kompilację, datę wydania, nazwę, typ, datę instalacji), rozmiar pliku stronicowania, informacje o monitorach (liczbę, producenta, zezwolenia ekranu, rozdzielczość, typ), informacje o sterowniku karty graficznej (producenta, datę wydania, wersję);

- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń EventTrace / EventMetadata firmy Microsoft: informacje o kolejności zdarzeń systemowych (typ, godzinę, datę, strefę czasową), metadane o pliku z wynikami śledzenia (nazwę, strukturę, parametry śledzenia, rozbicie liczby operacji śledzenia według typu), informacje o systemie operacyjnym (nazwę, typ, wersję, kompilację, datę wydania, godzinę uruchomienia);

- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń Process / Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power firmy Microsoft: informacje o rozpoczętych i zakończonych procesach (nazwę, PID, parametry uruchamiania, wiersz poleceń, kod zwrotny, parametry zarządzania energią, czas uruchomienia i zakończenia, typ tokena dostępu, SID, SessionID, liczbę zainstalowanych deskryptorów), informacje o zmianach priorytetów wątków (TID, priorytet, czas), informacje o operacjach dyskowych procesu (typ, czas, pojemność, liczbę), historię zmian w strukturze i pojemności procesów dostępnej pamięci;

- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń StackWalk / Perfinfo firmy Microsoft: informacje o licznikach wydajności (wydajność poszczególnych sekcji kodu, kolejność wywołań funkcji, PID, TID, adresy i atrybuty ISR i DPC);

- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń KernelTraceControl-ImageID firmy Microsoft: informacje o plikach wykonywalnych i bibliotekach dynamicznych (nazwę, rozmiar obrazu, pełną ścieżkę), informacje o plikach PDB (nazwę, identyfikator), dane zasobu VERSIONINFO dla plików wykonywalnych (nazwę, opis, twórcę, lokalizację, wersję i identyfikator aplikacji, wersję i identyfikator pliku);

- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń FileIo / DiskIo / Image / Windows Kernel Disk firmy Microsoft: informacje o operacjach na plikach i dyskach (typ, pojemność, czas uruchomienia, czas zakończenia, czas trwania, stan zakończenia, PID, TID, adresy wywołania funkcji sterownika, I/O Request Packet (IRP), atrybuty obiektu pliku Windows), informacje o plikach związanych z operacjami na plikach i na dyskach (nazwę, wersję, rozmiar, pełną ścieżkę, atrybuty, przesunięcie, sumę kontrolną obrazu, opcje otwarcia i dostępu);

- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń PageFault firmy Microsoft: informacje na temat błędów dostępu do strony pamięci (adres, czas, pojemność, PID, TID, atrybuty obiektu pliku Windows, parametry alokacji pamięci);

- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń Thread firmy Microsoft: informacje o tworzeniu/ukończeniu wątków, informacje o uruchomionych wątkach (PID, TID, rozmiar stosu, priorytety i alokację zasobów CPU, zasoby I/O, strony pamięci pomiędzy wątkami, adres stosu, adres funkcji inicjującej, adres bloku środowiska Thread Environment Block (TEB), znacznik usługi Windows);

- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń Microsoft Windows Kernel Memory firmy Microsoft: informacje o operacjach zarządzania pamięcią (stan zakończenia, czas, liczbę, PID), strukturę alokacji pamięci (typ, pojemność, SessionID, PID);

- informacje o działaniu Oprogramowania w przypadku problemów z wydajnością: identyfikator instalacji Oprogramowania, typ i wartość spadku wydajności, informacje o sekwencji zdarzeń w ramach Oprogramowania (czas, strefę czasową, typ, stan zakończenia, identyfikator komponentu Oprogramowania, identyfikator scenariusza działania Oprogramowania, TID, PID, adresy wywołań funkcji), informacje o połączeniach sieciowych do sprawdzenia (URL, kierunek połączenia, rozmiar pakietu sieciowego), informacje o plikach PDB (nazwę, identyfikator, rozmiar obrazu pliku wykonywalnego), informacje o plikach do sprawdzenia (nazwę, pełną ścieżkę, sumę kontrolną), parametry monitorowania wydajności Oprogramowania;

- informacje o ostatnim nieudanym ponownym uruchomieniu systemu operacyjnego: liczbę nieudanych prób ponownego uruchomienia od momentu instalacji systemu operacyjnego, dane na temat zrzutu systemu (kod i parametry błędu, nazwę, wersję i sumę kontrolną (CRC32) modułu, który spowodował błąd działania systemu operacyjnego, adres błędu jako przesunięcie w module, sumy kontrolne (MD5, SHA2-256, SHA1) zrzutu systemu);

- informacje pozwalające zweryfikować autentyczność certyfikatów cyfrowych używanych do podpisywania plików: odcisk palca certyfikatu, algorytm sumy kontrolnej, klucz publiczny i numer seryjny certyfikatu, nazwę wystawcy certyfikatu, wynik weryfikacji certyfikatu i identyfikator bazy danych certyfikatu;

- informacje o procesie uruchamiającym atak na mechanizm autoochrony Oprogramowania: nazwę i rozmiar pliku procesu, jego sumy kontrolne (MD5, SHA2-256, SHA1), pełną ścieżkę pliku procesu i kod szablonu ścieżki pliku, znaczniki czasu utworzenia/zbudowania, znacznik pliku wykonywalnego, atrybuty pliku procesu, informacje o certyfikacie użytym do podpisania pliku procesu, kod konta użytego do uruchomienia procesu, identyfikator operacji wykonanych w celu uzyskania dostępu do procesu, typ zasobu, za pomocą którego operacja jest wykonywana (proces, plik, obiekt rejestru, funkcja wyszukiwania FindWindow), nazwę zasobu, za pomocą którego operacja jest wykonywana, znacznik wskazujący powodzenie operacji, stan pliku procesu i jego sygnaturę według KSN;

- informacje o Oprogramowaniu Posiadacza praw: pełna wersja, typ, lokalizacja i stan działania używanego Oprogramowania, wersje zainstalowanych komponentów Oprogramowania i stanu ich działania, informacje o zainstalowanych aktualizacjach Oprogramowania, wartość filtra TARGET, wersja protokołu użytego do nawiązania połączenia z usługami Posiadacza praw;
- informacje o sprzęcie zainstalowanym na Komputerze: typ, nazwę, nazwę modelu, wersję oprogramowania układowego, parametry urządzeń wbudowanych i podłączonych, unikatowy identyfikator Komputera z zainstalowanym Oprogramowaniem;
- informacje o wersjach systemu operacyjnego i zainstalowanych aktualizacji, długość słowa, edycję i parametry trybu uruchamiania systemu operacyjnego oraz wersję i sumy kontrolne (MD5, SHA2-256, SHA1) pliku jądra systemu operacyjnego, a także datę i godzinę uruchomienia systemu operacyjnego;
- pliki wykonywalne i niewykonywalne, całkowicie lub częściowo;
- części pamięci RAM Komputera;
- sektory zaangażowane w proces rozruchu systemu operacyjnego;
- pakiety danych dotyczące ruchu sieciowego;
- strony internetowe i wiadomości e-mail zawierające podejrzane i szkodliwe obiekty;
- opis klas i instancji klas repozytorium WMI;
- raporty dotyczące aktywności aplikacji:
    - nazwę, rozmiar i wersję przesyłanego pliku, jego opis i sumy kontrolne (MD5, SHA2-256, SHA1), identyfikator formatu pliku, nazwę dostawcy pliku, nazwę produktu, do którego należy plik, pełną ścieżkę do pliku na Komputerze, kod szablonu ścieżki, znaczniki czasu utworzenia i modyfikacji pliku;
    - datę/godzinę rozpoczęcia i zakończenia okresu ważności certyfikatu (jeśli plik posiada podpis cyfrowy), datę i godzinę podpisu, nazwę wystawcy certyfikatu, informacje o właścicielu certyfikatu, odcisk palca, klucz publiczny certyfikatu i odpowiednie algorytmy oraz numer seryjny certyfikatu;
    - nazwę konta, z którego proces został uruchomiony;
    - sumy kontrolne (MD5, SHA2-256, SHA1) nazwy Komputera, na którym proces jest uruchomiony;
    - tytuły okien procesów;
    - Identyfikator antywirusowych baz danych, nazwa wykrytego zagrożenia według klasyfikacji Posiadacza praw;
    - dane na temat zainstalowanej licencji, jej identyfikator, typ i datę wygaśnięcia;
    - lokalny czas Komputera w momencie dostarczenia informacji;
    - nazwy i ścieżki plików, do których proces uzyskał dostęp;
    - nazwy i wartości kluczy rejestru, do których proces uzyskał dostęp;
    - adresy URL i IP, do których proces uzyskał dostęp;
    - adresy URL i IP, z których pobrano uruchomiony plik.

Przekazywanie danych podczas korzystania z rozwiązań Detection and Response

Na komputerach z zainstalowanym programem Kaspersky Endpoint Security przechowywane są dane przygotowane do automatycznego wysłania na serwery Kaspersky Endpoint Detection and Response, Kaspersky Sandbox i Kaspersky Anti Targeted Attack Platform. Pliki są przechowywane na komputerach w zwykłej, niezaszyfrowanej formie.

Określony zestaw danych jest zależny od rozwiązania, w ramach którego używana jest aplikacja Kaspersky Endpoint Security.

Kaspersky Endpoint Detection and Response

Wszystkie dane, które aplikacja przechowuje lokalnie na komputerze, są usuwane z komputera po odinstalowaniu Kaspersky Endpoint Security.

Dane otrzymane w wyniku wykonania zadania Skanowanie IOC (zadanie standardowe)

Kaspersky Endpoint Security automatycznie przesyła dane dotyczące wyników wykonania zadania skanowania *Skanowanie IOC* do Kaspersky Security Center.

Dane uwzględnione w wynikach wykonania zadania *Skanowanie IOC* mogą zawierać następujące informacje:

- Adres IP z tablicy ARP
- Adres fizyczny z tablicy ARP
- Typ i nazwa rekordu DNS
- Adres IP chronionego urządzenia
- Adres fizyczny (adres MAC) chronionego urządzenia
- Identyfikator uwzględniony we wpisie dziennika zdarzeń
- Nazwa źródła danych zapisana w dzienniku
- Nazwa dziennika
- Czas zdarzenia
- Skróty MD5 i SHA256 pliku
- Pełna nazwa pliku (łącznie ze ścieżką)
- Rozmiar pliku

- Zdalny adres IP, z którym nawiązano połączenie podczas skanowania
- Adres IP lokalnej karty sieciowej
- Port otwarty na lokalnej karcie sieciowej
- Numer protokołu (zgodnie ze standardem IANA)
- Nazwa procesu
- Argumenty procesu
- Ścieżka do pliku procesu
- Identyfikator procesu (PID) systemu Windows
- Identyfikator procesu nadrzędnego (PID) systemu Windows
- Konto użytkownika, które rozpoczęło proces
- Data i godzina rozpoczęcia procesu
- Nazwa usługi
- Opis usługi
- Ścieżka i nazwa usługi DLL (svchost)
- Ścieżka i nazwa pliku wykonywalnego usługi
- Identyfikator usługi (PID) systemu Windows
- Typ usługi (na przykład sterownik jądra lub karta sieciowa)
- Stan usługi
- Tryb uruchomienia usługi
- Nazwa konta użytkownika
- Nazwa woluminu
- Litera woluminu
- Typ woluminu
- Wartość rejestru systemu Windows
- Wartość gałęzi rejestru
- Ścieżka klucza rejestru (bez gałęzi i nazwy wartości)
- Ustawienie rejestru
- System (środowisko)

- Nazwa i wersja systemu operacyjnego zainstalowanego na urządzeniu
- Nazwa sieciowa chronionego urządzenia
- Domena lub grupa, do której należy chronione urządzenie
- Nazwa przeglądarki
- Wersja przeglądarki
- Czas ostatniego dostępu do zasobu internetowego
- Adres URL z żądania HTTP
- Nazwa konta użyta w żądaniu HTTP
- Nazwa pliku procesu, który wykonał żądanie HTTP
- Pełna ścieżka do pliku procesu, który wykonał żądanie HTTP
- Identyfikator procesu (PID) systemu Windows, który wykonał żądanie HTTP
- Strona odsyłająca HTTP (adres URL źródła żądania HTTP)
- Identyfikator URI zasobu żądanego przez HTTP
- Informacje o kliencie użytkownika HTTP (aplikacji, która wysłała żądanie HTTP)
- Czas wykonania żądania HTTP
- Unikalny identyfikator procesu, który wykonał zapytanie HTTP

Dane do tworzenia łańcucha rozwoju zagrożeń

Dane do tworzenia łańcucha rozwoju zagrożeń są domyślnie przechowywane przez siedem dni. Dane są automatycznie wysyłane do aplikacji Kaspersky Security Center.

Dane do tworzenia łańcucha rozwoju zagrożeń mogą zawierać następujące informacje:

- Data i godzina incydentu
- Nazwa wykrywania
- Tryb skanowania
- Stan ostatniej akcji związanej z wykrywaniem
- Powód niepowodzenia przetwarzania wykrywania
- Typ wykrytego obiektu
- Nazwa wykrytego obiektu

- Stan zagrożenia po przetworzeniu obiektu
- Powód niepowodzenia wykonywania akcji w odniesieniu do obiektu
- Akcje wykonywane w celu wycofania złośliwych działań
- Informacje o przetwarzanym obiekcie:
  - Unikalny identyfikator procesu
  - Unikalny identyfikator procesu nadrzędnego
  - Unikalny identyfikator pliku procesu
  - Identyfikator procesu systemu Windows (PID)
  - Wiersz polecenia procesu
  - Konto użytkownika, które rozpoczęło proces
  - Kod sesji logowania, w której proces jest uruchomiony
  - Typ sesji, w której proces jest uruchomiony
  - Poziom integralności przetwarzanego obiektu
  - Członkostwo konta użytkownika, które rozpoczęło proces, w uprzywilejowanych grupach lokalnych i domenowych
  - Identyfikator przetwarzanego obiektu
  - Pełna nazwa przetwarzanego obiektu
  - Identyfikator chronionego urządzenia
  - Pełna nazwa obiektu (lokalna nazwa pliku lub adres internetowy pobranego pliku)
  - Skrót MD5 lub SHA256 przetwarzanego obiektu
  - Typ przetwarzanego obiektu
  - Data utworzenia przetwarzanego obiektu
  - Data ostatniej modyfikacji przetwarzanego obiektu
  - Rozmiar przetwarzanego obiektu
  - Atrybuty przetwarzanego obiektu
  - Organizacja sygnująca przetwarzany obiekt
  - Wynik weryfikacji certyfikatu cyfrowego przetwarzanego obiektu
  - Identyfikator zabezpieczeń (SID) przetwarzanego obiektu

- Identyfikator strefy czasowej przetwarzanego obiektu
- Adres internetowy pobierania przetwarzanego obiektu (tylko dla plików na dysku)
- Nazwa aplikacji, która pobrała plik
- Skróty MD5 i SHA256 aplikacji, która pobrała plik
- Nazwa aplikacji, która ostatnio zmodyfikowała plik
- Skróty MD5 i SHA256 aplikacji, która ostatnio zmodyfikowała plik
- Liczba uruchomień przetwarzanego obiektu
- Data i godzina pierwszego uruchomienia przetwarzanego obiektu
- Unikalne identyfikatory pliku
- Pełna nazwa pliku (lokalna nazwa pliku lub adres internetowy pobranego pliku)
- Ścieżka do przetwarzanej zmiennej rejestru systemu Windows
- Nazwa przetwarzanej zmiennej rejestru systemu Windows
- Wartość przetwarzanej zmiennej rejestru systemu Windows
- Typ przetwarzanej zmiennej rejestru systemu Windows
- Wskaźnik członkostwa przetwarzanego klucza rejestru w punkcie automatycznego uruchamiania
- Adres internetowy przetwarzanego żądania internetowego
- Źródło łącza przetwarzanego żądania internetowego
- Klient użytkownika przetwarzanego żądania internetowego
- Typ przetwarzanego żądania internetowego (`GET` lub `POST`)
- Lokalny port IP przetwarzanego żądania internetowego
- Zdalny port IP przetwarzanego żądania internetowego
- Kierunek połączenia (przychodzący lub wychodzący) przetwarzanego żądania internetowego
- Identyfikator procesu, w którym osadzono złośliwy kod

Kaspersky Sandbox

Wszystkie dane, które aplikacja przechowuje lokalnie na komputerze, są usuwane z komputera po odinstalowaniu Kaspersky Endpoint Security.

Dane serwisowe

Kaspersky Endpoint Security przechowuje następujące dane przetwarzane podczas automatycznego reagowania:

- Przetwarzane pliki i dane wprowadzone przez użytkownika podczas konfigurowania wbudowanego agenta Kaspersky Endpoint Security:
  - Pliki poddane kwarantannie
  - Klucz publiczny certyfikatu używanego do zintegrowania z serwerem Kaspersky Sandbox
- Pamięć podręczna wbudowanego agenta Kaspersky Endpoint Security:
  - Czas zapisania wyników skanowania w pamięci podręcznej
  - Skrót MD5 zadania skanowania
  - Identyfikator zadania skanowania
  - Wynik skanowania obiektu
- Kolejka żądań skanowania obiektów:
  - Identyfikator obiektu w kolejce
  - Czas umieszczenia obiektu w kolejce
  - Stan przetwarzania obiektu w kolejce
  - Identyfikator sesji użytkownika w systemie operacyjnym, w którym utworzono zadanie skanowania obiektów
  - Identyfikator systemu (SID) użytkownika systemu operacyjnego, którego konto zostało użyte do utworzenia zadania
  - Skrót MD5 zadania skanowania obiektów
- Informacje o zadaniach, dla których wbudowany agent Kaspersky Endpoint Security oczekuje na wyniki skanowania z serwera Kaspersky Sandbox:
  - Godzina odebrania zadania skanowania obiektu
  - Stan przetwarzania obiektu
  - Identyfikator sesji użytkownika w systemie operacyjnym, w którym utworzono zadanie skanowania obiektów
  - Identyfikator zadania skanowania obiektów
  - Skrót MD5 zadania skanowania obiektów
  - Identyfikator systemu (SID) użytkownika systemu operacyjnego, którego konto zostało użyte do utworzenia zadania
  - Schemat XML automatycznie tworzonego wskaźnika IOC

- Skrót MD5 lub SHA256 skanowanego obiektu
- Błędy przetwarzania
- Nazwy obiektów, dla których utworzono zadanie
- Wynik skanowania obiektu

Dane uwzględnione w żądaniach kierowanych do serwera Kaspersky Sandbox

Następujące dane z żądań z wbudowanego agenta Kaspersky Endpoint Security do Kaspersky Sandbox są przechowywane lokalnie na komputerze:

- Skrót MD5 zadania skanowania
- Identyfikator zadania skanowania
- Zeskanowany obiekt i wszystkie powiązane pliki

Dane otrzymane w wyniku wykonania zadania Skanowanie IOC (zadanie autonomiczne)

Kaspersky Endpoint Security automatycznie przesyła dane dotyczące wyników wykonania zadania skanowania *Skanowanie IOC* do Kaspersky Security Center.

Dane uwzględnione w wynikach wykonania zadania *Skanowanie IOC* mogą zawierać następujące informacje:

- Adres IP z tablicy ARP
- Adres fizyczny z tablicy ARP
- Typ i nazwa rekordu DNS
- Adres IP chronionego urządzenia
- Adres fizyczny (adres MAC) chronionego urządzenia
- Identyfikator uwzględniony we wpisie dziennika zdarzeń
- Nazwa źródła danych zapisana w dzienniku
- Nazwa dziennika
- Czas zdarzenia
- Skróty MD5 i SHA256 pliku
- Pełna nazwa pliku (łącznie ze ścieżką)
- Rozmiar pliku

- Zdalny adres IP, z którym nawiązano połączenie podczas skanowania
- Adres IP lokalnej karty sieciowej
- Port otwarty na lokalnej karcie sieciowej
- Numer protokołu (zgodnie ze standardem IANA)
- Nazwa procesu
- Argumenty procesu
- Ścieżka do pliku procesu
- Identyfikator procesu (PID) systemu Windows
- Identyfikator procesu nadrzędnego (PID) systemu Windows
- Konto użytkownika, które rozpoczęło proces
- Data i godzina rozpoczęcia procesu
- Nazwa usługi
- Opis usługi
- Ścieżka i nazwa usługi DLL (svchost)
- Ścieżka i nazwa pliku wykonywalnego usługi
- Identyfikator usługi (PID) systemu Windows
- Typ usługi (na przykład sterownik jądra lub karta sieciowa)
- Stan usługi
- Tryb uruchomienia usługi
- Nazwa konta użytkownika
- Nazwa woluminu
- Litera woluminu
- Typ woluminu
- Wartość rejestru systemu Windows
- Wartość gałęzi rejestru
- Ścieżka klucza rejestru (bez gałęzi i nazwy wartości)
- Ustawienie rejestru
- System (środowisko)

- Nazwa i wersja systemu operacyjnego zainstalowanego na urządzeniu
- Nazwa sieciowa chronionego urządzenia
- Domena lub grupa, do której należy chronione urządzenie
- Nazwa przeglądarki
- Wersja przeglądarki
- Czas ostatniego dostępu do zasobu internetowego
- Adres URL z żądania HTTP
- Nazwa konta użyta w żądaniu HTTP
- Nazwa pliku procesu, który wykonał żądanie HTTP
- Pełna ścieżka do pliku procesu, który wykonał żądanie HTTP
- Identyfikator procesu (PID) systemu Windows, który wykonał żądanie HTTP
- Strona odsyłająca HTTP (adres URL źródła żądania HTTP)
- Identyfikator URI zasobu żądanego przez HTTP
- Informacje o kliencie użytkownika HTTP (aplikacji, która wysłała żądanie HTTP)
- Czas wykonania żądania HTTP
- Unikalny identyfikator procesu, który wykonał zapytanie HTTP

Kaspersky Endpoint Detection and Response Expert (on-premises)

Wszystkie dane, które aplikacja przechowuje lokalnie na komputerze, są usuwane z komputera po odinstalowaniu Kaspersky Endpoint Security.

Dane serwisowe

Wbudowany agent Kaspersky Endpoint Security przechowuje lokalnie następujące dane:

- Dane wymagane do integracji z komponentem EDR Expert (on-premises):
  - Adres i port do połączenia z serwerem węzła centralnego KATA
  - Adres i port do połączenia z serwerem transmisji telemetrycznej
  - Adres i port do połączenia z serwerem odpowiedzi

    - Informacje o certyfikatach używanych do integracji z węzłem centralnym KATA
    - Informacje o certyfikatach użytych do integracji z serwerem transmisji telemetrycznej
    - Informacje o certyfikatach używanych do integracji z serwerem odpowiedzi
- Pliki poddane kwarantannie

Dane z przesłanych zdarzeń telemetrycznych

- **Dane telemetryczne**
    - Informacje o plikach:
        - Unikalne identyfikatory pliku
        - Typ plików
        - Pełna ścieżka pliku
        - Rozmiar pliku
        - Atrybuty pliku
        - Identyfikator strefy
        - Data i godzina utworzenia pliku
        - Data i godzina ostatniej modyfikacji pliku
        - Nazwa oryginalnego pliku
        - Nazwa aplikacji
        - Wersja aplikacji
        - Dostawca aplikacji
        - Opis pliku
        - Wersja pliku
        - Skróty MD5 i SHA256 obiektu
        - Wynik weryfikacji podpisu pliku
        - Nazwa wystawcy certyfikatu
        - Nazwa posiadacza certyfikatu
        - Numer seryjny certyfikatu

- Dane dotyczące skanowania AMSI:
  - Unikalny identyfikator procesu, który zainicjował aktywność
  - Typ zawartości obiektu przekazanego do AMSI
  - Zawartość obiektu przekazanego do AMSI
  - Nazwa obiektu
  - Skróty MD5 i SHA256 obiektu
- Dane dotyczące blokowania aplikacji:
  - Unikalny identyfikator procesu, który zainicjował blokowanie aplikacji
  - Unikalny identyfikator procesu nadrzędnego
  - Unikalny identyfikator systemowy procesu
  - Polecenie użyte do uruchomienia procesu
  - Identyfikator sesji logowania
  - Poziom integralności procesu
  - Status procesu
  - Unikalny identyfikator pliku procesu
  - Wiersz polecenia procesu
  - Lista unikalnych identyfikatorów plików interpretowanych
- Dane o zablokowanych otwarciach plików:
  - Unikalny identyfikator procesu, który zainicjował otwarcie pliku
  - Unikalne identyfikatory pliku
- Dane dotyczące ładowania sterownika:
  - Unikalny identyfikator załadowanego sterownika
- Dane o zdarzeniach:
  - Unikalny identyfikator zdarzenia
  - Data i godzina zdarzenia
- Dane dotyczące modyfikacji pliku:
  - Unikalny identyfikator procesu, który zainicjował modyfikację pliku
  - Unikalne identyfikatory pliku

    - Rodzaj operacji modyfikacji
    - Flaga wskazująca, że plik zostanie usunięty po ponownym uruchomieniu komputera
    - Unikalny identyfikator zmodyfikowanego pliku
    - Unikalny identyfikator pliku przed modyfikacją
    - Zestaw flag bitowych, które określają sposób, w jaki plik został otwarty
    - Dane o operacjach na liście kontroli dostępu
    - Dane o zmianach właściciela lub grupy nadrzędnej pliku
- Dane o sesji logowania:
    - Identyfikator sesji logowania
    - Nazwa zalogowanego użytkownika
    - Typ konta użytkownika
    - Typ sesji
- Dane o połączeniach sieciowych:
    - Unikalny identyfikator procesu, który zainicjował połączenie
    - Lokalny adres IP używany do inicjowania połączenia
    - Zdalny adres IP punktu końcowego połączenia
    - Kierunek połączenia
    - Protokół transferu danych
    - Metoda HTTP
    - Ścieżka bez nazwy hosta
    - Nazwa hosta
    - Dynamiczny stan procesu w momencie połączenia
    - Flaga wskazująca, że połączenie jest otwarte na poziomie gniazda typu raw
    - Wersja protokołu TLS używana w sesji połączenia
    - Nazwa serwera TLS
    - Skróty MD5 i SHA1 certyfikatu serwera TLS
    - Lista nazw Subject Alternative Name (SAN) certyfikatu
    - Nazwa wystawcy certyfikatu TLS

    - Numer seryjny certyfikatu
    - Użyty algorytm szyfrowania
    - Daty rozpoczęcia i zakończenia obowiązywania certyfikatu
    - Odcisk palca JA3 klienta TLS
    - Odcisk palca JA3S serwera
- Dane przechwycone podczas nasłuchiwania na porcie sieciowym:
    - Unikalny identyfikator procesu, który zainicjował połączenie
- Dane wejściowe z wiersza polecenia:
    - Unikalny identyfikator procesu, który zainicjował wejście konsoli
    - Typ wejścia konsoli
    - Tekst wprowadzony przez użytkownika lub proces
- Dane o utworzeniu procesu:
    - Unikalny identyfikator procesu
    - Unikalny identyfikator procesu nadrzędnego
    - Unikalny identyfikator systemowy procesu
    - Polecenie użyte do uruchomienia procesu
    - Identyfikator sesji logowania
    - Poziom integralności procesu
    - Unikalny identyfikator pliku procesu
    - Lista unikalnych identyfikatorów plików interpretowanych
    - Typ procesu
- Dane o module załadowanym przez proces:
    - Unikalny identyfikator procesu, który zainicjował pobieranie
    - Pełna ścieżka do pliku przesłanego do procesu
    - Unikalny identyfikator pliku modułu
    - Pełna kwalifikowana nazwa zestawu .NET, jeśli załadowany plik jest modułem .NET
    - Flagi zestawu .NET zdefiniowane w jego manifeście

- Dane o zakończeniu procesu:
  - Unikalny identyfikator procesu zakończonego
- Dane dotyczące modyfikacji rejestru:
  - Unikalny identyfikator procesu, który zainicjował modyfikację rejestru
  - Typ operacji rejestru
  - Pełna ścieżka do klucza rejestru
  - Nazwa wartości w kluczu rejestru
  - Typ danych przechowywanych w wartości klucza rejestru
  - Dane określone w wartości klucza rejestru
  - Nazwa klucza przed zmianą nazwy
  - Informacje dotyczące zmiany właściciela klucza lub grupy kluczy podstawowych
  - Lista zmian na liście kontroli dostępu (ACL) klucza
- Dane o wykrytym zagrożeniu i jego przetwarzaniu:
  - Flaga wskazująca, że wykrywanie zagrożeń zostało uruchomione w tle
  - Werdykt dotyczący zagrożenia
  - Nazwa werdyktu
  - Unikalny identyfikator rekordu bazy danych
  - Czas zapisania rekordu zagrożenia w bazie danych
  - Tryb przetwarzania zagrożenia
  - Typ zainfekowanego obiektu
  - Nazwa zainfekowanego obiektu
  - Skróty MD5 i SHA256 obiektu
  - Unikalny identyfikator zainfekowanego obiektu
  - Unikalny identyfikator procesu, który pobrał zainfekowany obiekt z Internetu
  - Adres URL, z którego pobrano zainfekowany obiekt
  - Adres e-mail nadawcy, który wysłał zainfekowany obiekt
  - Protokół sieciowy, za pośrednictwem którego otrzymano zainfekowany obiekt
  - Adres lokalny, z którego otrzymano zainfekowany obiekt

    - Adres zewnętrzny, z którego otrzymano zainfekowany obiekt
    - Typ zawartości obiektu
    - Zawartość obiektu
- Dane o dostępie do procesów:
    - Unikalny identyfikator procesu, który podjął próbę dostępu
    - Unikalny identyfikator procesu docelowego, do którego uzyskano dostęp
    - Zestaw praw żądanych od procesu docelowego
    - Typ operacji
    - Zestaw wywołań w momencie dostępu do procesu
    - Deskryptor procesu źródłowego
    - Deskryptor procesu docelowego
- Dane o DNS:
    - Unikalny identyfikator procesu, który zainicjował zapytanie DNS
    - Adres IP serwera DNS
    - Flagi zarządzające zachowaniem zapytania DNS
    - Stan zakończenia żądania
    - W pełni kwalifikowana nazwa domeny określona w zapytaniu DNS
    - Typ danych w zapytaniu DNS
    - Odpowiedzi serwera DNS
- Dane dotyczące wstrzyknięcia kodu:
    - Unikalny identyfikator procesu, który próbował wstrzyknąć kod
    - Użyta metoda dostępu
    - Zestaw wywołań w momencie wykrycia wstrzykniętego kodu
    - Unikalny identyfikator procesu docelowego, do którego przesłano kod
    - Dane o zmianach w sekwencji poleceń procesu docelowego
    - Adres procesu docelowego
    - Nazwa biblioteki DLL, która została przesłana do procesu docelowego
    - Pełna ścieżka do pliku DDL

- Dane o operacjach z kanałami nazwanymi:
  - Unikalny identyfikator procesu, który utworzył kanał lub połączył się z nim
  - Pełna nazwa nazwanego kanału
  - Typ operacji (utworzenie lub połączenie)
- Dane o zapytaniach WMI:
  - Unikalny identyfikator procesu, który zainicjował operację WMI
  - Typ operacji WMI
  - Nazwa urządzenia docelowego dla zapytania WMI
  - Konto użytkownika, które zainicjowało zapytanie WMI
  - Tekst zapytania WMI
  - Przestrzeń nazw, w której wykonywane jest zapytanie WMI
  - Nazwa filtra WMI
  - Nazwa obiektu konsumenta
  - Tekst opisujący działanie obiektu konsumenta
- Dane o zapytaniach LDAP:
  - Unikalny identyfikator procesu, który wykonał zapytanie LDAP
  - Zakres wyszukiwania zapytań LDAP
  - Filtr LDAP
  - Parametr określający partycję usługi Active Directory, do której skierowano zapytanie
  - Atrybuty wyszukiwania LDAP
- Dane o podłączonych urządzeniach USB:
  - Typ działania urządzenia USB
  - Typ urządzenia USB
  - Identyfikator urządzenia USB
  - Nazwa urządzenia USB
  - Ścieżka do urządzenia USB
  - Flaga wskazująca, że urządzenie USB jest dyskiem systemowym
- Dane dotyczące tworzenia, usuwania i modyfikowania zaplanowanego zadania

- Dane dotyczące tworzenia, usuwania i modyfikacji usług
- Dane dotyczące podłączania/odłączania systemu plików
- Dane dotyczące działania komponentu EDR Expert on-premise:
  - Informacje o uruchamianiu/zatrzymywaniu agenta
  - Informacje o instalowaniu/odinstalowywaniu agenta
  - Unikalny identyfikator startu agenta
  - Identyfikator systemowy procesu agenta
  - Unikalny identyfikator procesu agenta
  - Powód zakończenia agenta
  - Kod zakończenia procesu agenta

- Ustawienia filtrowania zdarzeń:
  - Nazwy modułów
  - Pełne ścieżki do obiektów
  - Skróty MD5 i SHA256 obiektów
  - Identyfikatory wpisów w dzienniku zdarzeń systemu Windows
  - Ustawienia certyfikatów cyfrowych
  - Kierunek ruchu, adresy IP, porty, protokoły, pełne ścieżki do plików wykonywalnych
  - Nazwy użytkowników
  - Typy logowania użytkowników
  - Typy zdarzeń telemetrycznych, dla których są stosowane filtry

Dane uwzględnione w żądaniach składnika EDR Expert kierowanych do wbudowanego agenta Kaspersky Endpoint Security

- Ustawienia zadania ogólnego:
  - Typ zadania
  - Ustawienia planowania zadań
  - Nazwy i hasła kont, których można używać do wykonywania zadań
  - Wersje ustawień

    - Identyfikatory obiektów poddanych kwarantannie
    - Ścieżki do obiektów
    - Skróty MD5 i SHA256 obiektów
    - Wiersz polecenia z argumentami używany do rozpoczynania procesu
    - Flagi dodatkowych akcji wykonywanych po wykonaniu zadań
    - Identyfikatory plików IOC do pobrania z serwera
    - Pliki IOC
    - Nazwa usługi
    - Typ uruchomienia usługi
    - Foldery, dla których należy odebrać wyniki zadania pobierania danych śledczych (*Get forensic*)
    - Maski nazw obiektów i rozszerzeń dla zadania pobierania danych śledczych (*Get forensic*)
- Ustawienia izolacji sieci:
    - Typy ustawień
    - Wersje ustawień
    - Listy wykluczeń izolacji sieci i ustawień wykluczeń: kierunek ruchu, adresy IP, porty, protokoły i pełne ścieżki do plików wykonywalnych
    - Flagi dodatkowych akcji
    - Czas wyłączenia automatycznej izolacji
- Ustawienia zapobiegania wykonywania:
    - Typy ustawień
    - Wersje ustawień
    - Listy reguł zapobiegania wykonywaniu i ustawień reguł: ścieżki do obiektów, typy obiektów, skróty MD5 i SHA256 obiektów
    - Flagi dodatkowych akcji

Dane z żądań wysłanych przez Kaspersky Endpoint Security do komponentu EDR Expert

Podczas integracji z rozwiązaniem EDR Expert (on-premises) następujące dane są przechowywane lokalnie na komputerach.

- W żądaniach synchronizacji:
  - Unikalny identyfikator
  - Podstawowa część adresu internetowego serwera
  - Nazwa komputera
  - Adres IP komputera
  - Adres MAC komputera
  - Czas lokalny na komputerze
  - Stan autoochrony Kaspersky Endpoint Security
  - Nazwa i wersja systemu operacyjnego zainstalowanego na urządzeniu
  - Wersji Kaspersky Endpoint Security
  - Wersje ustawień aplikacji i ustawień zadań
  - Stany zadań: identyfikatory zadań, stany wykonania, kody błędów
- W żądaniach związanych z pobieraniem plików z serwera:
  - Unikalne identyfikatory plików
  - Unikalny identyfikator Kaspersky Endpoint Security
  - Unikalne identyfikatory certyfikatów
  - Podstawowa część adresu internetowego serwera z zainstalowanym składnikiem Central Node
  - Adres IP hosta
- W raportach z wyników realizacji zadań:
  - Adres IP hosta
  - Informacje o obiektach wykrytych podczas skanowania IOC lub skanowania YARA
  - Flagi dodatkowych akcji wykonywanych po wykonaniu zadań
  - Błędy wykonania zadań i zwracane kody
  - Stany wykonania zadań

    - Czas wykonania zadań
    - Wersje ustawień używanych do wykonywania zadań
    - Informacje o obiektach przesłanych na serwer, obiektach poddanych kwarantannie i obiektach przywróconych z kwarantanny: ścieżki do obiektów, skróty MD5 i SHA256, identyfikatory obiektów poddanych kwarantannie
    - Informacje o procesach uruchomionych lub zatrzymanych na żądanie serwera na komputerze: identyfikator PID i UniquePID, kod błędu, skróty MD5 i SHA256 obiektów
    - Informacje o usługach uruchomionych lub zatrzymanych na komputerze na żądanie serwera: nazwa usługi, typ uruchomienia, kod błędu, skróty MD5 i SHA256 obrazów plików usług
    - Informacje o obiektach, dla których wykonano zrzut pamięci do skanowania YARA (ścieżki, identyfikator pliku zrzutu)
    - Pliki żądane przez serwer
- Dane związane z uruchomionymi procesami:
    - Nazwa pliku wykonywalnego z pełną ścieżką i rozszerzeniem
    - Parametry automatycznego uruchamiania procesu
    - Identyfikator procesu
    - Identyfikator sesji logowania
    - Nazwa sesji logowania
    - Data i godzina rozpoczęcia procesu
    - Skróty MD5 i SHA256 obiektu
- Informacje o plikach:
    - Ścieżka pliku
    - Nazwa pliku
    - Rozmiar pliku
    - Atrybuty pliku
    - Data i godzina utworzenia pliku
    - Data i godzina ostatniej modyfikacji pliku
    - Opis pliku
    - Nazwa firmy

- Skróty MD5 i SHA256 obiektu
- Klucz rejestru (dla punktów automatycznego uruchamiania)

- Dane związane z błędami występującymi podczas pobierania informacji o obiektach:
  - Pełna nazwa obiektu przetwarzanego podczas wystąpienia błędu
  - Kod błędu

- Dane w wynikach skanowania YARA:

  Wbudowany agent Kaspersky Endpoint Security automatycznie przesyła wyniki skanowania YARA do serwera Kaspersky Anti Targeted Attack Platform w celu zbudowania łańcucha rozwoju zagrożeń.

  Dane są tymczasowo przechowywane lokalnie w kolejce do wysyłania wyników wykonania zadań do serwera Kaspersky Anti Targeted Attack Platform. Dane są usuwane z pamięci tymczasowej po ich przesłaniu.

  - Skróty MD5 i SHA256 pliku
  - Pełna nazwa pliku
  - Ścieżka pliku
  - Rozmiar pliku
  - Nazwa procesu
  - Argumenty procesu
  - Ścieżka do pliku procesu
  - Identyfikator procesu (PID) systemu Windows
  - Identyfikator procesu nadrzędnego (PID) systemu Windows
  - Konto użytkownika, które rozpoczęło proces
  - Data i godzina rozpoczęcia procesu

- Dane w wynikach skanowania IOC:
  - Adres IP z tablicy ARP
  - Adres fizyczny z tablicy ARP
  - Nazwa rekordu DNS
  - Typ rekordu DNS
  - Nazwa hosta
  - Adres IP
  - Identyfikator zdarzenia w dzienniku
  - Nazwa źródła danych zapisana w dzienniku

- Nazwa dziennika
- Nazwa użytkownika
- Data i godzina wygenerowania zdarzenia w formacie ISO
- Skróty MD5 i SHA256 pliku
- Pełna nazwa pliku
- Rozmiar pliku
- Zdalny adres IP, z którym nawiązano połączenie podczas skanowania
- Adres IP i port lokalnego adaptera
- Protokół
- Nazwa procesu
- Argumenty procesu
- Ścieżka do pliku procesu
- Identyfikator procesu (PID) systemu Windows
- Identyfikator procesu nadrzędnego (PID) systemu Windows
- Konto użytkownika, które rozpoczęło proces
- Data i godzina rozpoczęcia procesu
- Ścieżka do klucza rejestru
- Nazwa klucza rejestru
- Wartość tekstowa klucza rejestru
- Nazwa usługi
- Opis usługi
- Ścieżka i nazwa usługi DLL
- Ścieżka i nazwa pliku wykonywalnego usługi
- Identyfikator usługi (PID) systemu Windows
- Rodzaj usługi
- Stan usługi
- Tryb uruchomienia usługi
- Nazwa systemu operacyjnego

- Wersja systemu operacyjnego
- Nazwa sieci komputerowej bez domeny
- Domena lub grupa robocza
- Nazwa użytkownika
- Nazwa woluminu
- Litera woluminu
- Typ woluminu

Kaspersky Network Detection and Response (KATA)

Wszystkie dane, które aplikacja przechowuje lokalnie na komputerze, są usuwane z komputera po odinstalowaniu Kaspersky Endpoint Security.

Dane telemetryczne

- **Dane dotyczące plików**
  - Unikalne identyfikatory pliku
  - Typ plików
  - Pełna ścieżka pliku
  - Rozmiar pliku
  - Atrybuty pliku
  - Identyfikator strefy
  - Data i godzina utworzenia pliku
  - Data i godzina ostatniej modyfikacji pliku
  - Nazwa oryginalnego pliku
  - Nazwa aplikacji
  - Wersja aplikacji
  - Dostawca aplikacji
  - Opis pliku

- Wersja pliku
- Skróty MD5 i SHA256 obiektu
- Wynik weryfikacji podpisu pliku
- Data i godzina utworzenia sygnatury pliku
- Łańcuchy certyfikatów używane w pliku podpisu
- Typ łańcucha certyfikatu
- Certyfikaty w łańcuchu
- Nazwa wystawcy certyfikatu
- Nazwa posiadacza certyfikatu
- Numer seryjny certyfikatu
- Algorytm odcisku palca certyfikatu
- Odcisk palca certyfikatu
- Okres ważności certyfikatu

- **Dane o sesji logowania**
  - Identyfikator sesji logowania
  - Nazwa konta zalogowanego użytkownika
  - Typ konta użytkownika
  - Typ sesji
  - Adres IP komputera, z którego podjęto próbę logowania
  - Adres IP komputera lokalnego, na którym podjęto próbę logowania
  - Flaga wskazująca, że sesja reprezentowana przez to zdarzenie ma podwyższone uprawnienia i prawa administratora
  - Parametr wskazujący, czy inne sesje są powiązane z tą sesją logowania
  - Protokół używany w sesji terminalowej
  - Protokół IPv4 używany w sesji terminalowej
- **Dane o komunikacji sieciowej**
  - Początek i koniec okresu gromadzenia danych
  - Lista połączeń

- Lokalny adres IP komputera
- Lokalny adres MAC komputera
- Zdalny adres IP komputera
- Zdalny adres MAC komputera
- Adres IP bramy
- Liczba przesłanych pakietów danych
- Liczba odebranych pakietów danych
- Całkowita liczba przesłanych bajtów
- Protokół transferu danych
- Pole EtherType ramki Ethernet
- Prefiks ładunku pierwszego pakietu w przedziale
- Adres IPv4 interfejsu sieciowego, przez który przechwycono komunikację

- **Dane o połączeniu sieciowym**
  - Unikalny identyfikator procesu, który zainicjował połączenie
  - Protokół transferu danych
  - Lokalny adres IP używany do inicjowania połączenia
  - Zdalny adres IP punktu końcowego połączenia
  - Metoda HTTP
  - Ścieżka bez nazwy hosta
  - Nazwa hosta
  - Dynamiczny stan procesu w momencie połączenia
  - Kierunek połączenia
  - Dynamiczny stan procesu
  - Pole EtherType ramki Ethernet
- **Dane przechwycone podczas nasłuchiwania na porcie sieciowym**
  - Unikalny identyfikator procesu, który zainicjował połączenie
  - Protokół transferu danych

- Lokalny adres
- Dynamiczny stan procesu w momencie połączenia

- **Wynik weryfikacji połączenia**
  - Ustawienia sieciowe hosta
  - Opis interfejsu sieciowego
  - Nazwa domeny DNS
  - Lokalny adres MAC komputera
  - Numer metryki połączenia IP
  - Lista adresów IP
  - Adres IP
  - Maska sieciowa
  - Adres IP bramy
  - Adres MAC bramy
  - Lista zainstalowanych poprawek
  - Numer poprawki
  - Data instalacji poprawki
  - Model urządzenia
  - Dostawca urządzenia
  - ID hosta w Kaspersky Security Center
  - Opis zainstalowanego antywirusa Kaspersky
  - Nazwa komponentu zainstalowanego antywirusa Kaspersky
  - Wersja komponentu zainstalowanego antywirusa Kaspersky
  - Wersja bazy danych zainstalowanego komponentu antywirusa Kaspersky
  - Data ostatniej aktualizacji bazy danych zainstalowanego komponentu antywirusa Kaspersky
  - Status komponentów zainstalowanego antywirusa Kaspersky
  - Lista kluczy licencyjnych
  - Numer seryjny klucza
  - Typ klucza

- Data wygaśnięcia klucza
- Stan klucza

- **Dane dotyczące tworzenia procesów w hoście**
  - Unikalny identyfikator procesu
  - Unikalny identyfikator procesu nadrzędnego
  - Unikalny identyfikator systemowy procesu
  - Polecenie użyte do uruchomienia procesu
  - Identyfikator sesji logowania
  - Identyfikator sesji terminalowej
  - Unikalny identyfikator pliku procesu
  - Poziom integralności procesu
  - Lista tokenów uprawnień procesu
  - Uprawnienia atrybutu
  - Lista unikalnych identyfikatorów plików interpretowanych
  - Status procesu
  - Polecenie użyte do uruchomienia procesu
- **Dane o zakończeniu procesu**
  - Unikalny identyfikator procesu
- **Dane o wykrytym zagrożeniu**
  - Informacje o zagrożeniu
  - Werdykt dotyczący zagrożenia
  - Numer rekordu AMR
  - Wersja bazy danych antywirusowych
  - Tryb wykrywania zagrożeń
  - Unikalny identyfikator zagrożenia
  - Technologia ochrony
  - Informacje o zainfekowanym obiekcie
  - Typ zainfekowanego obiektu

- Nazwa zainfekowanego obiektu
- Skróty MD5 i SHA256 obiektu
- Unikalny identyfikator zainfekowanego procesu
- Unikalny identyfikator zainfekowanego obiektu
- Unikalny identyfikator procesu, który pobrał zainfekowany obiekt z Internetu
- Adres URL, z którego pobrano zainfekowany obiekt
- Adres e-mail nadawcy, który wysłał zainfekowany obiekt
- Protokół sieciowy, za pośrednictwem którego otrzymano zainfekowany obiekt
- Adres lokalny, z którego otrzymano zainfekowany obiekt
- Adres zewnętrzny, z którego otrzymano zainfekowany obiekt
- Typ zawartości obiektu
- Kontekst wykrytego zagrożenia
- Zawartość obiektu
- Flaga wskazująca, że wykrywanie zagrożeń zostało uruchomione w tle

- **Dane dotyczące przetwarzania zagrożeń**
  - Informacje o zagrożeniu
  - Werdykt dotyczący zagrożenia
  - Numer rekordu AMR
  - Wersja bazy danych antywirusowych
  - Tryb wykrywania zagrożeń
  - Nazwa zainfekowanego obiektu
  - Skróty MD5 i SHA256 obiektu
  - Unikalny identyfikator zainfekowanego procesu
  - Unikalny identyfikator zainfekowanego obiektu
  - Protokół sieciowy, za pośrednictwem którego otrzymano zainfekowany obiekt
  - Adres lokalny, z którego otrzymano zainfekowany obiekt
  - Adres zewnętrzny, z którego otrzymano zainfekowany obiekt
  - Stan przetwarzania zagrożenia

- Powód, dla którego nie można skorygować zagrożenia
- Lokalny adres fizyczny

- **Dane o użytkownikach**
  - Identyfikator SID użytkownika
  - Identyfikator użytkownika
  - Nazwa użytkownika
  - Pełna nazwa użytkownika
  - Opis użytkownika
  - Określa, czy konto jest aktywne czy zablokowane
  - Określa, czy hasło wygasło
  - Określa, czy wymagana jest zmiana hasła
  - Określa, czy dozwolona jest zmiana hasła
  - Typ konta użytkownika
  - Określa, czy dla tego konta włączone jest automatyczne logowanie
  - Lista grup, do których należy użytkownik

Integracja z Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Wszystkie dane, które aplikacja przechowuje lokalnie na komputerze, są usuwane z komputera po odinstalowaniu Kaspersky Endpoint Security.

Podczas integracji z Kaspersky Unified Monitoring and Analysis Platform (KUMA) przesyłane są dane dotyczące ustawień połączenia, a także wszystkie zdarzenia zarejestrowane w dziennikach systemu Windows.

Główne dzienniki zdarzeń systemu Windows to: System, Security, Application, ForwardedEvents i HardwareEvents. Użytkownicy mogą również tworzyć i wykorzystywać niestandardowe dzienniki, aby spełnić swoje specyficzne wymagania.

Zgodność z prawem Unii Europejskiej (RODO)

Kaspersky Endpoint Security może przesyłać dane do Kaspersky w następujących scenariuszach:

- Korzystanie z Kaspersky Security Network.
- Aktywowanie aplikacji przy użyciu kodu aktywacyjnego.

- Aktualizowanie modułów i antywirusowych baz danych aplikacji.
- Otwieranie odnośników w interfejsie aplikacji.

Niezależnie od klasyfikacji danych i terytorium, z którego dane są otrzymywane, firma Kaspersky stosuje się do najwyższych standardów bezpieczeństwa danych i wdraża różne prawne, organizacyjne i techniczne środki ochrony danych użytkowników, aby zagwarantować bezpieczeństwo i poufność danych, a także żeby zapewnić przestrzeganie praw użytkowników zagwarantowanych przez obowiązujące prawo. Treść Polityki prywatności jest dostępna w pakiecie dystrybucyjnym aplikacji oraz na stronie internetowej Kaspersky.

Zanim zaczniesz korzystać z Kaspersky Endpoint Security uważnie przeczytaj opis przesyłanych danych w Umowie licencyjnej i w Oświadczeniu Kaspersky Security Network. Jeśli określone dane przesyłane z Kaspersky Endpoint Security zgodnie z jednym z wyżej opisanych scenariuszy można zaklasyfikować jako dane osobowe zgodnie z prawem lokalnym lub standardowym, musisz upewnić się, że takie dane są przetwarzane zgodnie z prawem i uzyskać zgodę użytkowników końcowych na gromadzenie i przesyłanie tych danych.

Przeczytaj Umowę licencyjną i odwiedź stronę internetową Kaspersky, aby dowiedzieć się więcej o otrzymywaniu, przetwarzaniu, przechowywaniu i niszczeniu przez Kaspersky informacji dotyczących korzystania z aplikacji po zaakceptowaniu Umowy licencyjnej i Oświadczenia Kaspersky Security Network. Pliki license.txt i ksn_<ID języka>.txt zawierają treść Umowy licencyjnej i Oświadczenia Kaspersky Security Network i można je znaleźć w pakiecie dystrybucyjnym aplikacji.

Jeśli nie chcesz przesłać danych do Kaspersky, możesz wyłączyć dostarczanie danych.

Korzystanie z Kaspersky Security Network

Korzystając z Kaspersky Security Network, możesz wyrazić zgodę na automatyczne dostarczanie danych wymienionych w Oświadczeniu Kaspersky Security Network. Jeśli nie zgadzasz się na przekazanie tych danych firmie Kaspersky, skorzystaj z Kaspersky Private Security Network (KPSN) lub wyłącz korzystanie z KSN. Więcej informacji o sieci KPSN można znaleźć w dokumentacji do Kaspersky Private Security Network.

Aktywowanie aplikacji przy użyciu kodu aktywacyjnego

Korzystając z kodu aktywacyjnego, wyrażasz zgodę na automatyczne dostarczanie danych wymienionych w Umowie licencyjnej. Jeśli nie zgadzasz się na przesłanie tych danych do Kaspersky, użyj pliku klucza do aktywacji Kaspersky Endpoint Security.

Aktualizowanie modułów i antywirusowych baz danych aplikacji

Korzystając z serwerów Kaspersky, wyrażasz zgodę na automatyczne dostarczanie danych wymienionych w Umowie licencyjnej. Kaspersky wymaga tych informacji do sprawdzenia, czy Kaspersky Endpoint Security jest używany legalnie. Jeśli nie wyrażasz zgody na dostarczenie tych informacji do Kaspersky, użyj Kaspersky Security Center do aktualizacji baz danych lub Kaspersky Update Utility.

Otwórz odnośniki w interfejsie aplikacji

Korzystając z odnośników w interfejsie aplikacji, wyrażasz zgodę na automatyczne dostarczanie danych wymienionych w Umowie licencyjnej. Dokładna lista danych przesyłanych w każdym określonym odnośniku zależy od miejsca, w którym odnośnik się znajduje w interfejsie aplikacji, a także od problemu, który ma zostać rozwiązany. Jeśli nie wyrażasz zgody na dostarczenie tych danych do Kaspersky, użyj uproszczonego interfejsu aplikacji lub ukryj interfejs aplikacji.

Zapisywanie zrzutu pamięci

Jeśli masz włączoną opcję zapisu zrzutów pamięci, Kaspersky Endpoint Security utworzy plik zrzutu pamięci, który będzie zawierał wszelkie dane pamięci z procesów aplikacji w momencie, gdy ten plik zrzutu pamięci został utworzony.

Informacje o znakach towarowych

Zastrzeżone znaki towarowe i usługowe stanowią odpowiednio własność ich właścicieli.

Adobe, Acrobat, Flash, Reader i Shockwave są zastrzeżonymi znakami towarowymi lub znakami towarowymi Adobe zarejestrowanymi w Stanach Zjednoczonych i/lub innych krajach.

Amazon, Amazon Web Services, AWS są znakami towarowymi firmy Amazon.com, Inc. lub jej podmiotów stowarzyszonych.

Apple, FireWire, iTunes, Mac i Safari są znakami towarowymi firmy Apple Inc.

ARM to zarejestrowany znak towarowy firmy Arm Limited (lub jej spółek zależnych) w Stanach Zjednoczonych i/lub innych krajach.

AutoCAD jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Autodesk, Inc. i/lub jej oddziałów w Stanach Zjednoczonych i/lub innych krajach.

Słowo, znak i logo Bluetooth są własnością firmy Bluetooth SIG, Inc.

Borland jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Borland Software Corporation.

Cisco, Cisco AnyConnect, IOS to zastrzeżone znaki towarowe lub znaki towarowe firmy Cisco Systems, Inc. i/lub podmiotów stowarzyszonych na terenie Stanów Zjednoczonych i niektórych innych krajów.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop i 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.

Cloudflare, Cloudflare Workers i logo Cloudflare są znakami towarowymi i/lub zastrzeżonymi znakami towarowymi firmy Cloudflare, Inc. w Stanach Zjednoczonych i innych jurysdykcjach.

Core jest znakiem towarowym firmy Intel Corporation lub jej spółek zależnych.

dBase jest znakiem towarowym firmy dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC i inne znaki towarowe są znakami towarowymi firmy Dell Inc. lub jej podmiotów zależnych.

Docker i logo Docker są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Docker, Inc. w Stanach Zjednoczonych i innych krajach. Docker, Inc. i inne podmioty mogą również posiadać prawa do znaków towarowych w innych terminach użytych w niniejszym dokumencie.

ESET jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy ESET spol. s r.o. lub odpowiedniego podmiotu ESET.

Foxit to zastrzeżony znak towarowy firmy Foxit Corporation.

Radmin jest zarejestrowanym znakiem towarowym firmy Famatech.

Google, Android, Google Public DNS, Google Chrome i Chrome są znakami towarowymi firmy Google LLC.

HUAWEI, FusionCompute i FusionSphere są znakami towarowymi firmy Huawei Technologies Co., Ltd.

ICQ jest znakiem towarowym i/lub znakiem usługowym firmy ICQ LLC.

Intel jest znakiem towarowym firmy Intel Corporation lub jej spółek zależnych.

IBM jest znakiem towarowym firmy International Business Machines Corporation, zarejestrowanym w wielu jurysdykcjach na świecie.

Lenovo i Lenovo ThinkPad są znakami towarowymi firmy Lenovo, zarejestrowanymi w Stanach Zjednoczonych i/lub innych krajach.

Linux jest zastrzeżonym znakiem towarowym firmy 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.

LogMeIn Pro i Remotely Anywhere to znaki towarowe firmy LogMeIn, Inc.

Mail.ru jest znakiem towarowym firmy Mail.ru LLC.

McAfee jest znakiem towarowym lub zarejestrowanym znakiem towarowym firmy McAfee LLC lub jej spółek zależnych w Stanach Zjednoczonych i/lub innych krajach.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server i Windows Store są znakami towarowymi grupy spółek Microsoft.

Mozilla, Firefox i Thunderbird są znakami towarowymi Mozilla Foundation w Stanach Zjednoczonych i innych krajach.

NetApp to znak towarowy lub zastrzeżony znak towarowy firmy NetApp, Inc., zarejestrowany w Stanach Zjednoczonych i/lub innych krajach.

OpenSSL jest znakiem towarowym będącym własnością OpenSSL Software Foundation.

OpenStack jest znakiem towarowym firmy OpenStack Foundation, zarejestrowanym w Stanach Zjednoczonych i innych krajach.

Oracle, Java i JavaScript są zastrzeżonymi znakami towarowymi firmy Oracle i/lub jej oddziałów.

Python jest znakiem towarowym lub zarejestrowanym znakiem towarowym Python Software Foundation.

Realtek jest znakiem towarowym firmy Realtek Semiconductor Corporation.

SAMSUNG jest znakiem towarowym SAMSUNG, zarejestrowanym w Stanach Zjednoczonych i innych krajach.

Thawte jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Symantec Corporation lub jej oddziałów, zarejestrowanym w Stanach Zjednoczonych i innych krajach.

Trend Micro jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Trend Micro Incorporated.

VERISIGN jest zastrzeżonym lub niezastrzeżonym znakiem towarowym firmy VeriSign, Inc. i jej oddziałów, zarejestrowanym w Stanach Zjednoczonych i innych krajach.

VMware, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools i VMware vSphere są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy VMware, Inc., zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

Informacje o kodzie firm trzecich

Informacje o kodzie firm trzecich znajdują się w pliku legal_notices.txt przechowywanym w folderze instalacyjnym aplikacji.